Information Technology and Management Science
ISSN 2255-9094 (online)
2021, vol. 24, pp. 26–32
https://doi.org/10.7250/itms-2021-0004
https://itms-journals.rtu.lv

1862
RIGA TECHNICAL UNIVERSITY

NFC-Blockchain Based COVID-19 Immunity Certificate: Proposed System and Emerging Issues

Fredrick Ishengoma*
The University of Dodoma, Dodoma, Tanzania

***Abstract* – Vaccine requirements are becoming more mandatory in several countries as public health experts and governments become more concerned about the COVID-19 pandemic and its variants. In the meantime, as the number of vaccine requirements grows, so does the counterfeiting of vaccination documents. Fake vaccination certificates are steadily growing, being sold online and on the dark web. Due to the nature of the COVID-19 pandemic, there is a need of robust authentication mechanisms that support touch-less technologies like Near Field Communication (NFC). Thus, in this paper, a blockchain-NFC based COVID-19 Digital Immunity Certificate (DIC) system is proposed. The vaccination data are first encrypted by the Advanced Encryption Standard (AES) algorithm on Hadoop Distributed File System (HDFS) and then uploaded to the blockchain. The proposed system is based on the amalgamation of NCF and blockchain technologies which can mitigate the issue of fake vaccination certificates. Furthermore, the emerging issues of employing the proposed system are discussed with future directions.**

***Keywords* – Blockchain technology, COVID-19, Digital Immunity Certificate, HDFS, NFC.**

I. Introduction

Governments around the world are implementing mass immunization programmes and with most countries vaccinating their citizens there appears to be hope at the end of the COVID-19 pandemic darkness [1], [2]. As governments and businesses are pondering how to safely restore in-person activities, Digital Immunity Certificates (DICs) are emerging as one of the solutions. These certificates are primarily meant to allow travellers to pass the ordinarily mandated testing and quarantining required to cross international borders. Thus, the employment of DICs have open up borders by recognising those that have already been vaccinated [3].

Since early April 2021, citizens in countries like Denmark, one of the first countries to issue the DIC, have been utilising the "Coronapas" to gain entrance to public places [4]. Estonia, which is recognised for being one of the most digitally advanced countries, uses a QR code linked to individuals' medical information to allow foreign travel [5]. Along the same line, the European Union (EU) has released open-source documentation outlining the proposed structure and technical details that would be utilised to create a standard and interoperable EU DIC [6].

In other countries, DICs are used to determine who can and who cannot engage in community gatherings and physical employment activities, especially those which involve a large number of people. However, on the other hand, DICs have encouraged counterfeit for financial gain and easy mobility within the country and abroad. With the advancement of imaging techniques, the falsification of immunity certificates is steadily growing [7]. Given the sensitive nature of the personal healthcare records in DICs, a more reliable and trustable mechanism is required. Thus, government authorities must have a system that is more robust against counterfeiting.

Blockchain technology is a technology that enables decentralized and transaction-based data sharing across a wide network of participants [8]. Recently, there has been growing research attention in BCT for transactions that involve untrusted participants and need significant security [9]. Integrating DIC with BCT introduces an additional layer of immutableness; thus, once data are entered in the blockchain, they cannot be manipulated.

Moreover, some of the DICs are implemented on a centralized database that has a single point of failure. In this paper, Hadoop Distributed File System (HDSF) lies as a baseline system working with BCT. When the HDFS receives data, it disintegrates the data into individual blocks and distributes them to the cluster nodes, which eliminate a Single Point of Failure (SPOF). Moreover, BCT has no SPOF due to its distributed and shared nature. Thus, the proposed system has two layers supporting availability and guarantees that there is no manipulation of data.

Additionally, with the emergence of COVID-19, there is a need for innovations that support touch-less technologies, thus making Near-Field Communication (NFC) popular in both research and society. NFC is a wireless data transfer technology that operates by detecting nearby NFC-enabled devices and communicating without the use of the Internet [10]. NFC, on the other hand, is not only a connectivity technology; it is also an enabler. It can be used to make mobile payments and provide secure access to buildings or public transit. In this paper, BCT and NFC are integrated with the aim of having a robust authentication system during this COVID-19 era. There are several studies which have proposed and implemented the blockchain and QR-code based DIC [21] – [26]. However, much has not been explored on the BCT-NFC-based DIC. This study proposes BCT-NFC based DIC.

