A FRAMEWORK FOR BIRTH DATA REGISTRATION AND VERIFICATION USING SMART CONTRACTS, PUBLIC KEY ENCRYPTION, AND NATIONAL IDENTIFICATION NUMBER (NIN)

BY

BENNETT, Chimdinma Uche
MT*ech*/SICT/2018/9193

DEPARTMENT OF COMPUTER SCIENCE
FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA

APRIL, 2023

A FRAMEWORK FOR BIRTH DATA REGISTRATION AND VERIFICATION USING SMART CONTRACTS, PUBLIC KEY ENCRYPTION, AND NATIONAL IDENTIFICATION NUMBER (NIN)

BY

BENNETT, Chimdinma Uche
MT*ech*/SICT/2018/9193

A THESIS SUBMITTED TO THE POSTGRADUATE SCHOOL FEDERAL UNIVERSITY OF TECHNOLOGY, MINNA, NIGERIA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF TECHNOLOGY (MTECH) IN COMPUTER SCIENCE

APRIL, 2023

ABSTRACT

The digitization of birth registration using blockchain technology has emerged as a potential solution to address the challenges faced by traditional birth registration systems. The use of blockchain offers decentralization, security, and transparency, which can help improve the integrity and reliability of birth records. Existing security solutions, such as centralized architectures, high computation and communication costs, and lack of scalability, robustness, and auditability, have limitations that blockchain can overcome. The designed framework proposed in this study aims to simplify the birth registration process and enhance data transfer, transparency, and effective record maintenance using blockchain technology, specifically the Corda platform. The framework includes steps such as registering birth data, issuing digital birth certificates, storing a digital copy of the certificate, and verifying the integrity of the certificate using smart contracts. The use of private encryption further enhances the security of the birth records. To evaluate the performance of the framework, the BLOCKBENCH evaluation framework is used, which measures parameters such as latency, throughput, fault tolerance, and scalability. The results of the evaluation using Corda as a case study show that as the number of nodes increases from 1 to 50, the latency decreases and the throughput increases, indicating higher scalability values. This suggests that Corda achieves good scalability with moderate network growth. The proposed framework using Corda blockchain platform is recommended for local governments and healthcare centers to improve the birth registration process, enhance the integrity and security of birth records, and enable efficient record management. The use of blockchain technology can help address the challenges faced by traditional birth registration systems, such as lack of interoperability, unverifiable declarations of age, and low credibility of birth certificates due to corruption. However, it is important to carefully consider the implementation and customization of the framework to suit the specific requirements and regulations of each local government or healthcare center.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

1.0 INTRODUCTION

1.1 Background to the Study

The World Health Organization (WHO) estimates that 140 million births take place worldwide each year (World Health Organisation, 2016). Through birth registration, society first recognizes a child's existence and identity, and birth registration is one of the ten vital records recommended by the United Nations that is to be documented (Department of Economic and Social Affairs - Statistics Division, 2014). Birth registration is a universal, continuous, permanent, and compulsory record responsible for national planning (Mills *et al.,* 2019), which is a form of civil registration that establishes an individual's legal identity. Birth certificate (BC) issued as a legal document after a birth is registered is to identify a person in their capacity as a nation's citizen and where this is not available; there is provision for birth attestation or age declaration issued by a competent court of law, which can be generally referred to as proof of age. All these documents exist in paper form (UNICEF, 2019), with or without duplicates making access to such records quite difficult in cases of theft or loss. In Warasart and Kuacharoen (2012), a physical birth certificate cannot be effectively replaced by an electronic document, but with the advent of various scanning and printing techniques, the integrity of both the people in possession of birth certificates and the authorities who issued them is at risk. The ease of change has increased due to the lack of tools for BC verification and validation (Shah & Kumar, 2019). Verifying that a birth certificate is legitimate and that the person holding it is the rightful owner is necessary. More

specifically, a birth record must be validated to guarantee that its information is accurate and that the birth certificate was issued by a reliable source (Chen *et al.*, 2017).

Blockchain Technology (BCT) being an emergent digital technology (Al-Housni, 2019), has recently acquired significant traction in a number of industry, public, and corporate sectors, particularly in the financial and banking sectors as a result of the sharp rise in bitcoin valuation. A blockchain is essentially a distributed ledger or shared database (Tara, 2018) that permits the recording (but not alteration or deletion) and sharing of information amongst various entities. It is a distributed data structure made up of blocks that are chained together and include records or transactions that are kept in chronological order (Mehdi, 2017). Birth registration, crucial events like marriage and death, is a continual and permanent record of occurrence. Individual occurrences can be recorded using blockchain technology, which has the advantages of being a distributed ledger, unchangeable, and secure. Blockchain Technology (BCT) is, a decentralized ledger (Tara, 2018) where a "block"—a record of every transaction made in the network—is made up of encrypted data representing the whole transaction history. The shared information is transparent; thanks to this distributed ledger's chain of information "blocks," each of which is marked by a cryptographic signature (Jacobovitz, 2016.). In this work, BCT will be used to implement registration, verification, and validation of BC.

1.2 Statement of Problem

Birth registration is a vital statistics' civil registration component, and is a measure to monitor the impact of sustainable development and decision making for the government (Mills *et al*., 2019). According to the United Nations Children's Fund (UNICEF), birth registration exists on paper in most parts of the world (UNICEF, 2019) or as silos of birth records that may

differ from place to place with no form of interoperability within the same country; implying that birth information only exists at the place where the birth is registered. Unverifiable declaration of age issued by the courts has also become the norm of the day. This threatens the integrity of the birth certificate holders and the government body that issues the certificate. Therefore, validation and verification of an individual's birth record have become a challenge. It is necessary to ensure the integrity of the birth certificate presented by any individual. Birth record has to be verified to ensure that its content is correct and issued from an authentic source. The credibility of Nigerian birth certificates has been rated low by a Danish Report partly due to the level of corruption in the Nigerian civil service (Danish National ID Centre, 2018). Hence, the integrity of most of the birth certificates or declarations of age and the issuing authorities is questionable (Shah & Kumar, 2019).

The integrity and security of important data like birth certificates, medical records, passports, and even financial transactions have not truly improved with the digitization of these information, but it has reduced the time and effort required to maintain those records (Shah & Kumar, 2019).

In order to solve the birth registration problem, blockchain technology will be used as a means of storing, verifying and validating each individual birth record and ensuring the integrity of birth data. Blockchain technology is suitable for decentralized and transactional sharing of data, and its cryptographic techniques ensure that no record is replicated across all network nodes, building trust in the distributed software architecture.

1.3 Aim and Objectives

The aim of this work is to design a framework for birth data registration and verification using smart contracts, public key encryption, and National Identification Number (NIN with the following objectives:

1. To design a birth registration system that utilizes smart contracts for new live birth certification processes.
2. To develop a secure and efficient system that utilizes blockchain technology to store and verify birth records, ensuring the integrity of the data and improving the credibility of birth certificates in Nigeria.
3. To develop a plan for implementing the birth certification process on a blockchain network.

1.4 Significance of the Study

The use of blockchain technology is widespread, including health, education, property management, civil registration, voting processes etc. Blockchain technology is a preferred solution for storing and ensuring the integrity of vital records like birth certificate and other legal records because of its transparency and secure nature that does not allow for double entry and/or altering of data by unauthorized members of the network. It provides a joint basis for exchanging information, managing information, and transferring value.

This research creates a basis for the adoption of blockchain technology for keeping civil vital record and ensuring the integrity of such records for the good of the general public.

1.5 Scope of the Study

This study is limited to the use of Corda blockchain framework that is both private and permissioned, public & private key encryption, smart contracts for record management and verification of vital birth records in Nigeria.

1.6 Definition of Terms

Credential: A system, procedure, item, or document known as a credential serves as a means of trust and authentication for a person's identification. Birth certificates, national ID cards, digital and mobile certificates, and unique ID numbers are some examples.

Digital Identity: A collection of credentials and traits that are electronically recorded, saved, and can be used to uniquely identify an individual in a computer-based environment

Electronic Identification: A credential used to identify and authenticate a person in a digital setting is known as electronic identification. generally speaking, a smartcard with a contact or contactless chip.

Identification: is the process of figuring out one's identity and recognizing oneself, as well as the act of figuring out what something is, or the identification of something for what it is.

Identity System: Systems that register and identify people for a general or specific purpose, including databases, credentials, and the processes, procedures, and infrastructure to produce and manage them.

Unique Identity Number: An individual's lifelong unique identification by a number typically based on biometric identification that can be used to link identities between databases and systems in the public and private sectors (WBG), 2017).

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Brief History of Birth Registration

Long before Jesus was born, there were population counts. Beginning in the 1500s, birth-related information was entered into church registers in England. However, the Bureau of Census was not founded as a permanent organization to provide birth registration regions and a uniform registration system until the 1902 Act of Congress. Although real registration of these occurrences beginning in 1892, the first attempt to compile statistics on births in Nigeria began in 1863 with the adoption of Ordinance No. 21 at the Lagos Colony. In Nigeria, a unified system of birth and death registration was first consciously attempted in 1979. Decree (Now Act) No. 69 of 1992, "Births, Deaths, ETC (Compulsory) Registration," went into effect on December 1st 1992. The National Population Commission was given exclusive national registration authority under the law. The potential utility of the birth certificate has increased as birth registration has transitioned from paper to electronic, but problems with updating the electronic format and preserving quality data have persisted. Understanding the birth certificate's historical context will give you a better understanding of how it has been and will continue to be used as a key public health document influencing public health practices and laws. (Brumberg *et al.*, 2012a).

Birth registration is recognized as a fundamental right under both article 7 of the Convention on the Rights of the Child and article 24, paragraph 2, of the International Covenant on Civil and Political Rights (UNIEF, 2019). The ongoing, permanent, and global recording of a birth's occurrence and characteristics in accordance with statutory requirements within the

civil registry is known as birth registration. It creates a person's legal existence and builds the groundwork for defending their civil, political, economic, social, and cultural rights. (UNICEF, 2019) As such, it is a fundamental means of protecting the human rights of the individual.

There are three interconnected stages to the birth registration process. The civil registrars must be informed of the birth first and foremost. After being informed, civil registrars formally record the birth. The registration should contain the person's name, date of birth, and place of birth as well as, if practical, the names, ages, customary residences, and nationalities of both parents. Third, the state produces a birth certificate, a private document attesting to the kid's registration at birth and acting as the most overt indication of the state's legal recognition of the child. Country-specific laws govern the process for registering births and issuing birth certificates, but it's crucial that the record be readily available and delivered at no cost. Birth certificates are revised in every 10 years with about 12 revisions since 1900 (Brumberg *et al*., 2012a). Name, date of birth, place of birth, parents' names and ages, father's occupation and place of residence, prior births, names of witnesses and their addresses, occupations, and occasionally relationships were the main components of a birth certificate. The format used to collect the data was open-ended. The requirement for "Simplicity in phrasing beauty and convenience in arrangement, spacing, and print, however, was developing."(Plecker, 1915).

The process for putting data on paper stayed the same even while the nature of birth registration changed. This led to considerable reporting delays that were blamed on the paper birth registration medium, which reduced its usefulness. Thus, in California in 1980, the

electronic birth certificate was created (Brumberg et al., 2012b). The most recent iteration, from 2003, included variables that make it easier to track significant public health trends.

Table 2.1: Information contained in birth certificates over time (Brumberg *et al*., 2012a)

Important alterations in the birth certificate's data from the early 1900s to 2003	
Early 1900	• Information mostly on the time and place of birth, if there were multiple gestations, the mother's age and race, the validity of the father's name and age, and any previous live births
1949	• The birth weight and gestational age were included.
1968	• Using the last menstrual period (LMP) to date the pregnancy because neonatology was first practiced in the 1960s. • Inclusion of questions on prenatal care
1979	• Dropped the more judgmental term "legitimate" in favor of asking about the mother's marital status. Apgar scores were added, after 26 years Virginia Apgar developed the test to assess the health of newborn babies • The addition of abortions (both spontaneous and induced) coincided with the legalization of induced abortions in January 1973. (Roe Vs Wade)
1989	• Clinical estimation of gestational age, maternal health risks, if the mother and father are Hispanic, smoking and alcohol usage, delivery techniques and complications, and obstetrical procedures • The first use of checklists
2003	• More information on obesity (pre- and post-pregnancy weight and height), infertility (fertility treatments or ART), nutrition (usage of the WIC program, breastfeeding at discharge), and maternal morbidities associated to labor and delivery (by trimester) (such as transfusion and ruptured uterus)

2.2 Brief History of Blockchain Technology:

The idea of blockchain can be compared to the idea of value exchange, where people once exchanged goods face-to-face through barter and could see and confirm what they were receiving, such as your banana for my apple. The ability to see and feel the goods being traded confirmed the accuracy or integrity of the procedure. When people desired to exchange larger quantities of goods across greater distances, things became more difficult. It was impractical to verify the entire contents of a wagon or ship before to a trade since merchants could not always rely that the expected goods would arrive as promised. Parties were no longer able to ensure the integrity of the transaction in a practical manner. Intermediaries developed as a result to meet that requirement. They made a name for themselves as reliable middlemen who, in return for payment, would guarantee a transaction on behalf of the parties involved. This applied to all types of sensitive information transmission, not just economic transactions. The absence of trust came to represent the process's shortcomings and weaknesses. (Fuch, 2019). Then came Blockchain technology to eradicate the intermediaries and third-party system. Blockchain technology's impact on various areas, including the financial sector, industrialization, and education, is one of the greatest innovations of the twenty-first century. Figure 2.1 depicts that blockchain technology dates back to the early 1990s.

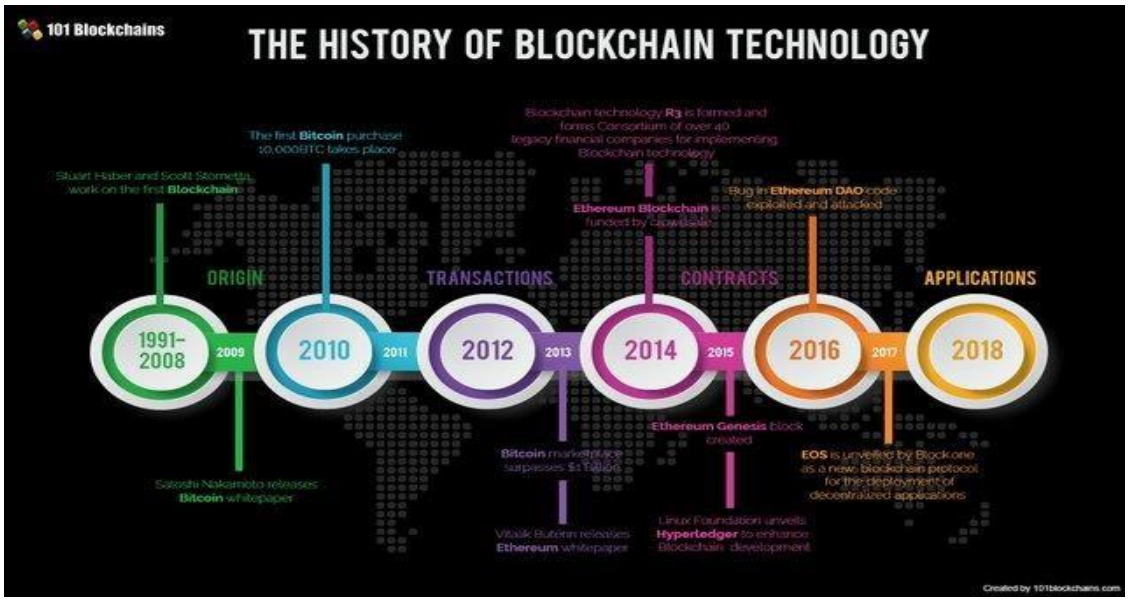

Figure 2.1: The History of Blockchain Technology (Gwyneth, 2020)

Blockchain, as introduced by Satoshi Nakamoto as a Bitcoin Cryptocurrency (Nakamoto, 2008), has gone beyond cryptocurrency. For the exchange of any service and transaction through a distributed network, it provides a reliable platform. As a result, it is expanding the scope of system security and effectiveness and transforming the current digital economy.

Blockchain has been referred to as "a method for storing and transmitting information that is transparent, safe, and runs without the use of a centralized control authority" since its inception as a collection of blocks used to store data. (Bodkhe *et al*., 2020).

With the introduction of the first of many contemporary cryptocurrencies, the Bitcoin network, this technology gained widespread recognition in 2009. The transfer of digital data that serves as electronic cash occurs in a distributed system like Bitcoin and comparable systems. Users of Bitcoin can digitally sign and transfer their ownership of that information to another user, and the Bitcoin blockchain publicly records this transfer, enabling all users of the network to independently confirm the transactions' legitimacy. A dispersed network

of people independently maintains and manages the Bitcoin blockchain. Because of this and cryptographic procedures, the blockchain is resistant to later attempts to change the ledger (modifying blocks or forging transactions). Bitcoin and Etheruem are only two examples of the numerous cryptocurrency systems that have been made possible by blockchain technology. As a result, blockchain technology is frequently seen as being tied to Bitcoin or even cryptocurrency products in general. However, a wider range of applications are possible with the technology, and it is being researched for a number of industries. (Yaga *et al*., 2018).

Many changes in data consumption, tight consumer relationships developed across social networks, smartphones, Internet of Things (IoT) analytics, and cloud platforms have been brought about by the shift toward digitalization. In order to provide better-informed judgments and improve the user experience, new models and architectures are being developed to modernize this combination of data and client expectations. A distributed system presents important issues for ensuring security fundamentals due to the enormous volume of data in networks. A person going by the name Satoshi Nakamoto enhanced the usability of digital currency in 2008. Although there are numerous possible uses for this technology, blockchain has been closely identified with digital or cryptocurrency because of Nakamoto's article (Nakamoto, 2008),. Government and business have investigated and tested supply chains, identity management, and recordkeeping over the past three years. blockchain has been closely associated with digital or cryptocurrency although there are many potential uses for this technology. Within the last three years, there have been explorations and pilots in government and industry for supply chains, identity management, and recordkeeping (Bhatia & Wright de Hernandez, 2019). Blockchain essentially creates a distributed append-only ledger where messages can be permanently recorded as its main

innovation. With potentially significant economic and political ramifications, this novel idea does away with the requirement to maintain central middlemen. With the widespread adoption of electronic ledgers as a method of record-keeping, blockchain technology began to quickly advance beyond its initial use in payment systems. As a general-purpose technology, it is currently being investigated by a burgeoning developer community and a thriving start-up ecosystem. (Allessie *et al*., 2019)

Blockchain is a distributed ledger system that has gained popularity; it is a type of ledger in which value-transfer transactions (in the form of cryptocurrencies, tokens, or information), are consecutively organized into blocks. Each block has a signature that is dependent on that block's exact content (a string of data). This signature is also seen in the next block, which connects all preceding blocks to the first. Blocks are immutably recorded throughout the peer-to-peer network using cryptographic trust and assurance algorithms.

In less than ten years from its advent in 2008, the concept of distributed ledgers has entered mainstream research and policy agendas. Growing experimentation with distributed ledgers and the emergence of the first operational implementations provide an opportunity to go beyond hype and speculation based on theoretical use cases (Allessie *et al*., 2019). The positive response, spurred by the success of Bitcoin and the explosion of potential use cases, has raised hopes for blockchain's revolutionary role in industry and government.

The revolution of blockchain technology from inception as seen in figure 2.2 has gone through various modifications known as generations from Blockchain 1.0 to 4.0 (Swan *et al*., 2015, Xu *et al*., 2017).

The first generation of technology began in 2009 with the launch of the bitcoin network, which saw the birth of the first cryptocurrency. Payments were at the center of the idea, and how they could be used to generate cryptocurrencies like bitcoin. As a result, Blockchain 1.0 provided a number of advantages over traditional payment mechanisms, including cheap transaction costs and transaction anonymity, hence eliminating counterfeiting by enabling secure, trackable, and transparent transactions, in addition to reducing double spending (Kumar Singh *et al*., 2021).

In 2010, the generation of blockchain technology was introduced, which comprised smart contracts and financial services for diverse applications. This generation advocated blockchain development using the Etheruem and Hyperledger frameworks. Hyperledger provides a modular and extendable architecture that may be used in a variety of industries, from banking and healthcare to supply chains, and Ethereum promotes itself as completely independent of any specific field of use (Buterin, 2013).

The third-generation blockchain converged towards decentralized applications and developing decentralized applications, various study topics including health, governance, IoT, supply chain, business, and smart city were studied. (Vora *et al.*, 2019). Etheruem, hyperledger, and other platforms were used, as they could code smart contracts for a variety of decentralized applications (Yu *et al*., 2018), (Palma *et al.*, 2019).

The fourth-generation mainly focuses on services such as public ledgers and distributed databases in real-time. This level has seamless integration of Industry 4.0-based applications. The current specifications of Industry 4.0 require an enterprise resource-planning platform that can provide automation and integration of different execution platforms as a single

coherent unit. It uses the smart contract which eliminates the need for paper-based contracts and regulates within the network by its consensus (Holland *et al.*, 2018).

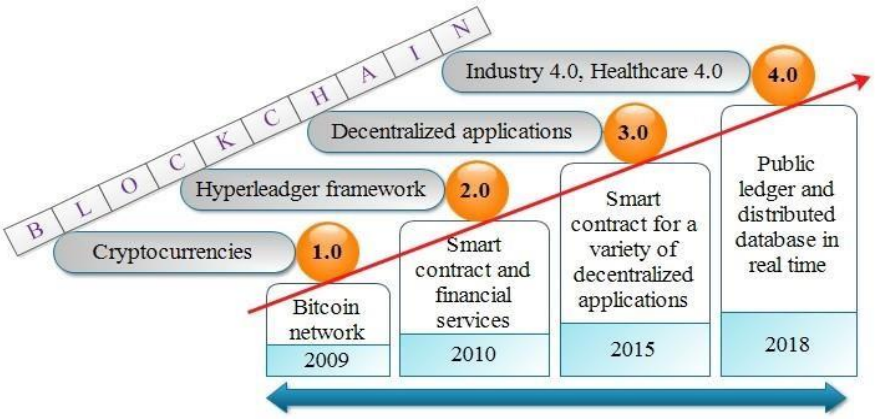

Figure 2.2: Blockchain generations (Bodkhe *et al.*, 2020)

2.3 Blockchain Technology Fundamentals

Blockchain is a type of distributed ledger technology that allows several parties in a database to share and reproduce information (Bhatia & Wright de Hernandez, 2019). The database is updated according to pre-determined rules, and it is then shared with all parties. These transactions are linked in a chain, ensuring that everyone has an exact copy of the ledger. Distributed ledger uses the system for replicating and storing transactional data on a blockchain network. The ledger expands on this idea by replicating data across multiple nodes. Blockchain eliminates the need for third-party services to validate transactions because it is a peer-to-peer network that timestamps them. This form of recordkeeping contains consensus or trust-based transactions and is tamper-resistant. “Blockchain” is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not necessarily have a pre-existing trust relationship (Crittenden, 2020).

The core components of the blockchain architecture are; Nodes, Transactions, Blocks, Chain, Miners, and Consensus.

A node is a user or a computer (each has an independent copy of the whole blockchain ledger). A transaction is the smallest building unit of a blockchain system (records, information, and so on) that serves the blockchain's purpose. Block contains a record of the most recent transactions whose content can be any type of activity can be tracked and each block consists of a block header and a block body. Miners are the dedicated nodes that execute block verification before adding anything to the blockchain structure. A Chain is a set of blocks that are arranged in a specified order. When the block reaches the maximum size, it is chained or linked by a hash. Consensus (consensus protocol) is a collection of rules and agreements that govern how blockchain transactions are carried out. The rules, such as limiting the size or number of transactions, are established when the network is first created.

A hash is an algorithm that generates a fixed-length value from a variable string of data (Bhatia & Wright de Hernandez, 2019). Inserting the hash value of one block into the next block links the new block with the preceding block. Repeating a hash function on an unaltered block of data will always generate the same fixed-length value. If a block of data is altered, the resulting hash output will be different. A different output indicates that the original block has been altered and may no longer be trustworthy. Multiple hash values can be brought together, and hashed, creating a single hash or a Merkle root. Additional hashes are added to the root thus creating a Merkle tree (Bhatia & Wright de Hernandez, 2019). Blockchain architecture facilitates increased trust and transparency by its very nature. In the sense of ethical principles, the system exemplifies a culture of cooperation and engagement

between stakeholders and one that demonstrably behaves as intended (Crittenden, 2020).Figure 2.3 shows the typical architecture of blockchain.

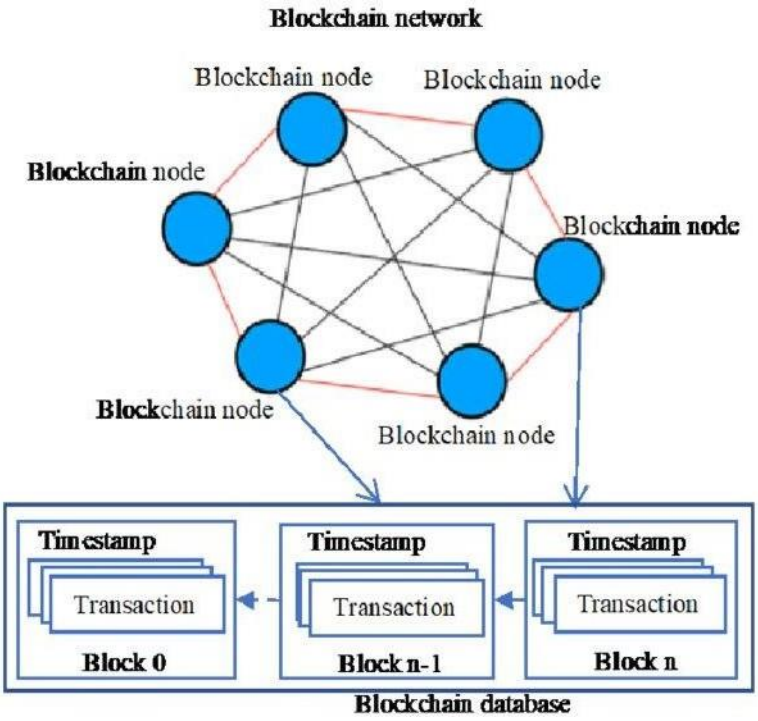

Figure 2.3: Blockchain Architecture (Salman *et al*., 2018)

Many sectors and businesses will be disrupted by blockchain technology as it has proved its robustness, immutability, auditability, in many crucial practical applications. The blockchain structure offers traceability of actions, alterations, alerts, which is an important property of a system needed for the development of sustainable technologies. A crucial part of blockchain technology regarding the optimization of the processes is the smart contract.

It is a self-executable computer code, open and transparent, encoding the terms of a regular contract. It can automate the processes, thus decreasing the human-factor mistakes or counterfeits. In this paper, we are presenting the feasibility of blockchain technology in the certification processes, with an application developed for birth certification. The example is

easily transferable in other areas and business models such as logistics, supply chain management, or other segments where certification is essential (Karamachoski *et al*., 2020).

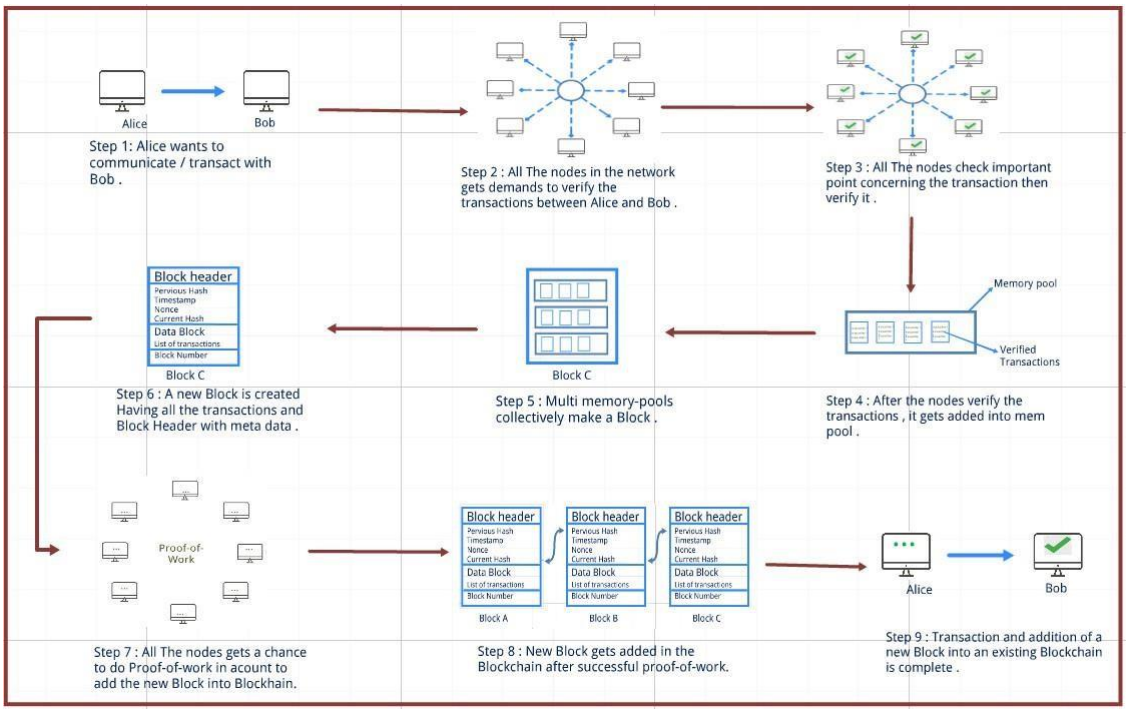

Figure 2. 4: How blockchain works: (Hamlaoui, 2019)

The first implementation of blockchain was on the Bitcoin protocol using main data structures as transactions and blocks recorded in an encrypted distributed ledger. There are two collections of transactions: one contains incomplete transactions, the second contains complete transactions but not included yet in the blocks of the main chain. Each block "aggregates a timestamped" collection of transactions to be inserted in the distributed ledger. New blocks created by mining, are validated through competition with a large computational effort, new transactions and append them to the main chain. Three categories of blocks there exists during Bitcoin transactions: blocks in the main chain containing encrypted confirmed transactions, blocks linked to the main chain but not included due to, and orphan blocks (not connected with blocks from the main chain). With exception of the orphan blocks, the first

two categories are included in a directed rooted tree with links towards the root (with a previous pointer). The rooted tree converges to the blockchain which, from technical point of view, is a back linked list of transactions built using hash pointers. A cryptographic signature identifies each block. A private/public key infrastructure is maintained by the network participating to BCT (Railean, 2017).

The Blockchain for cryptocurrencies like Bitcoin, Ethereum, and many others are designed in such a way there are guaranteed: (1) the transaction irreversibility (it is impossible to undo a transaction); (2) no Counterfeiting (it is impossible to increase the money supply at will); (3) no double spending (it is impossible to spend the same value more than once) (Railean, 2017).

Blockchain can be public, private or a hybrid, and the overall purpose of a blockchain will determine which is best. But the real value of blockchain technology is realized only when the widest possible number of users are able to access data, so if all participants in a network are truly "trusted," then blockchain may not be the best technology option. Most likely, that public blockchain will play an important role as the technology develops. For that to happen, technical and non-technical people will have to get comfortable with hashes and other references derived from their confidential data being placed on public blockchain (Fuch, 2019).

2.3.1 Ledgers

Throughout history, pen and paper ledgers have been used to keep track of the exchange of goods and services so a ledger is a collection of transactions. In modern times, ledgers have been stored digitally, often in large databases owned and operated by a centralized trusted

third party (i.e., the owner of the ledger) on behalf of a community of users. There is growing interest in exploring having distributed ownership of the ledger. Blockchain technology enables such an approach using both distributed ownership as well as a distributed physical architecture. The distributed physical architecture of blockchain networks often involve a much larger set of computers than is typical for centrally managed distributed physical architecture (Yaga *et al*., 2018).

2.3.2 Blocks

The structure of a block can be assumed to be divided into two sections, one comprising of the header with all metadata and the other consisting of all the transaction details. Figure 2.5 illustrates the structure of block. The first set of metadata consists of Previous Hash which is used to chain the current block with its preceding block in the blockchain. The second set of meta data comprises of the information pertaining to mining competitions such as Timestamp, Difficulty and Nonce. Mining in Blockchain is performed by high end computers that solve complex mathematical problems to receive rewards in return, thus completing the verification procedures (Kiayias *et al*., 2016). Timestamp gives the creation time details for a particular block thus eliminating the denial of service scenarios. Difficulty gives the complexity that was used to create this block. In cryptography, nonce is an arbitrary number that can be used only once in the entire communication. In Blockchain, nonce is the number that miners are competing for. Successfully mining means that the winning miner was the first to guess the nonce, which is a string of random numbers affixed to the hashed contents of the block, which is again rehashed. The final metadata includes the Merkle Tree root which a data structure to summarize all the transaction details in the corresponding block in an efficient manner.

In order to identify a block, users can either use the block hash or the block height. Block height is described as the number of blocks before it. Thus it can be calculated as the length of the block minus one. The block height of the entire blockchain is obtained from the height of the most recent block or the highest block in the chain.