* Corresponding author. E-mail: ishengomaf@gmail.com

The rest of the paper is organised as follows: Section 2 presents the related works. Section 3 describes the methodology used in the study. Section 4 discusses the proposed BCT-NFC DIC system while the emerging issues are considered in Section 5. Conclusions are listed in Section 6 followed by the References.

A. Hadoop Distributed File System (HDFS)

Hadoop Distributed File System (HDFS) is a distributed file system that enables high-speed access to application data. Data are stored in different locations, and in the incident that one storage location is unable to provide the data needed, the data can easily be obtained from another. HDFS is a master–slave data storage system. Each cluster is comprised of NameNodes, which serve as the master server, managing the file system namespace and granting appropriate access to clients. Two or more distinct machines are configured as NameNodes in a typical Hadoop cluster. At any given time, only one of the NameNodes is active, while the rest are in the standby state. The active NameNode is in charge of all client operations in the cluster, whereas the standby acts as a slave, retaining just enough state to allow for a quick failover, if necessary. The DataNode slaves are tasked with the responsibility of managing the storage associated with the node on which it runs. Additionally, the NameNode maps the blocks to DataNodes.

The DataNodes are constantly in communication with the NameNode to ascertain whether they are required to perform specific tasks. As a result, the NameNode is constantly informed of the status of each DataNode. If the NameNode notices that one of the DataNodes is not functioning properly, it can immediately reassign the task of that DataNode to another node that contains the same data block. Additionally, DataNodes communicate with one another, allowing them to work cooperatively during normal file operations.

B. Near Field File Communication

Near Field Communication or NFC facilitates short-range communication among compatible devices. This necessitates the use of at least one sending device and one receiving device [11]. It can be used by a variety of devices and is classified as either passive or active [12]. NFC offers three unique modes of operation to define what type of information will be transferred between devices. However, the peer-to-peer mode is the most prevalent application for smartphones, which permits two NFC-enabled devices to interchange various types of data [13].

NFC has risen in popularity since it runs on a specific frequency of 13.56 MHz, which has been standardized as a fast and secure mode of communication [14]. Unlike Bluetooth, NFC data transfer does not require human pairing or device discovery. Moreover, when compared to Bluetooth, NFC consumes significantly less power. Nevertheless, there are some downsides to this power-saving strategy, most notable, the transmission range is shorter than that of Bluetooth [15]. While NFC has a range of only a few inches (about 10 cm), Bluetooth connections can carry data up to 10 m or more from the source. When another NFC device enters the 4-inch range, an NFC connection is automatically established. As the two devices are in range, they quickly communicate and provide prompts to the user. The narrow radius of NFC is considered a big security benefit by researchers, and it is one of the reasons why it has become popular as a secure alternative technique. The key advantage of NFC over barcode and QR technologies, similar to RFID, is that it does not need a line of communication between the tag and the reader. The widespread use of NFC technology in applications demanding high degrees of security, such as electronic passports and "contactless" credit cards, demonstrates the trustworthiness of the solution.

The integration of NFC-based wireless power and data interchange with low-cost electronics and sensors has opened up a slew of novel sensing applications that were previously thought to be theoretically and economically impossible. In particular, NFC has the potential to fill a significant technological gap that cannot be fully resolved with other wireless technologies (such as Bluetooth and WiFi) [16].

C. Blockchain Technology

A distributed digital ledger of transactions is known as a blockchain whereby cryptographic techniques are used and ledger cannot be modified or manipulated. The blockchain is made up of interconnected blocks with a consensus algorithm to maintain immutability [17]. Since the blockchain network is administered by its nodes, there is no need for a single authority to create trust. As a result, to add a new block to the ledger, it must be distributed across the blockchain peer-to-peer network.

The primary characteristics of blockchain technology are as follows:

- *Decentralization.* Instead of being dependent on a single trusted source, data are distributed between multiple or all parties, based on the consensus algorithm. It means that not only are numerous copies of a data item saved on multiple nodes but also that the data integrity is overseen by several decentralized entities [18]. This overcomes the issue of a single point of failure that exists in centralized databases.
- *Immutability.* The information is saved persistently and immutably as data are recorded to the blockchain after a significant number of parties have consented. Modifying the data in one block would need modifying the data in all subsequent blocks up to the last one, which is regarded as unfeasible.
- *Scalability.* The block rate, which is made up of information throughput and propagation time, is determined by the consensus algorithm and the number of parties in the chain. For applications that demand high throughput, it can be a limiting factor. Since each node has a copy of the blockchain, there are scalability concerns about the overall quantity of data that can be kept. Moreover, a new node must download a copy of the blockchain and authenticate the integrity of the entire chain to check its integrity [19].
- *Privacy*. Every member of the blockchain has access to all of the data on the blockchain. The scope of the disclosure is limited to private or permissioned blockchains. Extra layers, such as zero-knowledge proofs or a commitment mechanism, are critical to attaining privacy.

To make a new block, one or more transactions are linked together and a node proposes this newly generated block to the network. The transactions in the block can be verified by other nodes in the network. There is a hash for each of these blocks. The hash is calculated using the information in the block and by adding the preceding block hash in a new block [20]. The blocks are connected in this manner. As a result, if anyone tampers with the prior block, the new hash generated will be inconsistent with the one in the subsequent block and the chain will be broken as a result of this discrepancy. Thus, hashing is used to guarantee that the blocks are not tampered with after they have been authenticated and put on the chain as depicted in Fig. 1.

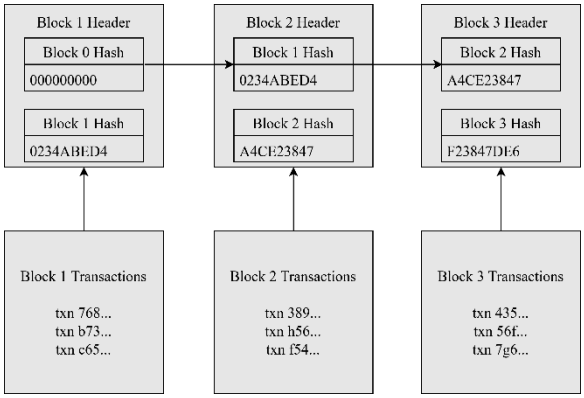


Fig. 1. Block chaining process.

When a block is accepted and registered, a cryptographic hash for that block is created, which is then included in the next block. Following the formation of the first block, every consecutive valid block must include the hash value of parent block header [20]. Every valid block is linked to the ones preceding it by the hash of the prior block header, which is included in every block. As a result, a chain of blocks (blockchain) is formed by connecting each block to the previous blocks.

D. NFC and BCT Integration

Integrating NFC and blockchain into a unified system mitigates the flaws of each technology separately. For instance, since blockchain functions only in the digital realm, an intermediary step is required to link physical items to the blockchain and all of its benefits. Physical things, locations, and markers can be translated into the digital realm via NFC tags. Likewise, because the NFC system requires close physical proximity to engage, the comparatively low range of NFC sensors prohibits interference from afar.

NFC tags, on the other hand, are vulnerable to duplication, manipulation, and other types of tampering. Blockchain interacts with the physical world through NFC tags, which blockchain verifies to identify and prevent tampering. While each of these technologies has been thoroughly investigated, the future possibilities and limitations of hybrid NFC-blockchain systems spark fresh innovations.

II. Related Works

The review of related work is presented in this section. The study [21] proposed blockchain-based COVID vaccination passport architectural framework (VacciFi) based on the EU General Data Protection Regulation (GDPR) while also considering recent developments, particularly in the EU. The suggested system employs a permissioned blockchain, which allows participating entities to operate in a more restricted environment. One limitation of this architecture is that it only stores vaccination data; nevertheless, in accordance with the EU recommendations, COVID passports should also be capable of storing negative COVID test results and information on how to recover from COVID infection in the event of a prior infection.