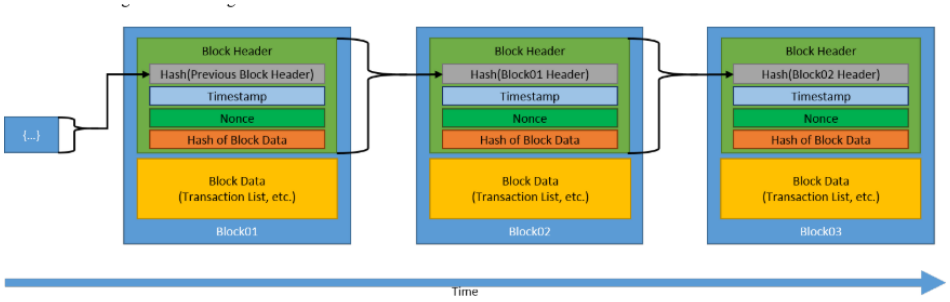

Figure 2. 5: Generic Chain of Blocks (Yaga *et al*., 2018)

2.3.3 Consensus

Blockchain is peer-to-peer network with no central manager or authority, however members of the network arrive at a consensus on the state of the ledger, the verification and order of records. Consensus mechanism is used to authenticate every single block and eventually used to achieve the required consensus and also, in the process remove invalid or contradictory transactions. The use of consensus algorithms is applied to ensure that the right order of transactions has been fixed and validated by due users to be added to the network (Du *et al*., 2017)

2.3.4 Consensus algorithms

Consensus algorithms are of the highest relevance to blockchain technology since the purpose of Bitcoin was to transfer value in an unregulated, distrusting environment, where a sure way of validating transactions was needed. The goal of the consensus algorithm is to

ensure a single history of transactions exists and that that history does not contain invalid or contradictory transactions. For example, that no account is attempting to spend more than the account contains, or to spend the same token twice, so-called double-spending (Bergquist, 2017). A token is a digital item that symbolizes permission to do a specific function or a physical item of value. (Allessie *et al.*, 2019).

Bitcoin solved the consensus problem by, for each new block announcing a target, which the hash of the previous block, the current block and a variable nonce has to equal less than. Since the output of the hashing function is evenly distributed, it's impossible to create a block such that it with certainty will be easy to reach the target. Therefore, there is a race between the mining computers in the network to find the right nonce. Once a target is reached, the mining computer broadcasts that block to the network and other participants validate the transactions. If enough validating nodes find the transactions to add up, they agree upon that block being added to the chain. This procedure is called proof-of-work (PoW)

2.3.5 Proof of Work

Participants, as miners, are required to include transactions within one block and then compute a hash function depending on some additional parameters) (Railean, 2017).

Since the goal is, not to give too much power to a single person or organization, a limited resource has to be chosen which will be spent upon voting for the validity of a block. In PoW, the resource is computing power (Bergquist, 2017).

2.3.6 Proof of Stake

Participants, as validators, must own some stake in the network, and "the creator of a new block is chosen in a deterministic way", depending on its wealth/stake (Railean, 2017).The

Proof of Stake (PoS) model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it. Stake is often an amount of cryptocurrency that the blockchain network user has invested into the system (through various means, such as by locking it via a special transaction type, or by sending it to a specific address, or holding it within special wallet software). Once staked, the cryptocurrency is generally no longer able to be spent. Proof of stake blockchain networks use the amount of stake a user has as a determining factor for publishing new blocks. Thus, the likelihood of a blockchain network user publishing a new block is tied to the ratio of their stake to the overall blockchain network amount of staked cryptocurrency (Yaga *et al.*, 2018).

In comparison, PoS is an energy-saving alternative to PoW. Miners in PoS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. Many blockchain adopt PoW at the beginning and transform to PoS gradually. For instance, Ethereum is planning to move from Ethash (a kind of PoW) to Casper (a kind of PoS) (Zheng *et al*., 2017).

2.3.7 Smart Contracts

An attractive attribute of blockchain technology is smart contracts. A smart contract runs on the top of the blockchain. Smart contracts help us exchange money, property, shares, or anything of value in a transparent way getting rid of intermediary services. Smart Contracts makes whole process super-efficient, eliminating expensive and time-consuming middle party. There are seven reasons why smart contracts is more useful: autonomy, trust, backups,

speed, saves money, accuracy. We can use smart contracts for all sort of situations that range from financial derivatives to insurance premiums, breach contracts, property law, credit enforcement, financial services, legal processes, crowd-funding agreements and so on. Smart contracts use the concept of gas to control the consumption of resources. Smart Contracts are written in a Solidity programming language. Solidity syntax is similar to JavaScript language, which supports inheritance, libraries and complex user-defined types. Solidity is a high-level language used for creation of smart contracts. The Solidity integration of C++, Python and JavaScript languages and it targets the Ethereum Virtual Machine (EVM). Smart contracts are, in the context of blockchain, simply logic that is published on a blockchain, can receive or perform transactions like any address (transactions may be rejected or require special arguments to function) and that can act as an immutable agreement. The purpose of the smart contracts is to act as a "computerized transaction protocol that executes terms of a contract" (Bergquist, 2017) and was first coined by cryptographer Nick Szabo. The basic idea, and the source of the contract-part in the name, is that certain parts of contracts can be included in software in such a way that the breach of them is either expensive or impossible. Smart contracts are often confused with Ricardian contracts, which is the digital recording and connection to other systems of a contract at law. This is not what is meant by smart contracts, since they do not need to be legal in any way, nor connected to outside systems. One could however, imagine value in the connection of smart contracts with Ricardian ones to "outsource" functionality of legal contracts to smart contracts (Bergquist, 2017). Smart contracts are digital contracts allowing terms contingent on decentralized consensus that are tamper-proof and typically self-enforcing through automated execution (Cong & He, 2019).

Smart contracts are contracts which are automatically enforced by computer protocols. Using blockchain technology it has become much easier to register, verify and execute Smart Contracts. Open source companies like Ethereum and Corda are enabling Smart Contracts using blockchain technology. Many companies which operate on bitcoin and blockchain technologies are supporting Smart Contracts. Many cases where assets are transferred only on meeting certain conditions which require Lawyers to create a contract and Banks to provide Escrow service can be replaced by Smart Contracts (Crosby *et al*., 2016).

Smart contracts as logic-based computer programs have a limited level of interactivity and do not allow people to negotiate and make changes based on the later agreed modifications like in traditional contracts, and they are not flexible with exceptions such as glitches. Also, due to the P2P nature of blockchain, letting ordinary users control their data directly is risky, and the exchange rate can be unpredictable when crypto-currencies are involved (Hu *et al*., 2018).

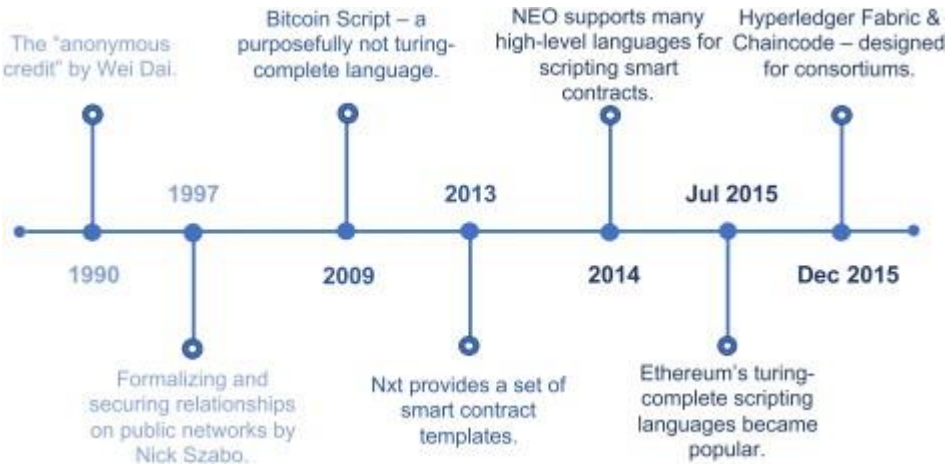

Figure 2. 6: History of Smart contract (Hu *et al*., 2018)

The smart contract was conceived by Nick Szabo in a paper “formalizing and securing relationships on public networks. He explained that cryptographic protocols could make it possible to write computer software that resembled contractual clauses and would narrow opportunities to terminate its performance obligations. In the following years, computer based contractual languages has been studied by scholars (Philippe, 2012).

Smart contracts can be used to replicate and improve on existing organizational mechanisms Efficiencies, transparencies, and accountabilities in contractual engagements (Fabian, 2018).

Smart contracts are gaining an increasing popularity in both public and private domains as they enable peer-to-peer operation on public blockchain and have the potential to improve efficiency and transparency in business collaborations (Hu *et al*., 2018). They are a set of instructions that validates data of one or more attributes value based on predefined conditions. There can be single or multiple smart contracts in a system. A system administrator who decides the attributes that needs to be verified creates the smart contract. Assume that there are t attributes in a record, and only r attributes ($r \leq t$) needs to be verified. Then a smart contract is created that receives r attributes as a transaction and validated. The set SC of smart contracts can be denoted as SC = {sc1, sc2, . . . , sc_w}, where w is the number of smart contracts (Rahman *et al.*, 2019).

2.4 Types of Blockchain

Blockchain is categorized on the basis of their applications. Primarily the two broad types of Blockchain are Public and Private Blockchain. Two variation also exist like the Consortium and Hybrid Blockchain. Figure 2.7 illustrates the types of Blockchain in a nutshell.

2.4.1 Public Blockchain

A public blockchain is open access that means it does not require any permission. It is free for everyone to join the network, read, write or participate within the blockchain. It is a decentralized blockchain that does not have any single entity to control the network. Once the data on the blockchain is validated, it is not possible to modify or alter the data and therefore, the public blockchain are considered as secured. Bitcoin and Ethereum are well-known examples of a public blockchain (Bele & Mehare, 2021).

2.4.2 Private Blockchain

Private Blockchain in contrast to the public blockchain, requires a permission it is restrictive, centralized, permissioned and operate only in closed networks such as any organization where only selected members are allowed to participate (Kumar Singh *et al*., 2021). This means that a private blockchain work will be based on the access controls which can restrict the number and type of people who would like to participate in the given network. The contents of the blockchain are only available to the permitted participants and any update or modification into the blockchain also necessitates the permission of the authority. In a private blockchain, only the entities participating in a transaction will have knowledge about it, whereas the others will not be able to access it. They are thus more secured and controlled than Public Blockchain and are commonly deployed in e-voting, supply chain management etc. Hyperledger Fabric of Linux Foundation is one of the perfect examples of a private blockchain (Bele & Mehare, 2021) and R3 Corda are popular examples of a Private Blockchain.

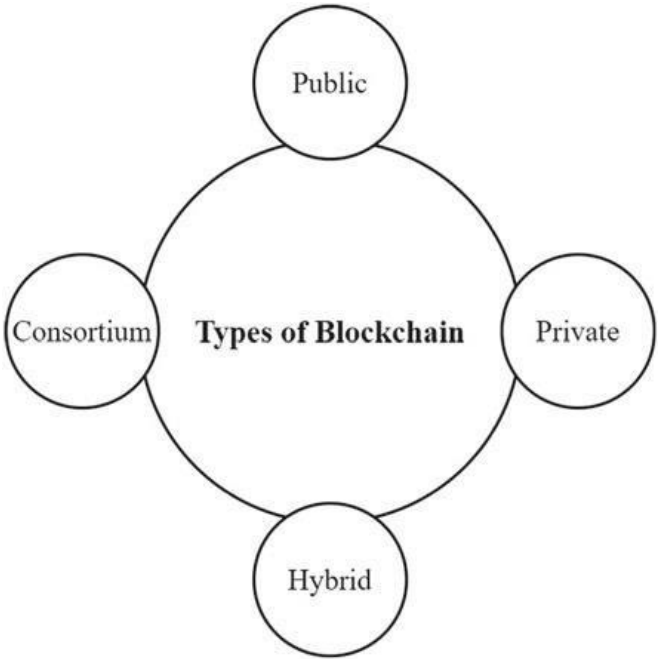

Figure 2.7: Types of Blockchain (Kumar Singh *et al*., 2021)

2.4.3 Consortium Blockchain

Consortium Blockchain is a specialized category of Private Blockchain Where multiple organizations control and manage the blockchain instead of only one (Darya, 2019) Thus it has the similar benefits as that of a Private Blockchain. Since it is a collaborative network, it is more productive and efficient both collectively as well as individually. Consortium blockchain is typically used by banks, government organizations, etc. Examples of consortium blockchain are; Energy Web Foundation, R3, etc.

Hybrid Blockchain is a combination of Public and Private Blockchain. It incorporates the privacy and permissioned facilities of Private Blockchain and the simplicity, flexibility and transparency of Public Blockchain. Participants of a Hybrid Blockchain can control the authority and accessibility of the data stored in it. (Kumar Singh *et al.*, 2021)

2.5 Cryptography and Blockchain

Encryption is a method of concealing a message content using mathematical rules, hence preventing unauthorized parties or the public from having access for the sake of information security (Hamlaoui, 2020). In the blockchain, cryptography is used to achieve the following two goals; secure the identity of the sender of the transactions and ensure that previous records cannot be tampered with. Blockchain uses cryptography on many levels; data security, information security in which the data cannot be tampered with while on transit not a key to rewriting it. The data maintains its integrity throughout transit and whereas being held on. Blockchain Cryptography additionally aids in non-repudiation. This implies that the sender and also the delivery of a message is verified, including confidentiality and privacy (Ritik *et al.*,2019).

The commonly used blockchain cryptographic technologies are symmetric-key cryptography, asymmetric (public-key) cryptography, and hash (Ritik *et al.*,2019).

2.5.1 Asymmetric (Public Key) Cryptography

This encryption method uses a pair of keys, an encryption key named public key, and a decryption key named private key. The key pair generated by this algorithm consists of a private key and a unique public key that is generated using the same algorithm. Blockchain technology uses asymmetric-key cryptography (also referred to as public key cryptography). Asymmetric-key cryptography uses a pair of keys: a public key and a private key that are mathematically related to each other. The public key is made public without reducing the security of the process, but the private key must remain secret if the data is to retain its cryptographic protection. Even though there is a relationship between the two keys, the private key cannot efficiently be determined based on knowledge of the public key. One can

encrypt with a private key and then decrypt with the public key. Alternately, one can encrypt with a public key and then decrypt with a private key.

Asymmetric-key cryptography enables a trust relationship between users who do not know or trust one another, by providing a mechanism to verify the integrity and authenticity of transactions while at the same time allowing transactions to remain public. To do this, the transactions are 'digitally signed'. This means that a private key is used to encrypt a transaction such that anyone with the public key can decrypt it. Since the public key is freely available, encrypting the transaction with the private key proves that the signer of the transaction has access to the private key. Alternately, one can encrypt data with a user's public key such that only users with access to the private key can decrypt it. A drawback is that asymmetric-key cryptography is often slow to compute.

2.5.2 Symmetric-key Cryptography

Both the sender and the receiver share a single key. This shared key is used for both encryption, which the sender uses to write plain text and send the encrypted text to the recipient as well as the recipient uses an equal key to decrypt the message and recover the plain text. This contrasts with asymmetric-key cryptography in which a single secret key is used to both encrypt and decrypt. With symmetric-key, cryptography users must already have a trust relationship established with one another to exchange the pre-shared key. In a symmetric system, any encrypted data that can be decrypted with the pre-shared key confirms it was sent by another user with access to the pre-shared key; no user without access to the pre-shared key will be able to view the decrypted data. Compared to asymmetric-key cryptography, symmetric-key cryptography is very fast to compute. Because of this, when one claims to be encrypting something using asymmetric-key cryptography, oftentimes the

data is encrypted with symmetric- key cryptography and then the symmetric-key is encrypted using asymmetric-key cryptography. This 'trick' can greatly speed up asymmetric-key cryptography (Yaga *et al.*, 2018).

2.6 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is one of the mechanisms to manage the keys in the public key cryptographic systems. Blockchain also utilizes the services of third party through PKI to authenticate the nodes of the Blockchain network. However, minimizing the dependency on third party by using the efficient key management is still a big challenge in the field of Blockchain (Pal *et al*., 2021). An emerging approach for PKI is to use the blockchain technology commonly associated with modern cryptocurrency. Since blockchain technology aims to provide a distributed and unalterable ledger of information, it has qualities considered suitable for the storage and management of public keys. While blockchain technology can approximate the proof of work often underpinning users' confidence in a PKI, it does not conclusively address issues such as administrative conformance to policy, operational security and software implementation quality (Dharwadker & Mills, 2019). These issues are associated with any certificate authority paradigm regardless of the underlying cryptographic methods and algorithms employed. A PKI that seeks to endow certificates with trustworthy properties is also expected to address these issues.

Current blockchain technology has its own restrictions, such as a low throughput, that cause potentially long response times and high transaction fees (Dharwadker & Mills, 2019).

2.7 Blockchain and Cryptocurrency

The first practical application using blockchain technology is Bitcoin, which is one of the highest valuable cryptocurrencies (Nakamoto, 2008). Bitcoin's value has been grown thousands of times since the appearance of the coin, and this is the main reason to explain the popularity of blockchain today (Nguyen *et al*., 2020).

2.7.1 Bitcoins the First Blockchain

Blockchain technology stems from the seminal white paper, (Nakamoto, 2008), outlining how the cryptocurrency Bitcoin could be constructed. Bitcoin solved a very important problem in the field of electronic money called double-spending, i.e. using the same electronic coin to pay for multiple things. Normally this is solved through a central authority, such as a bank or another trusted third party but Nakamoto proposed a time-stamp server, which ensures all transactions are appearing chronologically in the database (Bergquist, 2017).

2.7.2 Transactions in Bitcoin

The most basic component of a blockchain is a transaction. It may represent an exchange of something valuable (literally, a "transaction") or it may be a hash file representing something as simple as a single word or as complex as a software program. Whatever it is, the submitting party digitally signs it, and when it's received by the network, it's time-stamped (Fuch, 2019).

A transaction represents an interaction between parties. With cryptocurrencies, for example, a transaction represents a transfer of the cryptocurrency between blockchain network users.

For business-to-business scenarios, a transaction could be a way of recording activities occurring on digital or physical assets (Yaga *et al.*, 2018).

2.7.3 Post Bitcoin

Some properties of Bitcoin have been abstracted and rebuilt into what is called blockchain technology or distributed ledger technology. While still maintaining the main properties of Bitcoin, new blockchain are often more flexible in their applications and what actions they allow (Giudici *et al.,* 2020) It is a technology very much under development where new approaches and applications are being published frequently, most often through white papers published by start-ups or a group of corporate researchers. The basics of blockchain remain the same; it is a distributed, time-stamped database with consensus-establishing peers. Blockchain technology is characterized by the following traits:

Distributed: Nodes are considered equal in the sense that they all have a full copy of the entire history of the database. There can also be less equal nodes, also called lightweight nodes, which only have a couple of the last blocks stored locally. Generally, communication between nodes is done over the Internet with private-key cryptography

Time-stamped: Since every block of transactions is hashed into all the subsequent blocks, it becomes increasingly difficult to change history the further away in time the current block is. The blockchain at hand becomes a provably correct auditing tool.

Consensus: Nodes establish one truth about which version of the database is the correct one through a consensus-algorithm. This serves to validate transactions as well as to discourage for example double-spending attacks. The type of consensus-algorithm used is highly dependent on the structure and purpose of the blockchain.

2.8 Certificates and Blockchain

Certificates are important when applying for job whether at public or private sector. It is usually produced in hard copies and difficult to keep it safe. Certificates that have been issued need to be verify manually which is very time consuming and financially expensive, therefore the efficiency of the system can be increased by the digital certificate verification based on block chain technology (Bele & Mehare, 2021).

Certificates play an important role in education and in professional development in companies. Individual learning records become essential for people's professional careers. It is therefore important that these records are stored in long- term available and tamper-proof ledgers. A blockchain records transactions in a verifiable and permanent way, therefore it is very suitable to store fingerprints of certificates or other educational items. Blockchain reveals forgery of certificates and it supports learning histories.

(Grather *et al.*, 2018) Blockchain for Education platform presents as a practical solution for issuing, validating and sharing of certificates

2.8.1 Certificate Management

Certifiers can create, revoke and delete references to certificates stored in the Blockchain for Education platform. This is implemented in the smart contract CertMgmt (Grather *et al.,* 2018). The accreditation authority instantiates the CertMgmt contract together with the IdentityMgmt contract. The CertMgmt contract requires the address of the IdentityMgmt contract to enforce access control. Any manipulative operation on the CertMgmt contract, such as adding a certificate, requires that the caller is a registered certifier of an accredited

certification authority. Everyone can retrieve certificate records given the address of the CertMgmt contract and a hash of the certificate (Grather *et al.*, 2018).

The CertMgmt contract uses certificate records to store certificate information in the blockchain. Currently, this information consists of the SHA256 hash of the certificate, the starting and expiration date and a status field (on Hold) to indicate if a certificate is on hold. Dates represented as UNIX timestamps and for future proofing, are stored as 256- bit unsigned integers. Similarly, the on Hold status field stores a UNIX timestamp if a certificate is on hold. Thus, one can check when the on Hold status was set for a certificate (Grather *et al.*, 2018).

2.8.2 Digital Certificates

Digital certificates offer a process and steps to authenticate and secure internet transactions on open and closed networks. Digital certificates are used in securing emails, internet and mobile banking transaction, smart card authentication, file transfers and signing of digital software files. Digital certificate operates the way E-passport works. Passports are issued by countries to their citizen while certificate authorities issue digital certificate. The passport provides the way to verify your identity as the real owner and gain entry to your destination. Likewise, Digital certificates provide similar identification within the electronic world. The role of the certificate authority is to validate the certificate holder's identity and to sign the certificate in order that it cannot be tampered with. Once a certificate authority has signed a certificate, the holder will pass their certificate to others, websites and network resources to prove their identity and establish encrypted, confidential communications. Public Key Infrastructure or PKI technology is part of Digital Certificates described as virtual ID cards (Abubakar *et al.*, 2016).

2.9 Health Care and Blockchain

Generally, a healthcare blockchain is treated as a distributed ledger to store health records for sharing, exchanging or other purposes among stakeholders. In e-Health systems, data can be generated from different sources such as clinics, hospitals, and pathologies. In a blockchain-based Electronic Health Record (EHR) management system, all the data related to patients are stored in the distributed ledger offered by a blockchain network. The process of storing a set of related data is known as a transaction. Each transaction is evaluated by a group of participants, known as miners, before being stored in the distributed ledger (Dubovitskaya *et al*., 2020). Blockchain networks are capable of rejecting an unauthorized transaction which try to modify the data in the distributed ledger. As a result, no unauthorized person can modify the data in a blockchain network. A key concept of blockchain, smart contract, empowers trustless features among different entities in the EHR management system. A smart contract involves a computer program that contains a set of agreements and principles. All of the participants in the network must follow the set of agreements and principles. Hence, no trusted third party is required to store data in the blockchain (Rahman *et al.*, 2019)

2.9.1 Birth certificate and Blockchain technology

Birth certificates are the cornerstone for establishing legal identity around the world. Despite their importance, birth certificates are frequently simple, handwritten paper documents or computerized printouts, submitted with little attention to security. The birth certificate issuance process is often decentralized, potentially leading to different formats within the same country. These features make birth certificates relatively easy to forge and difficult to authenticate (Dharwadker & Mills, 2019).

In Nigeria birth certificate is a document that contains the date of birth, location (Town, Local Government Area (L.G.A), and state) of birth and details of the parents. It is issued by the National Population Commission for every child and is usually issued at the hospital where the child is born and it is compulsory for everyone. The National Population Commission (NPC) formed in 1992, is the only body responsible for registering every newborn and issuing certificates in the country (Makinde *et al*., 2016).

A person who did not get a birth certificate at birth can later apply as long as they are below 18. However, only people between age 18 and below are issued a birth certificate. People above age 18 are issued 'Age Declaration Affidavit'. Although now in Nigeria, you will have to provide an attestation letter issued by the NPC as the 'Age Declaration Affidavit' is not a sufficient document as it used to be years ago.

An attestation letter is a written document given as backup for the 'Age Declaration Affidavit'. However, in terms of legal value and effect, the attestation of a birth certificate is equal to a birth certificate. The NPC Act states that only people born after 1992 are eligible to apply for birth certificate as that was when the NPC was formed. Also, only birth certificate issued at birth or 60 days after birth is free any scenario after birth would require you to pay (Maduekwe *et al*., 2017).

Blockchain technology is decentralized data storage structure, capable to operate in trustless community, to track and record modifications and to reduce the need of third parties. Moreover, the blockchain database structure, also known as the distributed ledger, offers liveness, immutability, redundancy and non-repudiation of the records (Karamachoski *et al.*, 2020).

The records in the blockchain database are organized in blocks, where the blocks are generated in predefined time intervals. All the information generated in one blockchain network is stored in every participating node, thus creating a complete copy of the common database of the system, in every participating node. This property makes the database structure redundant, reliable and very robust

In many countries, applying for a passport requires the submission of a birth certificate, a process that can be inefficient, and at the same time may not enable the full authentication of individuals. A similar situation may exist in other circumstances, for instance, when applying for school or university admission, driver's licenses, marriage and separation certificates, and welfare benefits; enrolling for health care or health insurance; or registering to vote. One way to solve this problem is to make the birth certificate a highly secure document (like a banknote or passport), with personalization and issuance completed under highly secure conditions as some countries are using Digital Birth Certificate (DBC) (Dharwadker & Mills, 2019).

The birth certificate as a digital credential has become relevant in the context of Sustainable Development Goal. "By 2030, provide legal identity for all, including birth registration." Given the increasing digitization of state records and processes, as well as greater connectivity among departments, a DBC, if issued in a secure manner, can enable more timely processing and a greater level of authentication. In addition to having the capacity and administrative processes in place to manage DBCs, countries require a corresponding legal framework to recognize DBCs (Dharwadker & Mills, 2019).

.

2.10 Need to combine multiple systems to create the technology birth certificate

The certification procedures are part of our everyday life. A certificate is a verification of existence or possession of declared characteristics or acquired competences. In most cases the certificate is issued by an institution and handed in paper form to the holder. These bureaucratic procedures are time consuming, expensive and leave plenty of opportunities to issue fake documents. The advancement of technology offers a plethora of tools to the scammers to falsify the paper certificates, hence having a technology that offers protection against these malicious activities is quite beneficial (Karamachoski *et al.*, 2020).

2.10.1 National Identification Number (NIN)

According to section 14 of the National Identity Management Commission (NIMC) Act 2007 any person in respect of whom an entry is made in the National Identity Database (NIDB) is to be identified using unique and unambiguous features, including the biometrics. The generation and use of a unique identification number derives from this provision.

The NIN is a non-intelligent set of numbers randomly generated by which a registered person will be identified for life and once used can never be used again even after the person to whom it was originally assigned is dead. By the provisions of Section 18 of the NIMC Act mandatory registration of citizens aged sixteen years and above and Section 27 (mandatory use of the NIN in specified transactions), the harmonization process would be further enhanced.

The enrollment process which is initiated by the citizen appearing at the designated location as provided for in Section 18 of the NIMC Act, (provide demographic data and permit his/her biometrics to be taken), would ensure that personal information is collected in a manner

consistent with the harmonization objectives and thus reduce the need for such activities to be repeated by other stakeholders.

The National Identity Management System (NIMS) combines a National Identity Database (also known as a Central Identity Repository or Register (CIDR), a chip-based, secure identity card, and a network of access and means to irrefutably prove or assert the identity of an individual. The most important thing about the NIMS is that it will provide a Universal Identification Infrastructure for the entire country. This will help bring real and recognizable benefits to the Government, each of us - individually and collectively, and for legal residents in Nigeria.

The proposed national identity database, a key component of the ongoing implementation of the NIMC, will serve as a central source of identity data to be used in identity verification and authentication, and will be connected to various other final draft public exposure identity database in key institutions in Nigeria through the unique National Identification Number (NIN). It will also enable the streamlining of various registration and enrollment activities (standardize, eliminate duplication).

The national policy direction is to establish harmonized and seamlessly integrated final draft public exposure NIMS which is anchored on the unique NIN, and which connects the various institutional databases under a single platform (Yusuf *et al.*, 2011).

2.10.2 Document verification

Document verification is a complex domain that involves various challenging and tedious processes to authenticate. Moreover, various types of documents for instance banking documents, government documents, transaction documents, educational certificates etc.

might involve customized verification and authentication practices. The content for each type vary significantly, hence requires to be dealt in a distinct manner (Saleh *et al.*, 2020).

Certificates confirm the achievement of certain learning outcomes. Until today, certificates are usually issued on paper, which has several advantages. For example, recipients can easily store them and present them to any person and for any purpose. In addition, it is difficult to forge paper certificates if there are built- in security features. However, third parties need extra effort to verify paper certificates. Verification is usually achieved by asking the issuing certification authority, that is certification authorities have to maintain a long-term archive (Nauwerck & Forssell, 2018).

Blockchain technology is forecast to disrupt any field of activity that is founded on time-stamped record-keeping of titles of ownership. Within education, activities likely to be disrupted by blockchain technology include the award of qualifications, licensing and accreditation, management of student records, intellectual property management and payments (Srivastava *et al.*, 2019).

2.11 Review of Related Works

2.11.1 Blockchain and Document verification

Certification procedures are part of our everyday life. A certificate is a verification of existence or possession of declared characteristics or acquired competences. In most cases, the certificate is issued by an institution and handed in paper form to the holder. These bureaucratic procedures are time consuming, expensive and leave plenty of opportunities to issue fake documents. The advancement of technology offers a plethora of tools to the scammers to falsify the paper certificates, hence having a technology that offers protection against these malicious activities is quite beneficial (Karamachoski *et al.*, 2020).

In the last ten to fifteen years, the production of forged academic certificates has become a global problem as educational qualifications have gained increasing commercial value. The rising number of fake diplomas is common because of the crisis, where desperate people forge certificates in order to obtain job qualifications. However, recent research shows that the counterfeiting of diplomas involves not only lower-tier staff but also activists, members of the Government, officials, and university candidates. As a recent review has shown, transcript issuance administration and management face many adversities. In its physical form, a transcript is easily manipulated and hardly verifiable. When digitized, transcripts are still shared with difficulty between institutions or employer platforms while being highly exposed to security vulnerabilities. From a financial aspect, these issues can result in high costs and offer minimal rewards for those attempting to address them (Caldarelli & Ellul, 2021).

2.11.2 Other Related Works

The process of birth registration and verification is critical for tracking population growth and health outcomes, yet it remains a challenge in many parts of the world. In recent years, several research innovations have been proposed to improve the accuracy, efficiency, and accessibility of birth registration and verification systems. A review of research papers that highlight some of these innovations and their contributions and drawbacks.

Hanson *et al.*, (2018) explored the use of mobile technology for community health in Ghana, which can facilitate remote and cost-effective birth registration, especially in low- and middle-income countries (LMICs) where registration rates are low due to geographic and financial barriers. However, the authors note that lack of access to mobile technology and the need for robust data privacy and security measures are significant challenges.

The use fingerprints biometric based national birth registration system to ensure accurate and proper births estimation for sustainable national development planning in Nigeria using PHP programming language with JavaScript, Minitiae-based Fingerprint Matching Algorithm, and MYSQL database system was proposed by (Gabriel *et al*., 2022), however the system is a centralized database which may be prone to attack.

Aronoff-Spencer *et al.,* (2019) approach to infant registration and identification using non-contact optical imaging of fingerprints using detailed technology development history, including Human-Centered Design methods, various iterations of our platform. However, Other biometric identification modes besides fingers, especially iris scanning, are technically possible but fail due to infant behaviors (e.g. closed eyes), confounders (e.g. eye infection, trauma or irritation), or social factors (e.g. certain parents/certain cultures do not tolerate scanning of infant faces). Ears remain a promising secondary biometric in many settings and may improve over time.

Kuo *et al*., (2022) proposed a blockchain-based birth registration system, which offers a decentralized and tamper-proof way of registering births, improving security, accuracy, and accessibility. However, the authors also highlight several challenges, such as the lack of standardization, technical expertise, and infrastructure, as well as potential privacy and ethical concerns.

Certification procedures being an integral component of our daily lives, verifies the existence or possession of specified characteristics or acquired skills. In most circumstances, the bureaucratic procedures for producing a certificate by an institution and handing it out in print form to the bearer are time-consuming, costly, and offer a lot of room for fraudulent documents to be issued. Scammers now have a plethora of tools to fabricate

paper certificates thanks to technological advancements, thus having technology that protects against these nefarious acts is extremely important.

Various ways to secure certificates have been offered, however, they have all been found to be problematic. The signature is used to authenticate the document, which is in the form of a paper, and the authentication is provided by the certificate. However, forgery is achievable due to current document printing and scanning technologies. (Raghav *et al.*, 2019).

In their article "Certificate Verification Using Blockchain and Transcript Generation," (Lamkoti *et al*., 2021) stated, "To overcome this disadvantage, a technology known as blockchain enters our lives as a rescuer." Institutions, students, and service providers were the three actors in the plan all actors used a single hash as a key, making it publicly available once they know the hash. This is a flaw in their approach.