Another limitation in the proposed architecture is the right to be forgotten under the GDPR. This is a problem with the blockchain properties. Although blockchain can help with GDPR compliance, there is still a claim that it violates the GDPR Article 17 because data cannot be erased from the blockchain.

The study [22] allowed smart contracts based on the Ethereum blockchain to retain a digital medical identification for test-takers, making a quick and trusted response possible directly from the appropriate medical authorities. The proposed mechanism speeds up medical facility response times, limits the transmission of incorrect information with an immutable trusted blockchain, and has the potential to slow the spread of disease using digital medical certificates.

The [23] study proposes a mechanism that uses a two-factor authentication system and biometric cryptographic hashing methods to establish a unique identification for each user and stores COVID-19 immunization facts on a publicly available, decentralized, immutable blockchain. The mechanism uses an iris extraction method combined with a secure key input-hiding algorithm, a locality-sensitive hashing algorithm that can be used to authenticate users and anonymously locate immunization records on the blockchain without leakage of any personal identifying information.

The study [24] presented a blockchain-based medical data-sharing system. The system takes advantage of blockchain immutability and decentralization qualities to provide a secure, user-centric way of accessing and regulating sensitive medical data. The suggested system is based on a peer-to-peer network powered by the distributed InterPlanetary File System, on-chain tagging, and cryptographic generating techniques. To guarantee traceability and data integrity, the flow of information is managed by a smart contract implemented on a blockchain-based protocol. The framework usefulness is shown by the deployment of the framework in a pilot study.

A similar system has been proposed by [25] that presented a blockchain-based health passport system (BID-HCP) that assures that uninfected people can travel freely using a unified health certificate. Furthermore, the approach separates the user's location information from the user's identity, protecting the user's privacy while efficiently analysing the epidemic high-risk regions.

The study [26] has developed a framework that capitalizes on the permissioned blockchain features while maintaining

controlled sharing of confidential health records to display a patient's health status and COVID-19 history via a mobile QR code-based approach. The proposed architecture gives patients more control over their health records, with the healthcare service provider ensuring the data authenticity and immutability characteristic of the blockchain technology [26].

The authors of [27] address data tampering in cloud data storage by combining the IPFS and Ethereum networks. It eradicates the need to trust the cloud storage provider (CSSP), who acts as an authoritative figure with the power to modify or sell data for their own gain.

From the above literature, it is clear that most of the existing studies have proposed the use of BCT in DICs, while few have integrated QR codes and BCT. However, studies that have integrated BCT and NFC for dealing with counterfeit in DICs are still limited.

III. Research Methodology

This study is grounded on a design-based research methodology and the concept of mindful information technology use [27]. The most effective and cost-efficient characteristics of the technology are used to help solve problems with regard to the mindful use of technology. The design-oriented technique focuses on the engagement of researchers and practitioners to analyse real-world problems and provide a solution using the existing design concepts and technological breakthroughs. Following the requisite research and development, these systems are further upgraded before being deployed in the manufacturing environment as a solution to a specific problem [27].

This study aims at addressing the problem of verifying the authenticity of COVID-19 DICs when necessary. Traditional systems rely on conventional database technologies, which do not serve their intended function as there is a risk of single point of failure and offer minimal tracing to the originality of data. In addition, traditional databases lack a consensus mechanism, allowing an attacker or administrator to tamper with the data. The present research offers a new artefact based on the existing BCT and NFC technologies.

IV. BCT-NFC DIC System

Our system makes use of HDFS, a distributed file system, and distributes data across multiple nodes. Targeting each node on the system is extremely complicated, and decrypting vaccination data makes it even more challenging.

The proposed components in the system include the NCF enabled smartphone, NFC authenticating device, and HDFS. In the proposed system (Fig. 2), after the individual has received the vaccination, the vaccination data (V_{DT} – the date of vaccination, vaccination place, type of vaccination, any record of a disease that can interfere with vaccination, any complications, and individual ID, example, Citizen ID) are sent to the HDFS. HDFS encrypts the V_{DT} and stores the data in multiple nodes. These chunks of encrypted V_{DT} (EV_{DT}) are then recorded into the blockchain. The generated private key is sent back and stored in the citizen's NFC tag. In this system, NFC crypto-tag must be provisioned to make an NFC tag suitable for a blockchain use case. The tag will have a permanent connection to the blockchain after the provision. This can operate with a smartphone or a specialised NFC tag reader.

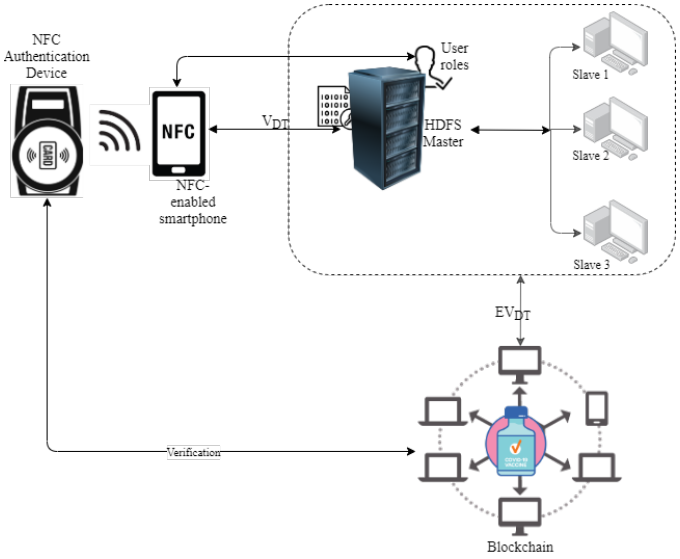
The NFC tag stores the private key that links to the blockchain data, allowing access to the vaccination data and verification process. This makes the authentication system tamper-proof and allows for robust vaccination verification right after vaccination.

The system uploads the vaccination data to the HDFS, which encrypts the data in order to maintain the system immutability. This stage renders vaccination data utterly worthless if it is ever acquired by a malicious attacker, as decrypting the data is extremely difficult. Encryption of vaccination data is performed "off-chain" to alleviate the system bottleneck. After encryption the data are then recorded in the blockchain. When the encrypted vaccination data are successfully stored, the server sends back a unique hash key.

Algorithm

```
Input: VD, CID, VHC,
Output: Encrypted VD (EVDT)
//VDT: Vaccination Data
//EVDT: Encrypted Vaccination Data
// CID: Citizen ID
// VHC: Vaccination Health Centre
//VD: Vaccination Date
//VR: Vaccination Region
//VT: Vaccination Type
//DN: Dose Number
//HS: Hadoop Server
//SC: Smart Contract
//TS: Transaction Status
1: for encrypting VDT do
2: Upload VDT to HS
3: HDFS encrypt VDT
4: HDFS returns EVDT
5: Record EVDT to SC (SCH)
6: Check TS
7: if Successful Transaction=True
8: Return Hash key
9: else
10: show error
11. end
12. end
```

Upon the verification process, the citizen's NFC enabled smartphone is paired with the server to cross-check the authenticity of the DIC using the hash-key. When the hash matches with the one in the server, the citizen is verified. Verification is performed in the system to determine whether vaccination data are already present and, if not, to add them. Additionally, this verification procedure can be used to determine whether vaccination data have been manipulated or are fraudulent. This can be done in the event of mass gathering events where immunity certification is significant, for instance, at the airport upon international travelling.



Nevertheless, a user role is required to enable authorised parties to make updates. Verification is required before the user is assigned a privileged position. As it is on the public blockchain, any participant, regardless of their role, can read the blockchain DIC data history without any special permission. The health institution that performed the immunization will have the privilege to register the vaccination data on the blockchain and update information about the status of vaccinations. For example, if an individual needs the second vaccination or booster, or had a record of complications with vaccinations, such information should be stored on the blockchain. Government agencies can have access to make remarks. It might be that a vaccination certificate was forged or stolen and could be recovered, or damage due to vandalism might have occurred.