Many security solutions and standards have been proposed over the years to improve the security levels of the aforementioned smart applications, but the existing solutions are either based on centralized architecture (having a single point of failure) or have high computation and communication costs, which drives home the point (Bodkhe *et al*., 2020). Furthermore, most existing security solutions have only addressed a few areas of security and do not address scalability, robustness, data storage, network latency, auditability, immutability, or traceability. Blockchain technology could be one of the solutions to the aforementioned problems. (Bodkhe *et al.*, 2020, Zhang *et al*., 2018).

Using the system analysis and design (SAD) methodology, (Oliha *et al*., 2019) created an electronic system for birth registration and record management, which required the use of

several clients and server-side development tools, including Hypertext Markup Language (HTML), JavaScript, and Cascading Style Sheet (CSS), Hypertext Pre-Processor (PHP), and My Structured Query Language (MySQL). As a result, the model was thoroughly tested and evaluated, demonstrating its ability to record births, maintain registers, and test the issues associated with record storage, such as verification, retrieval, and duplications. However, the user interfaces for birth registration and birth certificate preparation for various accredited institutions were not user-friendly.

The system designed by (Shah & Kumar, 2019) was explicitly for Birth Certificates and similar to (Lamkoti *et al*., 2021) design but runs the AES algorithm and stores the data in the Interplanetary File System (IPFS). In 2019, (Shah & Kumar, 2019) introduced a system designed for effective innovation to store birth records that cannot be tampered with, easy to maintain, reliable, and can be successfully shared. These techniques are also utilized to replace the verification methods of passwords, pins, smartcards, keys, and tokens. This system is implemented on a local blockchain network using public and private keys and the RSA algorithm is used for user login and registrations. Its drawback is seen, as the original document was not stored anywhere nor does it have the functionality to generate the certificates online.

Young *et al*., (2018) blockchain, parents or legal guardian manage digital identity till child turns eighteen hence leading to multiple consent openings to access information making it complex for use for users.

For a blockchain based tamper proof Electronic Health Record (EHR) management system, (Rahman *et al.*, 2019) used a wrapper layer integration mechanism, named as the blockchain hand shaker, between the existing cloud based EHR management system and public

blockchain network to develop a tamper-proof health record management system but cross domain diversities was not considered.

Certificate verification on the blockchain by (Saleh *et al*., 2020) made use of blockchain technology for just verification of certificates alone and not for the creation of certificates.

Hewa *et al.*, (2021), smart contracts were applied for blockchain based applications and the challenge discovered was that smart contracts alone do not necessarily guarantee privacy. In particular, they do not guarantee unlink ability, which is crucial not only for privacy but also for fungibility.

(Grather *et al*., 2018) Blockchain for Education platform was based on the Ethereum blockchain. Two smart contracts written in Solidity codify access control mechanisms (IdentityMgmt) and manage certificate records (CertMgmt) stored in the blockchain. The Interplanetary File system (IPFS) is used as a public distributed read-only storage for profile information of certification authorities. The BSCW (a web based group ware document management system stores and validate certificate. The system runs on the Ethereum blockchain, it introduces monetary overhead

Table 2.2: Review of Related Works

S/N	AUTHOR(S)	TITLE	YEAR	METHODOLOGY	CONTRIBUTION	DRAWBACK
1	Young, Andrew Winowatan, Michelle Verhulst, Stefaan	Blockchain Case Study: Registering Births on the Blockchain in Illinois	2018	Blockchain, Parents or legal guardian manage digital ID till child turns 18	Multiple consent openings to access information	Multiple access for the information on the journal. Complex for use for users
2	Rahman, Mohammad Saidur Khalil, Ibrahim Mahawaga, Pathum Chamikara Bouras, Abdelaziz Yi, Xun	A novel architecture for tamper proof electronic health record management system using blockchain wrapper	2019	blockchain-based tamper-proof electronic health record (EHR) management system	wrapper layer integration mechanism, named as the blockchain hand shaker, between the existing cloud- based EHR management system and public blockchain network to develop a tamper-proof health record management system	Cross domain diversities not considered
3	Saleh, Omar S. Ghazali, Osman Rana, Muhammad Ehsan	Blockchain based framework for educational certificates verification	2020	Use of blockchain for certificate verification		Used only for verification not creation

4	Hu, Yining Liyanage, Madhusanka Mansoor, Ahsan Thilakarathna, Kanchana Jourjon, Guillaume Seneviratne, Aruna	Blockchain-based Smart Contracts - Applications and Challenges	2018	Smart Contracts	Do not necessarily guarantee their privacy. In particular, they do not guarantee unlink ability, which is crucial not only for privacy but also for fungibility
5	Karamachoski, Jovan Marina, Ninoslav Taskov, Pavel	Blockchain-Based Application for Certification Management	2020	The application consists of two functional parts: one part is the certificate identification (CID) number storage procedure on the Ethereum Blockchain via Smart contract and the other segment is the front-end and the back-end of the application stored on the IPFS network. The CID number is paired to the address of the certificate record on the IPFS network	

6	Nauwerck, Gerolf Forssell, Rebecka Cowen	The Digital Work Environment-a Challenge and an Opportunity for CSCW	2018	Smart Contracts, Digital signature		
7	Grather, Wolfgang Kolvenbach, Sabine Ruland, Rudolf Schutte, Julian Torres, Christof Wendland, Florian	Blockchain for Education: Lifelong Learning Passport	2018	the Blockchain for Education platform based on the Ethereum blockchain. Two smart contracts written in Solidity codify access control mechanisms (IdentityMgmt) and manage certificate records (CertMgmt) stored in the blockchain. The Interplanetary Filesystem (IPFS) is used as a public distributed read-only storage for profile information of certification authorities. Finally, the BSCW document management system stores and validate certificates		the system runs on the Ethereum blockchain, it introduces monetary overhead.

8	Yakubov, Alexander Shbair, Wazen M. Wallbom, Anders Sanda, David State, Radu	A blockchain-based PKI management framework	2018	Public-Key Infrastructure (PKI) management framework	The advantages proposed by our framework mitigate the problems with traditional PKI such as the difficulties with rapid certificate revocation, elimination of single points-of-failure and CAs misbehavior. Evaluation results show the benefits of using blockchain technology to build robust PKI system due to reasonable performance and attractive maintenance costs.
9	Nguyen,Binh Minh Dao, Thanh Chung Do, Ba Lam	Towards a blockchain-based certificate authentication system in Vietnam	2020	Blockchain	
10	Bele, Roshani S Mehare, Jayant P	A Review On Digital Degree Certificate Using Blockchain Technology	2021	Blockchain for school certificates	

11	Bergquist, Jonatan	Blockchain Technology and Smart Contracts: Privacy-preserving Tools	2017	Use of Blockchains and smart contracts	Use of Blockchains and smart contracts	
12	Mcphee, Chris Ljutic, Anton Swan, Melanie Ryan, Philippa Wolfond, Greg Rooney, Hugh Aiken, Brian Rooney, Megan	Technology Innovation Management Review	2017	The use of blockchain to secure digital assets		
13	Capece, Guendalina Ghiron, Nathan Levialdi Pasquale, Francesco	Blockchain technology: Redefining trust for digital certificates	2020	Using blockchain to ensure integrity of digital certificates		
14	Aronoff-Spencer, Eliah Saggese, Steven Zhao, Yunting Kalisky, Tom Avery, Courtney Forster, Deborah Edith Duarte-Vera, Lilia Almada-Salazar, Lucila Alejandra	Biometric recognition of newborns and infants by non-contact fingerprinting lessons learned	2019	Used of non-contact imaging of infant fingerprint	Limited only with fingerprint	Other biometric identification modes besides fingers, especially iris scanning, are technically possible but fail

	Perales-Gonzalez, Daniel Hubenko, Alexandra Kleeman, Michael Chacon-Cruz, Enrique					due to infant behaviors
15	Omojokun Gabriel Aju*, Adeola David Akinwumi, Olubunmi Eunice Aliyu	Design and implementation of biometric child birth registration system for sustainable national development planning	2022	Use of PHP programming language with JavaScript, Minitiae-based Fingerprint Matching Algorithm, and MYSQL database system .	Online accessible interface for the government officials with birth registration responsibility to biometrically register a child at birth using fingerprint method and enabling a centrally managed birth registration database	Central registration database prone to attack

2.12 Where is Blockchain Being Used Today?

As seen in the early days of the internet, most of the current blockchain implementations are focused on improving back-office efficiencies and reducing the time and cost of operating processes. As these administrative processes mature, they will provide the foundation for new customer-facing commercial and strategic opportunities.

Financial Services: Blockchain technology originally devised as the foundation of Bitcoin, the first digital currency. However, experts were quick to realize that the technology represented far more, and that it could eventually change financial services as profoundly as the internet had changed media and entertainment in the 1990s and early 2000s. Most banking institutions are adopting blockchain and advanced distributed ledger technologies for a wide range of functions, including trade settlements, payment processing and cross-border transactions (Fuch, 2019).

Financial institutions and banks no longer see blockchain technology as threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications (Crosby et al., 2016).

Healthcare: The global healthcare industry manages vast amounts of clinical and administrative data, from the pharmaceutical supply chain to patient medical records and claims management. The introduction of smart medical devices including everything from personal fitness trackers to connected surgical suites presents an entirely new ecosystem of information to mine, and the pool of data collected is growing exponentially. Accurate, accessible data are critical to improving clinical outcomes and

reducing waste, and blockchain immutability and ability to connect currently siloes of information and serve as the "single source of truth" are key enablers.

Government: The blockchain will allow the development of e-government, land register, shares register, crow funding, keeping of digital assets, supply chain management, supply of electricity coming for instance from renewable energy (Philippe, 2012). Governments around the world, including those in Denmark, Dubai, Estonia, the European Union, Georgia, the Isle of Man, Switzerland and the United States, are already using blockchain for everything from property records to voting. Its ability to provide a chronological, immutable, single source of truth makes it ideal for individual identities, property records, patents and other primary data (Fuch, 2019).

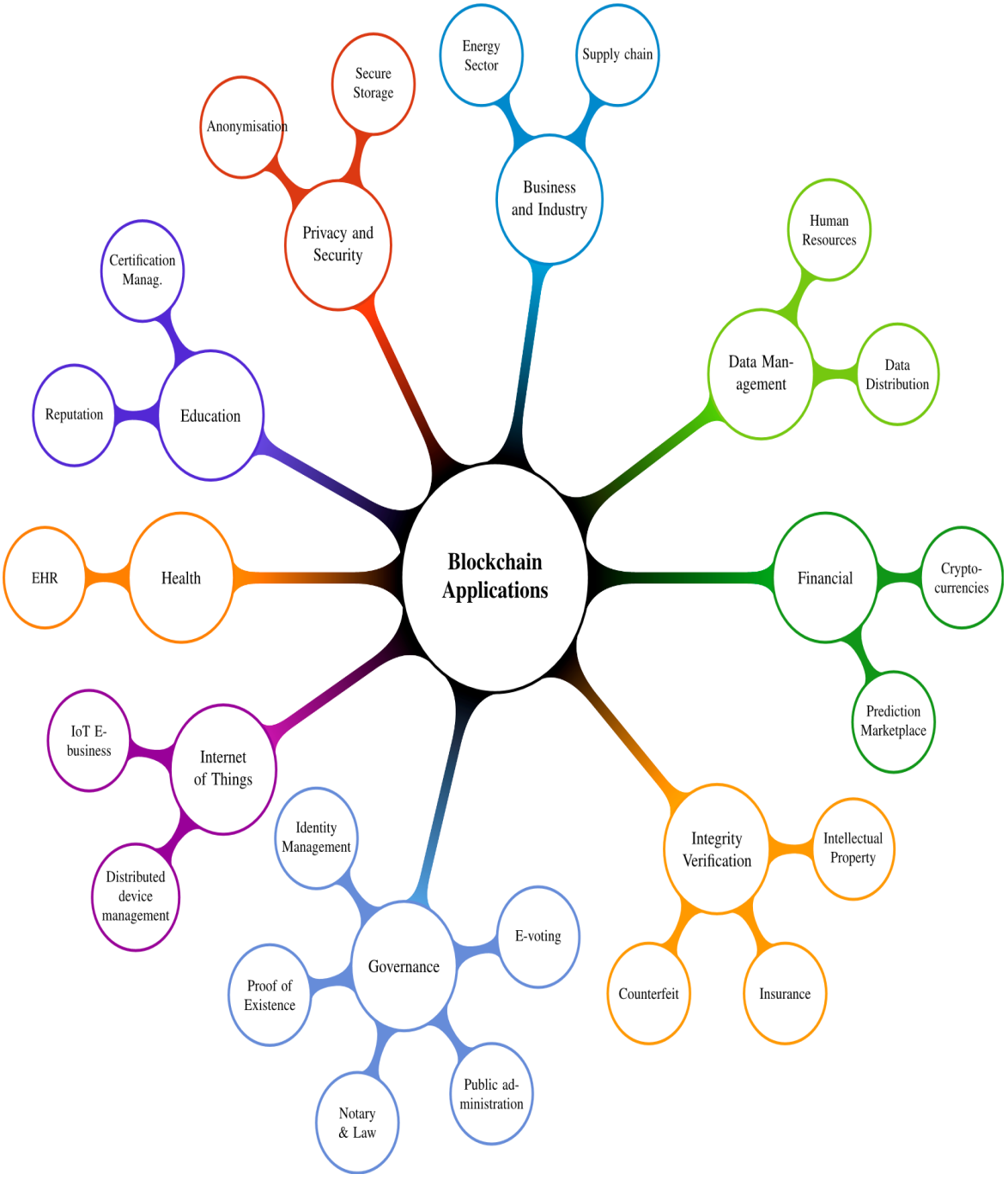

Figure 2.8: Blockchain applications and implementations (Casino F, Dasaklis T K and Patsakis C, 2019)

CHAPTER THREE

3.0 MATERIALS AND METHOD

3.1 Proposed System Architecture

In this section, we discuss our proposed architecture based on blockchain for birth registration and verification using smart contracts and public-private key encryption.

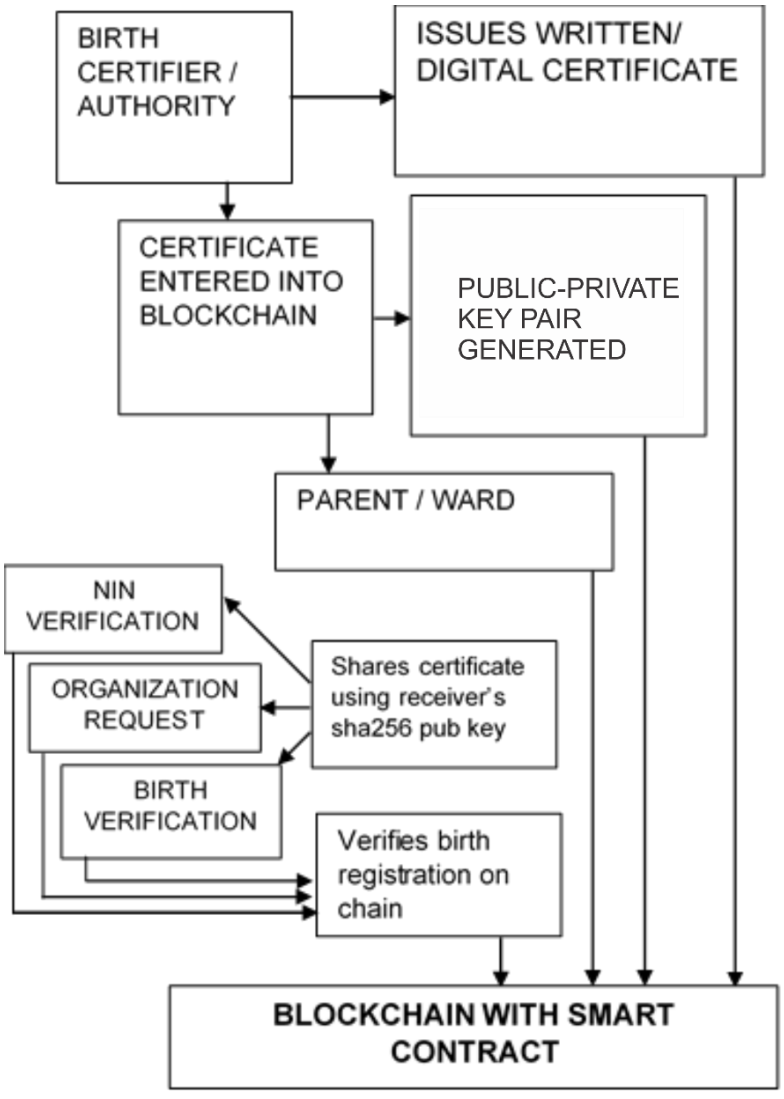

Figure 3.1: Proposed System Architecture

The system architecture depicted in Figure 3.1 consists of two main parts: the registration part and the verification part. In the registration part, a birth certifier/authority registers a

birth and issues a digital certificate to the parent or guardian. This certificate is then registered on the blockchain through a smart contract. Once the certificate is committed to the blockchain, a public-private key pair is generated in the form of a wallet address or token, which is also issued to the parent/guardian.

The verification system, which is the second part of the architecture, allows organizations to request verification of birth information. The birth information is shared by providing the public key of the certificate, which is fed into the blockchain and verified if found. When a birth record is added to the blockchain, it becomes part of the ledger transactions. Before certificate data is entered into the chain, the smart contract verifies the authenticity of the data and checks that both sender and receiver nodes are signed in the case of a transfer. For each certificate entered into the chain, a unique hash is generated with a timestamp. These hashes are generated using cryptographic functions to ensure that every certificate on the blockchain is uniquely identified.

Blockchain technology used in the system, abstracts the public key of the nodes and offers a human-readable nomenclature for nodes in the chain. Birth certificate owners can send their birth token to the specified name/account. The developed system operates on a consortium principle, where birth data stored on the ledger is only visible to the owner and whoever the owner sends it to. Furthermore, only chosen qualified nodes can access or consume client data via the smart contract by subscribing to the respective public streams. This ensures that everyone in the chain does not have access to citizens' birth certificates, providing a higher level of privacy and security.

3.1.1 Corda Blockchain

Corda is a permissioned peer-to-peer (P2P) distributed ledger technology (DLT) that facilitates the development of applications. With Corda, parties can freely discover and

transact with each other in a single, open network while having confidence in the identification of network participants.

Corda software adheres to a set of common standards and criteria. Some of these criterions are:

i. **Assured identity**: Parties will have confidence in the network's participants' identities. Identification in Corda is represented by a certificate issued by a relevant authority
ii. **Privacy**: The only people that have access to transaction information are those who are involved in the transaction and those who need to verify transaction source
iii. **Interoperability**: Corda is intended to allow numerous applications to coexist and interoperate on the same network; a defined set of contract interfaces is supplied to optimize interoperability from a wide range of providers.

3.1.2 Corda Smart Contracts (CorDapps)

CorDapp is a shorthand for Corda distributed application which run on the Corda node having these key components:

i. **States**: States keep track of data between transactions and are immutable, which means they can't be changed after they've been formed. Any modifications must instead result in the creation of a new successor state
ii. **Contracts**: Contracts define the validation criteria that will be applied to transaction inputs and outputs. Contracts guarantee that transaction states are valid and that invalid transactions are avoided. One or more contracts may exist in a CorDapp, each of which provides rules for one or more states

iii. **Flows**: Flows are the activities your CorDapp may take on a network, and they constitute your CorDapps business logic. Flows allow parties to coordinate their operations without the use of a central controller

iv. **Transactions**: A transaction is a request to update the ledger. It consumes current input states and outputs new ones to update the ledger. Before a transaction is accepted by the nodes, a transaction must be unique, valid, and signed by the appropriate parties

v. **Notary**: A notary is a Corda network service that helps prevent the duplicate expenditure of network assets. It does so by guaranteeing that each transaction includes unique input states that have not been utilized by a previous transaction. A transaction is regarded as finished after it is signed by the notary

vi. **Consensus**: In Corda, you may establish consensus by proving a transaction that is both valid and unique. Consensus is a method that allows nodes to agree on the network's current state. Before a proposed transaction can be entered into the ledger, both parties must agree that it is legal

3.1.3 The Proposed Algorithms

Each certifier node enters valid birth information into the CorDapp ensuring only credible information is entered into the chain by uploading birth data signing and encrypting data. An elliptic curve mathematical function is used to generate private and public keys for parents/ward. The birth data gets signed successfully to start the flow of the data in between relevant parties. The complete process for uploading and encrypting birth data in CorDapp is given in Algorithm 1. Once the data gets uploaded to the node, the CorDapp encrypts using digital signatures distributed through the Certificate Authority (CA). The nodes participating exchange the certificates for sharing private and public

keys to establish data legitimacy, valid proof of origin, and to make sure correct recipients obtain the data. As soon as the requester node gets the encrypted data, the decryption process is initialized to check for the validity of the received data. Each node generates a public and private node in the decryption process, respectively. Each of these transaction signatures are compared to match the sender and receiver signatures for starting decryption. The CorDapp creates the flow if the decrypted transaction is similar to the uploaded transaction. A detailed flow of the decryption and retrieving of the file is given in Algorithm 2.

Algorithm 1 Uploading and Encrypting Birth Data in CorDapp.

Input: Child Data($Birth_d$)
Result: Data signed and encrypted
Data: Each Certifier node(K) generates Public and private Key pairs PuK, PrK respectively.
$K_r \leftarrow Birth_d$ /* Request for $Birth_d$ Data */
$PuK1 \leftarrow PrK1 \leftarrow Ec(F)$
/* Private and Public keys are generated using elliptic curve(secp256r1) mathematical function */ $Txn+ \leftarrow E[Birt_d signed] \leftarrow PuK_2 + PrK_1 + SHA_{256}(Birth_d)$
/* The Data gets hashed and signed with digital signatures exchanged between Certifier Nodes and added to the transaction */
/* If hashes Birth data is signed successfully, start the data flow between relevant nodes*/
if $K_2(SHA_{256}(Birth_d)) == K_1(SHA_{256}(Birth_d))$ **then**
  if ($Birth_d$) is signed **then**
    K(Txn) ← *CallEchoInitiatorFlow ()*
    K(Txn) ← *DeployEchoflows*
    K(Txn) ← *Executeflows*
    /* Each Transaction once encrypted is added to Corda chain for synchronizing and validating*/
    C_n + ← K(Txn)
  end
  Discard Corda flow operations
end
End the process Repeat the steps for Birth data entry

Algorithm 2 Accessing and Decrypting Birth Data.

Input: Encrypted Birth Data($E(Birth_d)$)
Result: Data accessed and decrypted
Data: Each Certifier node(k) generates Public and private Key pairs PuK, PrK respectively.
$K_r \leftarrow E(Birth_d)$
/*A requester node n requests for Birth Data*/
$PuK1 \leftarrow PrK1 \leftarrow Ec(F)$
/* Private and Public keys are generated using elliptic curve(secp256r1) mathematical function */
$K(Txn) \leftarrow C_n$
/* The transaction in the requester node is accessed from Corda chain */
/* If the requester node transaction signatures match with the sender and receiver signatures, Decrypt the transaction */
/* If Decrypted Transaction is similar to Uploaded Transaction data, Start Corda Flows */
if *K(Txn) signatures match* **then**
    $D(K(Txn)) \leftarrow PrK_2 \leftarrow PuK_1 \leftarrow SHA_{256}(Birth_d)$
    if $D(K(Txn))==(K(Txn))$ then
        $K(Txn) \leftarrow$ CallEchoResponderFlow()
        $K(Txn) \leftarrow$ Executeflows
    End
    End the process
End
Decryption failed Repeat the steps for every encrypted Birth data request

3.1.4 Framework design

The parties involved in our blockchain data sharing scenario are the hospital attendants, citizens (individuals and organizations/agencies.), and government.

With Hospital attendants carrying out birth registrations for every new birth, these data help to offer better sharing and verification solutions to citizens' birth certificates using permissioned blockchain technology. We take data of newborns as the standard data required for a complete birth certificate processing that includes, name, city, gender, father, mother, paternal grandfather, paternal grandmother, maternal grandfather, maternal grandmother, and witness. The frontend node consists of a form for collecting newborns' data. It connects to the blockchain implemented at the backend and on

successful submission of the form, the transaction gets added to the blockchain. The other nodes in the blockchain have permissions as follows: “connect,” “receive,”, “create,” “issue,” “mine,”. These permissions allow the nodes to perform certain operations. The create permission allows the node to create a stream for sharing data and this is one of the key features of the proposed data sharing solutions. The “issue” permission allows a node to issue assets whereas “mine” permission allows them to take part in providing solutions to adding the validated blocks into the chain. This ensures that citizens' birth certificates are not accessible to everyone on the chain.

3.1.5 Calculating Private and Public Keys

For every transaction in the DLT, the system calculates its unique hash and transaction ID. The public key serves as the address to which the Digital birth certificate is sent. To calculate the (pubKey, n) and a priKey

First, we have to choose two prime numbers p and q, then we calculate

$$n(p,q) = p \cdot q. \quad (1)$$

After that, we calculate Euler's quotient function

$$\phi(n(p,q)) = (p-1) \cdot (q-1) \quad (2)$$

only if p and q are prime numbers. Otherwise, it is a NP problem.

Then we can use a random pubKey, which is not a divisor of $\phi(n)$ and is smaller than

$$\phi(n) \quad (3)$$

Calculating priKey means calculating b in following equation:

$$a \cdot \phi(n) + b \cdot pubKey = 1 \quad (4)$$

Where we can use the extended Euclidean algorithm. Now we can delete p, q and $\phi(n)$

3.2 Design Overview

A high-level overview is given of the registration system designed in this thesis. It goes from more abstraction at the top ("Software system level"), to lower level of abstraction in the bottom ("Contract level"). For the sake of relevance to the code written for the PoC, only the "Smart contracts"-component is explained in details.

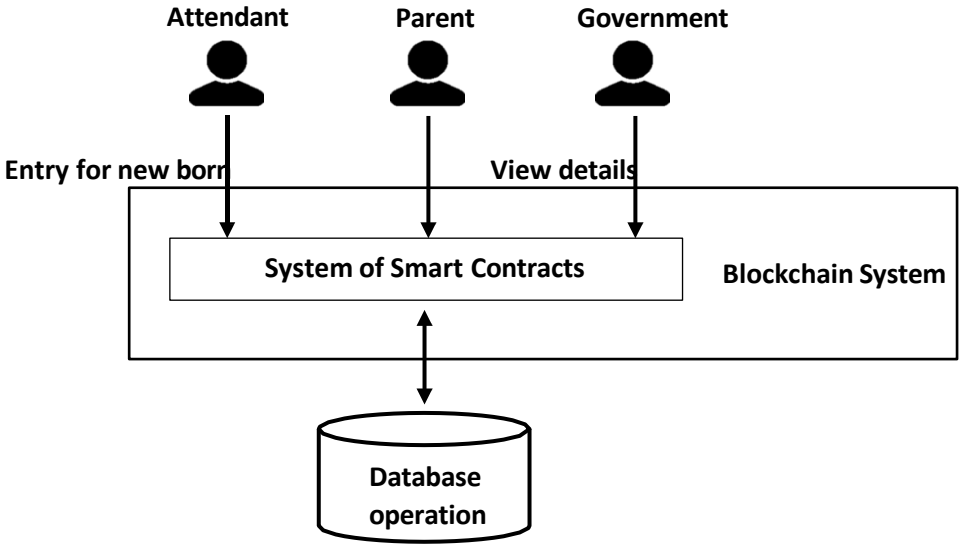

Figure 3.2: Overview of different users and their interactions with the blockchain and system of smart contracts that exist on the blockchain system

3.3 Evaluation Metrics

The scalability of a blockchain system can be evaluated using measures such as throughput and latency. Since we only successful transactions are considered, we can alternatively refer to the throughput as goodput. Transaction throughput is specifically defined as the number of transactions per second processed by the blockchain network. When a transaction is included in a block and committed to the blockchain, it has been successfully processed. Transaction latency is the amount of time between when a transaction is submitted and when the result is made available on all valid nodes in the network (after consensus and propagation time). By examining how throughput and latency change as more blockchain nodes are added to the system, scalability can be

determined. (Mazzoni *et al.*, 2022) Since more nodes must participate in the consensus process while testing larger networks, we may anticipate a higher transaction delay. As a result, we anticipate throughput to decrease as more nodes are added to the network for the same reason.

3.4 Research Analysis

Research type of this study is action research. Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goal of social science by joint collaboration within a mutually acceptable ethical framework. Four processes are covering the action research. First is diagnosing, identifies and defines the problem. Second is action planning, specifies the courses of action to be taken. Third is action taking, implement the planned action. Forth is evaluating, analyses the effects of the actions. Specifying learning identifies what was learnt.

3.5 Implementation

The following actors/nodes have been considered in the project.

3.5.1 New Birth

A new birth serves as the entry point into the system. Once birth takes place, a certifier is required to commit the birth details into the chain. This operation births the registration module. The module consists of a form that collects relevant information about the newborn and a credibility check by the certifier/registrar to ensure that information presented is valid. Information required by the form includes the registration center, town/village, LGA state, volume year, entry no, full name, sex, date of birth, place of birth, full name of father, full name of mother, and name of the registrar. Upon successful entry, this creates a pair of private and public keys that grant access to the child's wallet on the blockchain.

3.5.2 Certifier (Registrar) Module

The Certifier or Registrar module is a point of human authentication in the system. He ensures that credibility is maintained in the system. Before a block gets added to the chain (mined), information must be checked against falsity and duly acknowledged by the register for transactions within his jurisdiction. This ensures that only valid information is entered into the chain to provide credibility for the blockchain. The certifier/registrar could be a private or public regulator in this case.

3.5.3 Requester

The requester could be an organization (public or private) or an individual or group of individuals that require a user's birth certificate. For a successful transaction, the requester sends his public address to the user whose birth verification is needed. The user sends a copy of his birth certificate to the public address of the requester including his public address for verifying that the token is from the right source. The requester then accesses the received token (birth certificate) by providing his wallet address (private address in this case) which brings a completion to the transaction.

3.5.4 Technology

The proposed system will be implemented with the JAVA programming language. JAVA will be used as the backend language while SPRING BOOT will be used to develop the RESTFUL API that communicates with the frontend. Angular, a JAVASCRIPT framework work for frontend development will be utilized to develop an easy-to-use User Interface. The system will be hosted on firebase as a full web application that accesses the developed blockchain.

CHAPTER FOUR

4.0 RESULTS AND DISCUSSIONS

4.1 Experimental Setup

Corda is a scalable, permissioned peer-to-peer (P2P) distributed ledger technology (DLT) platform that enables the building of applications that foster and deliver digital trust between parties in regulated markets, this private blockchain platform ensures that transactions are only visible to the participating parties. Our system is built on Corda with nodes named Sender and Receiver to demonstrate the owner and receiver of birth certificate data. The User Interface (UI) interface is defined in Angular to send API calls to initiate transactions in the DLT. The system consists of three modules, the DLT, the Backend and the Interface. Elliptic curve cryptography is utilized to generate the public-private key pairs. The public key is to be shared with others to receive tokens (birth certificate data, in our case). Our private key is used to sign our transactions so that nobody can spend or have access to our tokens in the blockchain. Upon filing the form, a pair of private-public keys are generated which provide access to a child's wallet.

4.2 Login

To gain access into the blockchain, an organization is first registered into the platform and given a unique Authentication ID and a combination of characters as a password. On a successful sign-on, the system opens up the birth certificate form that has all the required details to be filled in including the ward's name, gender, city, paternal and maternal details. The login page is shown in figure 4.1.

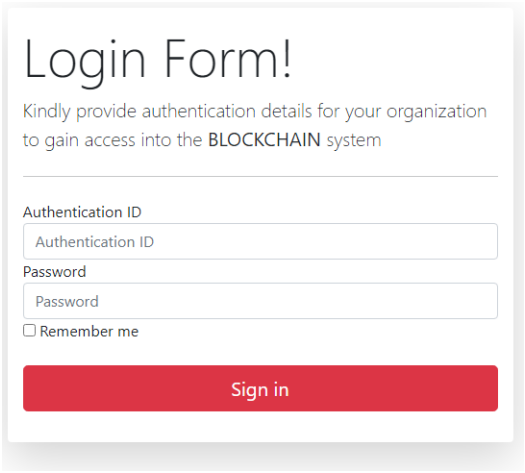

Figure 4. 1: Login form

4.3 Internal Process

On filling the form in Figure 4.2 and pressing the submit button, the system converts the form documents into a JSON format and sends them to the backend for validation. Upon successful validation of the JSON file, the system adds a new block with the JSON file to the chain deployed with Corda, an open Source Blockchain platform, and automatically generates a private-public key pair that holds the address of the just added block in the chain. The private key will be used to sign transactions in the future, while the public key will be used to communicate the transaction's address with the public.