V. Emerging Issues

A. NFC Issues

Since NFC lacks a security mechanism to protect its communication, vaccination information can be accessible in the open air. Thus, in an NFC connection, an eavesdropping attack is conceivable. An antenna positioned within 10 m of an operational NFC device can pick up the packets sent by that device. As a result, it opens the door to various security issues such as data corruption, data insertion, and man-in-the-middle attacks. An attacker with the right tools can eavesdrop on communication involving two NFC devices. Creating a secure connection between two NFC devices and utilising conventional encryption algorithms can safeguard against eavesdropping attacks. Establishing a shared secret key between two NFC devices could be accomplished by using RSA or elliptic curves. Nevertheless, since the hardware has constraints that delay transaction speed and add code complexity, this will raise overhead.

By utilising a jamming device that targets the NFC environment, a rogue actor can seek to make an NFC deceive or a reader inaccessible to its intended users via a Denial of Service (DoS) attack. The purpose of jamming is to prevent two NFC-enabled smartphones from communicating with the NFC-BCT device. An RFID jammer can send out a signal that disrupts communication and has the potential to damage transmitted data.

When the NFC device that connects to the blockchain takes longer to respond to the initial device, the attacker can perform a data insertion attack that introduces a message into the shared data between two NFC devices. The attack can only happen if the device has a latency that allows the attacker to inject data before the replying device. The data will be overrun and distorted if both the attacker and the replying device send the data at the same time. This problem can be solved not only by encryption but also by having the answering machine respond immediately.

B. BCT Issues

(1) *Data Privacy.* Blockchain technology is a viable tool for the transaction of sensitive data between untrusted parties. It is capable of processing health data and establishing a new ecosystem for health record exchange, with improved authenticity, reliability, privacy, security, and interoperability, and hence is particularly effective in the worldwide setting to prevent COVID-19 transmission. However, as data sharing is critical in the fight against COVID-19, people feel uncomfortable when their personal information is disclosed and misused. It is still up for debate if employers, airports, and entertainment and recreational facilities should have full access to vaccination data. Measures to ensure the security of these sensitive data from cyber-attacks are critical.

(2) *Blockchain Speed and Scalability.* One of the most significant technological challenges of the blockchain is scalability, particularly for public blockchains. The ability to process thousands of transactions per second is a hallmark of traditional transaction networks. Blockchains can be slow and inconvenient because of their complexity and encrypted distributed nature. Transactions can take a long time to complete, especially when compared to “conventional” payment methods like cash or debit cards. Visa, for instance, can process over 2000 transactions per second. However, when it comes to transaction speed, the two most popular blockchain networks, Bitcoin and Ethereum, are far behind. Transitions take longer to complete as the number of network participants grows. Thus, transaction costs are higher than usual, which limits the number of users on the network. Researchers are currently presenting an intriguing approach to the speed and scalability problem. One proposed solution, for example, is to build a second layer to the main blockchain network to allow for rapid transactions. Another intriguing idea is to divide subsets of nodes into smaller networks, each of which is accountable for its own set of transactions.

(3) *Blockchain Regulations.* There is a lack of legislative certainty surrounding the underlying blockchain technology, which impedes widespread use. Regulations have never been able to keep up with technological advancements. This is also true in the case of blockchain technology. Many businesses are

adopting the blockchain technology as a transactional tool. However, there are no clear regulations in place right now. As a result, when it comes to the blockchain, no one follows any regulations. Smart contracts, for example, need regulatory backing. If smart contracts are not covered by rules, adoption and investment in the blockchain business would be hampered.

(4) *Blockchain Carbon Footprint.* An additional issue with BCT is its high energy usage. The bulk of blockchains now on the market use a lot of power. The majority of blockchain technologies is based on bitcoin architecture and uses Proof of Work (PoW) as a consensus mechanism for transaction validation. Blockchain miners must solve complicated mathematics to utilise these protocols, and they demand a lot of processing power to validate and execute transactions, as well as secure the network. Meanwhile, the amount of energy wasted by machines competing to answer the mathematical challenge has surpassed all previous records.