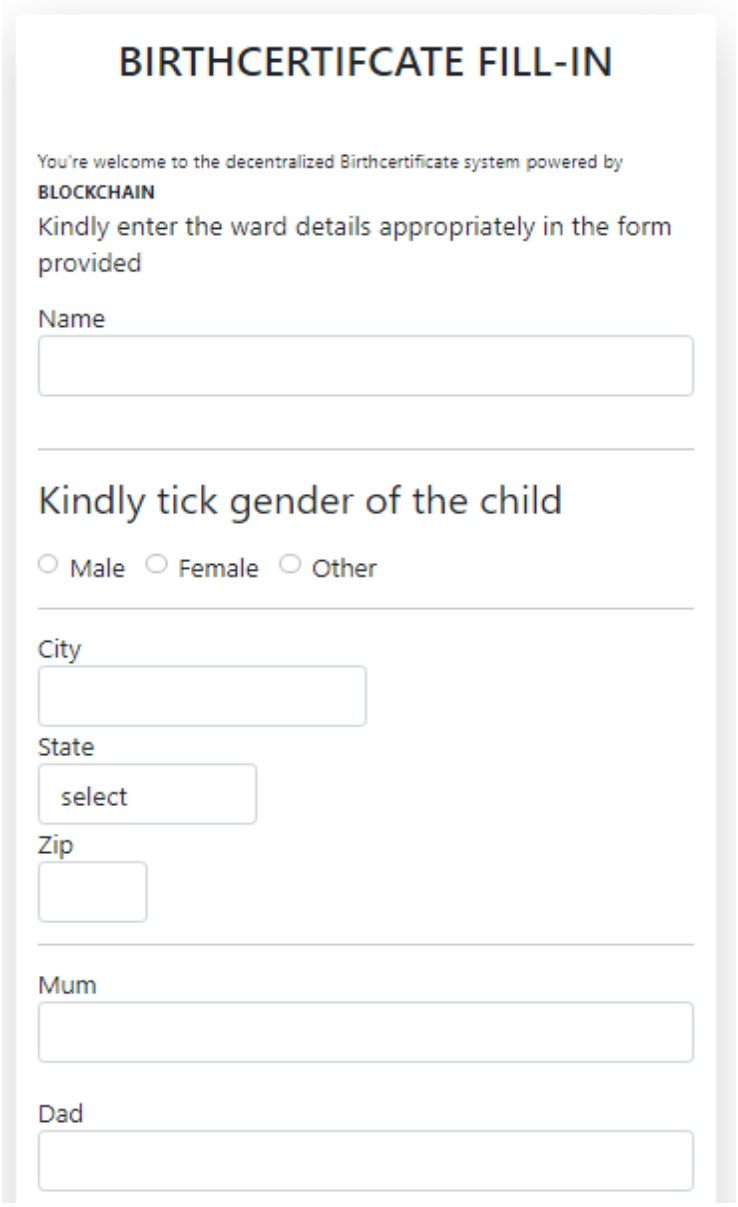

Figure 4.2: Certificate form

4.3.1 User Interface

To gain access into the blockchain, an organization is first registered into the platform and given a unique Authentication ID and a combination of characters as password. On successful sign on, the system opens up the birth certificate form that has all the required details to be filled in including the ward's name, gender, city, paternal and maternal details.

4.3.2 Birth Certificate Fill-in

This provides an interact able interface to entering the wards details into the DLT. It collects information like name, gender, city, state, zip, mum, dad, registrar, etc.

4.4 Transaction Flow

The nodes are deployed using the command on Windows:

```
gradelew.bat deployNodes
```

Figure 4. 3: Windows Command

To start up the DLT nodes on console, the following command is run (Windows)

Figure 4.3 is a sample Birth certificate transaction between Sender and Receiver Node.

```
start CertificateTransferInitiator town: GK, state: Niger, lga: GK, year: 2020, name: 1, sex: male, dob: 19012020, fatherName: Salawu, motherName: Blessing, registrarName: Matthew, receiver: "O=Receiver,L=Nigeria,C=NG"
```

Figure 4. 4: Node Transaction

The receiver gets access to the sent certificate data by running the following command

```
run vaultQuery contractStateType: com.template.states.CertificateState
```

Figure 4. 5: Receiver's Command

The command above exposes the contents of the ledger which shows the sent certificate data.

Figure 4.7 shows the process of updating the ledger and creating a 64-bit unique hash to present an unchangeable birth certificate record.

Figure 4.6: Ledger gets updated

Figure 4.6 shows the message confirming a blockchain has been successfully created to represent the birth certificate.

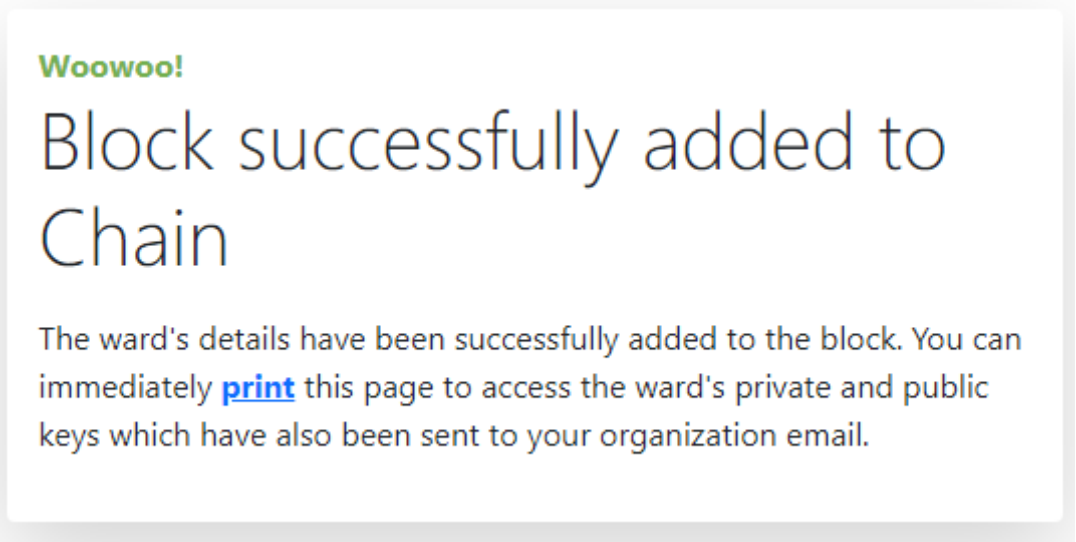

Figure 4.7: Successful ledger update

4.5 SQL Database setup

Before running the Corda node, the database user and schema namespace with administrative permissions was created. This grants the database user full access to a Corda node, such that it can execute both DDL (Data Definition Language) statements (to define data structures/schema content e.g. tables) and DML (Data Manipulation Language) queries (to manipulate data itself e.g. select/delete rows.

To connect to the master database as an administrator, the following script is run:

```
CREATE DATABASE my_database;
CREATE LOGIN my_login WITH PASSWORD = 'my_password',
DEFAULT_DATABASE = my_database;
CREATE USER my_user FOR LOGIN my_login;
```

Figure 4. 8: Database Connection Script

Connect to a user database as the administrator

```
CREATE SCHEMA my_schema;


CREATE USER my_user FOR LOGIN my_login WITH DEFAULT_SCHEMA =
my_schema;
GRANT SELECT, INSERT, UPDATE, DELETE, VIEW DEFINITION, ALTER,
REFERENCES ON SCHEMA::my_schema TO my_user;
GRANT CREATE TABLE TO my_user;
GRANT CREATE VIEW TO my_user;
```

Figure 4. 9: Admin Connection to User Database

4.6 System Testing

The system testing phase in software design is that phase, where the modules are interlinked together to create smooth navigation and flow of the system as a single entity. During system testing, all functions or different modules within the system are integrated and connected to the local host. System testing is usually carried out in a software system to be sure that each function is functioning as envisaged and error-free. Testing procedures used in this project are listed below:

4.6.1 Unit Testing

Unit testing is the testing of different modules that make up the centralized blockchain. The goal is to ascertain that each entity of the model code performs as expected. In a big software company, unit testing is usually performed by the software developers of each module in a test-driven-development procedure. As for this project, the unit testing was carried out by the researcher during the coding (development) phase of the system. We isolated a section of code and validate its correctness using JUnit testing.

4.6.2 Whole System Testing

System testing entails the testing of the whole system through interfacing of hardware and software components of the system in order to find errors with the system. During system testing, we used real data (DATA) to test the system output. A transaction flow was made to send data from one node to the another which was successfully received by the other end.

4.7 Performance Evaluation

A framework for evaluating private/permissioned blockchain platforms is called BLOCKBENCH. Parameters like latency, throughput, fault tolerance, and scalability can be measured with this tool. Corda blockchain platform and workloads can be integrated via a straightforward set of APIs. Corda performance test suite is installed and a single node or a small group of nodes with a notary allowed is deployed for the performance evaluation of the Corda platform. Through RPC calls, this test suite starts flows on nodes and records the latency and throughput using Apache JMeter.

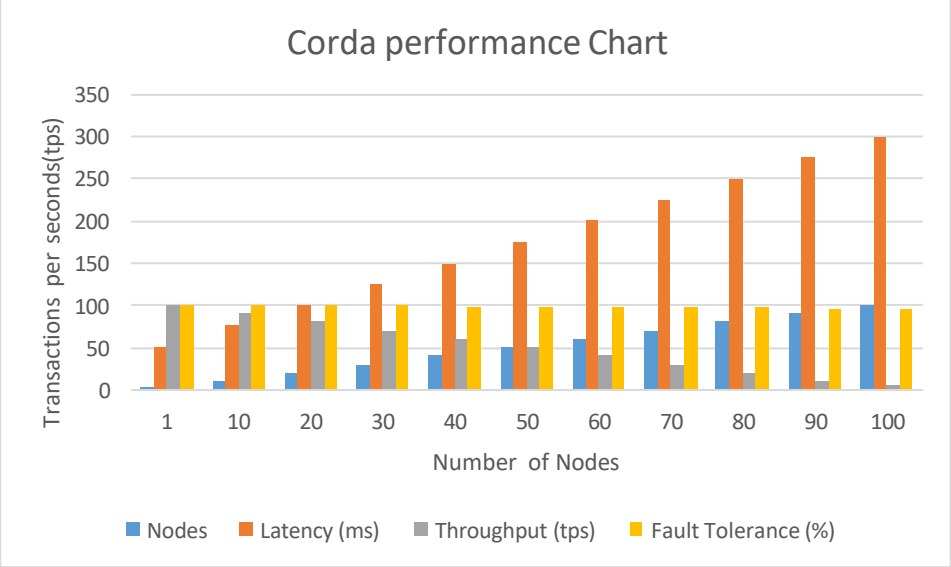

Figure 4. 10: Corda Performance Chart

The performance of Corda on BLOCKBENCH as seen from the graph in figure 4.10, as the number of nodes increases from 1 to 100 shows that Corda demonstrates a lower latency, indicating faster transaction processing times as the number of nodes increases. Corda also shows higher throughput values, indicating the network's ability to process a larger number of transactions per second as the number of nodes increases. The fault tolerance percentage achieved by Corda is consistently high across different numbers of nodes, indicating a resilient and robust network. From the performance of Corda on BLOCKBENCH, it can be inferred that Corda scales well with the growth in the number of nodes, as indicated by the lower latency and higher throughput values. Corda achieved a significantly lower latency which means that nodes are able to complete more flows in the same amount of time, which achieves higher throughput. The peer-to-peer messages between nodes can be compressed, which leads to more efficient use of network bandwidth. An exponential increase in latency was observed as the number of nodes that participate in the transaction are increased. Therefore, Corda scale better with the growth in network size (nodes). The presence of additional participants had minimal impact on its latency.

CHAPTER FIVE

5.0 CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Birth records are an integral part of humans because they provide a sense of belonging. Various systems are utilized for storing and securing births records which include centralized databases and a combination of biometric and cryptography technologies. In this project, we have used blockchain technology and implemented various cryptographic algorithm like, sha256 for providing seamless storage, security, and monitored the distribution of birth records. The system also incorporates web technologies like SPRING BOOT and Angular which makes registration easily accessible over the internet. While this system proves promising, it is still a work in progress.

The space of blockchain has potentials to foster emerging markets and economies including smart cities, value-based healthcare, decentralize sharing economy in a centralized context, machine to machine transactions, data sharing marketplace. These savvy advancements are needed for the country to witness economy stability and progress. This project has fully integrated the capabilities of blockchain technology into the Nigeria Birth registration system to achieve a seamless verification, storage and sharing of birth certificate amongst parties.

5.2 Recommendation

Blockchain has proven to be a very powerful tool that can be integrated in many different aspects in technology and life. This form of decentralized system makes the information written on to be immutable, and even though it can be accessed by anyone, it cannot be changed which makes it ideal for storing information. In the future, the system can be modified to generate not just a wallet address but also a unique identity number, and also

deployed across a plethora of devices like mobile and embedded chips for easier access to vital records.

5.3 CONTRIBUTION TO KNOWLEDGE

This research introduces a highly promising and innovative method for enhancing the precision, reliability, compatibility, and security of civil vital records. The approach leverages a secure and conscientious permissioned blockchain, offering extensive advantages to the realms of healthcare and technology. By employing this cutting-edge technology, significant contributions are made to the field, revolutionizing the way vital records are managed and ensuring heightened levels of accuracy, integrity, interoperability, and security, thereby paving the way for a more reliable and secure system in the future.

REFERENCES

Abubakar Idris, U., Awwalu, J., & kamil, B. (2016). User authentication in securing communication using Digital Certificate and public key infrastructure. International Journal of Computer Trends and Technology, 37 (1), 22–25. https://doi.org/10.14445/22312803/ijctt-v37p105

Al-Housni, N. (2019). An Exploratory Study in Blockchain Technology. PQDT - Global, 89. Retrieved from https://www.proquest.com/dissertations-theses/exploratory-study-blockchain-technology/docview/2199337101/se-2?accountid=27931

Allessie, D., Sobolewski, M., & Vaccari, L. (2019). Blockchain for digital government. In JRC Science for Policy Report: Vol. EUR 29677. https://doi.org/10.2760/93808

Aronoff-Spencer, E., Saggese, S., Zhao, Y., Kalisky, T., Avery, C., Forster, D., Edith Duarte-Vera, L., Almada-Salazar, L. A., Perales-Gonzalez, D., Hubenko, A., Kleeman, M., & Chacon-Cruz, E. (2019). Biometric recognition of newborns and infants by non-contact fingerprinting: Lessons learned. Gates Open Research, 3, 1-25.https://doi.org/10.12688/gatesopenres. 12914.2

Bele, R. S., & Mehare, J. P. (2021). A Review on Digital Degree Certificate Using Blockchain Technology. International Journal of Creative Research Thoughts (IJCRT), 9(2). 2320-2882. www.ijcrt.org

Bergquist, J. (2017). Blockchain Technology and Smart Contracts: Privacy-preserving Tools. 17023, 62. (Dissertation). Retrieved from http://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-323826

Bhatia, S., & Wright de Hernandez, A. D. (2019). Blockchain Is Already Here. What Does That Mean for Records Management and Archives? Journal of Archival Organization, 16(1), 75–84. https://doi.org/10.1080/15332748.2019.1655614

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., & Alazab, M. (2020). Blockchain for Industry 4.0: A comprehensive review. IEEE Access, 8, 79764–79800. https://doi.org/10.1109/ACCESS.2020.2988579

Brumberg, H. L., Dozor, D., & Golombek, S. G. (2012a). History of the birth certificate: From inception to the future of electronic data. Journal of Perinatology, 32(6), 407–411. https://doi.org/10.1038/jp.2012.3

Brumberg, H. L., Dozor, D., & Golombek, S. G. (2012b). History of the birth certificate: from inception to the future of electronic data. Journal of Perinatology 2012 32:6, 32(6), 407–411. https://doi.org/10.1038/jp.2012.3

Buterin, V. (2013). White Paper · ethereum/wiki Wiki · GitHub. undefined-undefined. https://www.mendeley.com/catalogue/3ecbac49-0506-34aa-b7c414fe4def78a5/?utm_source=desktop&utm_medium=1.19.8&utm_campaign=open_catalog&userDocumentId=%7Beb19804d-699a-396e-ba67-c5fb31648ebe%7D

Caldarelli, G., & Ellul, J. (2021). Trusted academic transcripts on the blockchain: A systematic literature review. Applied Sciences (Switzerland), 11(4),1-22. https://doi.org/10.3390/app11041842

Casino F Dasaklis T K and Patsakis C. (2019). A systematic literature review of blockchain-based applications current status classification and open issues. Telematics and Informatics, 51–81.

Chen, Y., Li, H., Li, K., & Zhang, J. (2017). An improved P2P file system scheme based on IPFS and Blockchain. Proceedings - 2017 IEEE International Conference on Big Data, BigData 2017, 2018-January, 2652-2657. https://doi.org/10.1109/BigData.2017.82582

Cong, L. W., & He, Z. (2019). Blockchain Disruption and Smart Contracts. In Review of Financial Studies (Vol. 32, Issue 5, pp. 1754–1797). Oxford University Press. https://doi.org/10.1093/rfs/hhz007

Crittenden, C. (2020). Blockchain in California: A Roadmap. Permalink 15(4), 250–260. https://doi.org/10.11436/mssj.15.250 https://escholarship.org/uc/item/2j9596dp

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation Review, *2*(6-10), 71.

Danish National ID Centre (2018). Issuance and appearance of the Nigerian Birth Certificate (Issue December). African and Black Diaspora: An International Journal, 3(1), 17-34.

Darya Yafimava. (2019). What are Consortium Blockchains, and What Purpose do They Serve? | OpenLedger Insights. https://openledger.info/insights/consortium-blockchains/

Department of Economic and Social Affairs - Statistics Division. (2014). Principles and Recommendations for a Vital Statistics System - Revision 3. In Statistical Papers, Series MNo.19/Rev.3(Issue19).http://unstats.un.org/unsd/Demographic/standmeth/principles/M19Rev3en.pdf

Dharwadker, S., & Mills, S. (2019). Options for Digital Birth Certificates. In Options for Digital Birth Certificates. World Bank, Washington, DC. https://doi.org/10.1596/32542

Du, M., Ma, X., Zhang, Z., Wang, X., & Chen, Q. (2017). A review on consensus algorithm of blockchain. 2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017, 2017-Janua, 2567–2572. https://doi.org/10.1109/SMC.2017.8123011

Dubovitskaya, A., Baig, F., Xu, Z., Shukla, R., Zambani, P. S., Swaminathan, A., Jahangir, M. M., Chowdhry, K., Lachhani, R., Idnani, N., Schumacher, M., Aberer, K., Stoller, S. D., Ryu, S., & Wang, F. (2020). ACTION-EHR: Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care. J Med Internet Res 2020;22(8):E13598 Https://Www.Jmir.Org/2020/8/E13598, 22(8), e13598. https://doi.org/10.2196/13598

Fabian, C. (2018). Un-chained: Experiments and Learnings in Crypto at UNICEF. Innovations: Technology, Governance, Globalization,12 (1-2), 30-45. https://doi.org/10.1162/inov_a_00265

Fuch, P. (2019). Blockchain. Retrieved from https://www.mercer.com/content/dam/mercer/attachments/private/gl-2019-blockchain-101-overview-mercer.pdf

Gabriel Aju, O., David Akinwumi, A., & Eunice Aliyu, O. (2022). Design and implementation of biometric child birth registration system for sustainable national development planning. 6(3), 138–146. www.aujst.com

Giudici, G., Milne, A., & Vinogradov, D. (2020). Cryptocurrencies: market analysis and perspectives. Journal of Industrial and Business Economics, 47(1), 1–18. https://doi.org/10.1007/s40812-019-00138-6

Grather, W., Kolvenbach, S., Ruland, R., Schutte, J., Torres, C., & Wendland, F. (2018). Blockchain for Education: Lifelong Learning Passport. Proceedings of 16th European Conference on Computer-Supported Cooperative Work, 1-8. https://doi.org/10.18420/blockchain2018

Gwyneth, I. (2020). Blockchain Technology History: Ultimate Guide. 101 Blockchains. https://101blockchains.com/history-of-blockchain-timeline/

Hamlaoui, S. (2020). Blockchain for The Drug Supply Chain Management. September 2020. Computers in biology and medicine, 140, 105100.

Hanson, C., Cox, J., Mbaruku, G., Manzi, F., Gabrysch, S., Schellenberg, D., Tanner, M., Ronsmans, C., & Schellenberg, J. (2018). Maternal and perinatal mortality in resource-limited settings - Authors' reply. The Lancet Global Health, 3(11), e673. https://doi.org/10.1016/S2214-109X(15)00157-6

Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177, 102857. https://doi.org/10.1016/j.jnca.2020.102857

Holland, M., Stjepandic, J., & Nigischer, C. (2018, August 13). Intellectual Property Protection of 3D Print Supply Chain with Blockchain Technology. 2018 IEEE International Conference on Engineering, Technology and Innovation, ICE/ITMC 2018 - Proceedings. https://doi.org/10.1109/ICE.2018.8436315

Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G., & Seneviratne, A. (2018). Blockchain-based Smart Contracts - Applications and Challenges. June.

Jacobovitz, O. (2016). Blockchain for identity management. In Technical Report (Issue 1). https://www.cs.bgu.ac.il/~frankel/TechnicalReports/2016/16-02.pdf

Karamachoski, J., Marina, N., & Taskov, P. (2020). Blockchain-Based Application for Certification Management. Tehnički Glasnik, 14(4), 488-492
14(4), 488–492. https://doi.org/10.31803/tg-20200811113729

Kiayias, A., Koutsoupias, E., Kyropoulou, M., & Tselekounis, Y. (2016). Blockchain Mining Games. EC 2016 - Proceedings of the 2016 ACM Conference on Economics and Computation, 365–382. https://doi.org/10.1145/2940716.2940773

Kumar Singh, S., Rao Vadi, V., & Professor, A. (2021). Evolutionary Transformation of Blockchain Technology. May. https://doi.org/10.1007/978-3-030-69395-4

Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2022). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.https://doi.org/10.1093/jamia/ocx6

Lamkoti, R. S., Maji, D., Bharati Gondhalekar, A., & Shetty, H. (2021). Certificate Verification using Blockchain and Generation of Transcript. India, 10(03), 539–544. https://www.ijert.org/research/certificate-verification-using-blockchain-and-generation-of-transcript-IJERTV10IS030260.pdf

Maduekwe, N. I., Banjo, O. O., & Sangodapo, M. O. (2017). The Nigerian Civil Registration and Vital Statistics System: Contexts, Institutions, Operation. Social Indicators Research, 134(2), 651–674. https://doi.org/10.1007/s11205-016-1448-5

Makinde, O. A., Olapeju, B., Ogbuoji, O., & Babalola, S. (2016). Trends in the completeness of birth registration in Nigeria: 2002-2010. Demographic Research, 35(1), 315–338. https://doi.org/10.4054/DemRes.2016.35.12

Mazzoni, M., Corradi, A., & Di Nicola, V. (2022). Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study. Blockchain: Research and Applications, 3(1). https://doi.org/10.1016/j.bcra.2021.100026

Mehdi Benchoufi, and P. R. (2017). Blockchain technology for improving clinical research quality. BioMed Central, 1–5. https://doi.org/10.1186/s13063-017-2035-z

Mills, S., Lee, J. K., & Rassekh, B. M. (2019). An introduction to the civil registration and vital statistics systems with applications in low- A nd middle-income countries. Journal of Health, Population and Nutrition, 38(Suppl 1), 1–4. https://doi.org/10.1186/s41043-019-0177-1

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

Nauwerck, G., & Forssell, R. C. (2018). The Digital Work Environment-a Challenge and an Opportunity for CSCW. ECSCW 2018 - Proceedings of the 16th European Conference on Computer Supported Cooperative Work, 17-20. https://doi.org/10.18420/ecscw2018

Nguyen, B. M., Dao, T. C., & Do, B. L. (2020). Towards a blockchain-based certificate authentication system in Vietnam. PeerJ Computer Science, 2020(3).https://doi.org/ 10.7717/peerj-cs.266

Oliha, F. O. Ebietomere, E. P. & Ekuobase, G. O. (2019). An electronic birth record management system for Nigeria. Nigerian Journal of Technology, 38(3), 763. https://doi.org/10.4314/njt.v38i3.31

Pal, O., Alam, B., Thakur, V., & Singh, S. (2021). Key management for blockchain technology. ICT Express, 7(1), 76–80. https://doi.org/10.1016/j.icte.2019.08.002

Palma, L. M., Vigil, M. A. G., Pereira, F. L., & Martina, J. E. (2019). Blockchain and smart contracts for higher education registry in Brazil. International Journal of Network Management, 29(3), e2061. https://doi.org/10.1002/nem.2061

Philippe Denis. (2012). Blockchain and Smart Contract: Lex Cryptographia. European University Institute, 2, 2–5. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32016R0679&from=PT%0Ahttp://eurlex.europa.eu/LexUriServ/LexUriServ. do?uri=CELEX:52012PC0011:pt:NOT

Plecker, W. A. (1915). a Standard Certificate of Birth. American Journal of Public Health, 5(10), 1044–1047. https://doi.org/10.2105/ajph.5.10.1044

Raghav, Andola, N., Verma, R., Venkatesan, S., & Verma, S. (2019). Tamper-proof certificate management system. 2019 IEEE Conference on Information and Communication Technology, CICT 2019, 1-6. https://doi.org/10.1109/CICT48419. 2019.9066236

Rahman, M. S., Khalil, I., Mahawaga, P. C., Bouras, A., & Yi, X. (2019). A novel architecture for tamper proof electronic health record management system using blockchain wrapper. BSCI 2019 - Proceedings of the 2019 ACM International Symposium on Blockchain and Secure Critical Infrastructure, Co-Located with AsiaCCS 2019, 97–105. https://doi.org/10.1145/3327960.3332392

Railean, E. (2017). Metasystems learning design theory on information visualization. Proceedings - 2017 21st International Conference Information Visualisation, IV 2017, 355–359. https://doi.org/10.1109/iV.2017.80

Ritik Banger, Risheek Mittal, Ronit Khowal, A. M. (2019). A Study On BlockChain And Cryptography. Jetir, 6(5). https://www.researchgate.net/publication/342151198_A_Study_On_BlockChain_And_Cryptography

Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. Journal of Critical Reviews, 7(3), 79-84. https://doi.org/10.31838/jcr.07.03.13

Salman, T., Jain, R., & Gupta, L. (2018). Probabilistic Blockchains: A Blockchain Paradigm for Collaborative Decision-Making. 2018 9th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2018, May 2019, 457–465. https://doi.org/10.1109/UEMCON.2018.8796512

Shah, M., & Kumar, P. (2019). Tamper proof birth certificate using blockchain technology. International Journal of Recent Technology and Engineering, 7(5), 95–98.

Srivastava, G., Dhar, S., Dwivedi, A. D., & Crichigno, J. (2019). Blockchain Education. 2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019. https://doi.org/10.1109/CCECE.2019.8861828

Swan, M., Cambridge, B. •, Farnham, •, Köln, •, Sebastopol, •, Tokyo, •, & Reilly, O. ’. (2020). Blockchain Blueprint for a New Economy. in e-LoA Technopreneurship Journal. Aptisi Transactions On Technopreneurship (ATT), 2(1), 98-103.

Tara Stähli. (2018). Managing Registration on the Blockchain – The Future of Identity Management in Humanitarian Cash Transfer Programmes? (Issue June). https://repository.graduateinstitute.ch/record/296249/files/241479712_341431897_15982_15928_289268956.pdf

UNICEF. (2019). CRVS - Birth, Marriage and Death Registration in Ghana - UNICEF DATA. https://data.unicef.org/resources/crvs/ghana/

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Rodrigues, J. J. P. C. (2019). BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records. 2018 IEEE Globecom Workshops, GC Wkshps 2018 - Proceedings. https://doi.org/10.1109/GLOCOMW.2018.8644088

Warasart, M., & Kuacharoen, P. (2012). Paper-based Document Authentication using Digital Signature and QR Code. 4TH International Conference on Computer Engineering and Technology, 40(January), 94-98. https://pdfs.semanticscholar.org/441e/a3bec73a5dd7ae8eff1e32ae3fd9521a1753.pdf

World Bank Group (WBG), the I. M. F. (IMF) and the O. E. C. and D. (OECD). (2017). The State of identification systems in Africa– a synthesis of country assessments. 1–68.

World Health Organisation. (2016). WHO recommendations. Intrapartum care for a positive childbirth experience. 200. http://apps.who.int/bookorders.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview - National Institute of Standards and Technology Internal Report 8202. NIST Interagency/Internal Report, 1–57.

Young, A., Winowatan, M., & Verhulst, S. (2018). Blockchange Case Study : Registering Births on the Blockchain in Illinois. Request for Information (RFI).” Department of Innovation and Technology, 2017. https://www2 .illinois.gov/ sites/doit/Documents /BlockchainInitiative/RFI Blockchainand Distributed Ledger Applications in the Public Sector.pdf October.

Yu, T., Lin, Z., & Tang, Q. (2018). Blockchain: The Introduction and Its Application in Financial Accounting. Journal of Corporate Accounting & Finance, 29(4), 37–47. https://doi.org/10.1002/jcaf.22365

Yusuf, L., Ayorinde, O., Ikoku, A. A., Identity, N., Commission, M., & Hosts, S. (2011). National Identity Management and Harmonization Committee National Identity Management System. August, 10–12. http://www.nimc.gov.ng/sites/default/ files/NIMS Strategy And Technology Overview Document_Final.Pdf

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2018). Blockchain Technology Use Cases in Healthcare. In Advances in Computers (1st ed., Vol. 111). Elsevier Inc. https://doi.org/10.1016/bs.adcom.2018.03.006

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, October, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

APPENDIX

```
// ************
// * Contract *
// ************
public class CertificateContract implements Contract {
   // This is used to identify our contract when building a transaction.
   public static final String CERTIFICATE_CONTRACT_ID =
      "com.template.contracts.CertificateContract";


   // A transaction is valid if the verify() function of the contract of all the transaction's
      input and output states
   // does not throw an exception.
   @Override
   public void verify(@NotNull final LedgerTransaction tx) throws
      IllegalArgumentException
 if (tx.getCommands().size() != 1) {
         throw new IllegalArgumentException("There can be only one command in a tx");
      }
      Command command = tx.getCommand(0);
      CommandData commandType = command.getValue();
      List<PublicKey> requiredSigners = command.getSigners();

      if (commandType instanceof CertificateRequest) {

//    Shape Rules

         if (tx.getInputStates().size() != 0) {
            throw new IllegalArgumentException("There cannot be input states in a
      CertificateRequest tx");
         }
         if (tx.getOutputStates().size() != 1) {
            throw new IllegalArgumentException("Only one loan can be disbursed in a tx");
         }
//    Content Rules

         ContractState outputState = tx.getOutput(0);
         if (!(outputState instanceof CertificateState)) {
            throw new IllegalArgumentException("Output state has to be of
      CertificateState");
         }
         CertificateState certificateState = (CertificateState) outputState;
         /*System.out.println("LoanType received: " + certificateState.getLoanType());
         if (!(certificateState.getLoanType().equals("Personal"))) {
```

```
            throw new IllegalArgumentException("Only Personal Loans can be applied by
        Fintech");
            }*/
//    Signer Rules

            PublicKey senderKey = certificateState.getSender().getOwningKey();

            if ((!requiredSigners.contains(senderKey))) {
                throw new IllegalArgumentException("Sender must sign the transaction");
            }
        }
    }

    // Used to indicate the transaction's intent.
    public static class CertificateRequest implements CommandData {
    }
}
// *************
// * Contract *
// *************
public class TemplateContract implements Contract {
    // This is used to identify our contract when building a transaction.
    public static final String ID = "com.template.contracts.TemplateContract";

    // A transaction is valid if the verify() function of the contract of all the transaction's
       input and output states
    // does not throw an exception.
    @Override
    public void verify(LedgerTransaction tx) {}

    // Used to indicate the transaction's intent.
    public interface Commands extends CommandData {
        class Action implements Commands {}
    }
}
// **********
// * State *
// **********
@BelongsToContract(CertificateContract.class)
public class CertificateState implements ContractState {
    private final String town;
    private final String state;
    private final String lga;
    private final String year;
    private final String name;
```

```
private final String sex;
private final String dob;
private final String fatherName;
private final String motherName;
private final String registrarName;
private final Party sender;
private final Party receiver;

public CertificateState(String town, String state, String lga, String year, String name,
    String sex, String dob, String fatherName, String motherName, String registrarName,
    Party sender, Party receiver) {
    this.town = town;
    this.state = state;
    this.lga = lga;
    this.year = year;
    this.name = name;
    this.sex = sex;
    this.dob = dob;
    this.fatherName = fatherName;
    this.motherName = motherName;
    this.registrarName = registrarName;
    this.sender = sender;
    this.receiver = receiver;
}


@Override
public List<AbstractParty> getParticipants() {
    return Arrays.asList(sender,receiver);
}

public String getTown() {
    return town;
}

public String getState() {
    return state;
}

public String getLga() {
    return lga;
}

public String getYear() {
    return year;
}
```

```
    public String getName() {
        return name;
    }

    public String getSex() {
        return sex;
    }

    public String getDob() {
        return dob;
    }

    public String getFatherName() {
        return fatherName;
    }

    public String getMotherName() {
        return motherName;
    }

    public String getRegistrarName() {
        return registrarName;
    }

    public Party getSender() {
        return sender;
    }

    public Party getReceiver() {
        return receiver;
    }
}
```