C. BCT-NFC DIC Issues

(1) *Equity and Ethical Dilemmas.* The ethical issues that concern international bodies and ethicists are how to avoid prejudice when utilising a COVID-19 DIC to obtain services as well as travelling. Since many nations have not managed to vaccinate their whole population yet, the risk is substantial for ethnic minorities, immigrants, and those from economically disadvantaged categories, amongst many others. Thus, the introduction of DICs has been viewed as creating a "two-tiered society", aggravating inequities between vaccinated and unvaccinated people. The challenges of equity are both local in terms of racialized minorities, rural communities, and individuals with disabilities, as well as international in terms of low and medium-income countries' accessibility to vaccines.

(2) *Interoperability*. The introduction of DICs has raised the issue of mutual recognition. There are currently no established guidelines for the creation and operation of COVID-19 DICs nor interoperability standards. Since DIC programmes are decentralized, people may have to obtain multiple DIC applications to go about their regular lives. Various vaccination combinations have been approved and deployed in different countries. Some technology used in one country may not be recognised or accepted in another. Moreover, the same BCT-NFC DIC in one country can differ in an operating algorithm and system in another country, which poses a challenge in managing DICs under international consensus. The issue is that because there are so many different technologies in DICs, DICs are in a precarious situation due to a lack of common standards that would allow DIC-supporting technologies to interact with one another.

(3) *Integration with Traditional Systems.* As BCT and NFC are being introduced in the ecosystem, there is also the issue of how to integrate BCT-NFC DICs with traditional business operations and systems. In most cases, organisations must entirely reorganise their old system or devise a mechanism to successfully connect the technologies if they choose to employ BCF-NFC DICs. One issue is that corporations do not have access to the requisite pool of blockchain expertise to participate in this process due to a scarcity of trained developers. This difficulty can be resolved by relying on a third party. However, most alternatives on the market necessitate a major investment of time and money on the part of the company to achieve the transformation.

(4) *Database Updating.* The subject of how long vaccinations will protect against COVID-19 if booster injections are essential, and whether vaccines will need to be boosted to combat evolving viral types is currently under research. Thus, it is too early to predict how long COVID-19 vaccines will protect people and how many booster doses may be required in the future. This brings the issue of how long the BCT-NFC DIC needs to be active or last before being renewed. Thus, the government databases must not only keep track of the citizens' vaccination but also the vaccination boosters. This means that, whenever a citizen gets an additional booster, that data must be fed into the blockchain. Due to the type of vaccination in the market and the emerging one, keeping updated on the type of vaccine, their boosters (as they emerge) and the citizens' updates on the boosters might be a challenging task.

Figure 3 summarizes the emerging issues in NCT-NFC DIC system.

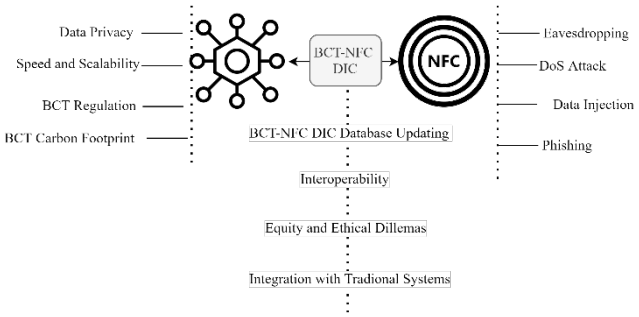


Fig. 3. Emerging issues in BCT-NFC DIC system.

VI. Conclusion

The paper has proposed a system based on NFC tags embedded in digital certificates to validate the COVID-19 vaccination backed by blockchain. The system is based on the HDFS, which first encrypts the vaccination data and then sends them to the multiple DataNodes. The vaccination data are then recorded in the blockchain. The integrated strengths of NFC and BCT enhance the DIC security and authenticity to an advanced level. With the proposed system, authorities can validate the vaccination of the citizen. As the data are recorded in the blockchain, the authenticity of the details is reliable. However, the potential benefits of the described system are accompanied by additional overheads and costs. NFC tags need to be integrated into every DIC, as well as an infrastructure should maintain user accounts, verify entities, and ensure that no user with special authorisations misuses the authority given. Yet, the viability of the proposed system has not been examined by the prototype implementation, and this remains an ongoing undertaking. One of the foreseen limitations of the proposed system is the possibility of lagging time due to the encryption process and recording data in the blockchain.

The paper has also presented emerging issues that can affect the adoption of the proposed system. These are NFC security issues, BCT issues and NFC-BCT issues. The study argues that more research is needed to explore the emerging issues such as interoperability, integration of BCT-NFC with traditional system approaches to mitigate BCT carbon footprint and lack of BCT regulations. In the light of this work, it is conceivable that the proposed BCF-NFC is a promising alternative to the existing systems in validating DICs in this era of the COVID-19 pandemic. Several interesting aspects are to be explored further in future research by the implementation of the proposed system.

REFERENCES

[1] W. R. Erdelen and J. G. Richardson, "A world after COVID-19: Business as usual, or building bolder and better?" *Global Policy*, vol. 12, pp.157–166, 2021. https://doi.org/10.1111/1758-5899.12904

[2] A. L Phelan, "COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges," *Lancet*, vol. 395, pp. 1595–1598, 2021. https://doi.org/10.1016/S0140-6736(20)31034-5

[3] T. Porat, R. Burnell, R. A. Calvo, E. Ford, P. Paudyal, W. L Baxter, and A. Parush. "Vaccine passports may backfire: Findings from a cross-sectional study in the UK and Israel on Willingness to get vaccinated against COVID-19," *Vaccines*, vol. 9(8), no. 902, Aug. 2021. https://doi.org/10.3390/vaccines9080902

[4] E-Estonia. The almighty QR code easing our travels. [Online]. Available: https://e-estonia.com/the-digital-green-certificate/ [Accessed: June 2021].

[5] I. E Agbehadji, B. O. Awuzie, and A. B Ngowi, "COVID-19 pandemic waves: 4IR technology utilisation in multi-sector economy," *Sustainability,* vol. 13, no. 18, p. 10168, Sept. 2021. https://doi.org/10.3390/su131810168

[6] S. Xie and H. Z. Tan, "An anti-counterfeiting architecture for traceability system based on modified two-level quick response codes," *Electronics*, vol. 10, no. 20, 2021. https://doi.org/10.3390/electronics10030320

[7] D. Kirilova, N. Maslov, and A. Reyn, "Blockchain as a new technology for development," *International Journal of Open Information Technologies,* vol. 7, no.1, 2021.

[8] M. M. Pryanikov and A. V. Chugunov, "Blockchain as the communication basis for the digital economy development: Advantages and problems," *International Journal of Open Information Technologies,* vol. 5, no. 6, 2017.

[9] V. Coskun, B. Ozdenizci, and K. Ok. "The survey on near field communication," *Sensors*, vol. 15, no. 6, pp. 13348–13405, 2015. https://doi.org/10.3390/s150613348

[10] P. Danny and C. Massimo, "NFC-based traceability in the food chain," *Sustainability*, vol. 9, no. 10, p. 1910, Oct. 2017. https://doi.org/10.3390/su9101910

[11] K. Fan, C. Zhang, K. Yang, H. Li, and Y. Yang, "Lightweight NFC protocol for privacy protection in mobile IoT," *Applied Sciences,* vol. 8, no. 12, p. 2506, Dec. 2018. https://doi.org/10.3390/app8122506

[12] C. Vedat, O. Kose, and O. Kerem."A survey on Near Field Communication (NFC) technology". *Wireless personal communications* vol. 71, no.3, 2013. https://doi.org/10.1007/s11277-012-0935-5.

[13] D. Silva-Pedroza, R. Marin-Calero, and G. Ramirez-Gonzalez, "NFC evaluation in the development of mobile applications for MICE in tourism", *Sustainability,* vol. 9, no. 11, p. 1937, Oct. 2017. https://doi.org/10.3390/su9111937

[14] C. Thammarat, "Efficient and secure NFC authentication for mobile payment ensuring fair exchange protocol," *Symmetry*, vol. 12, no. 10, p. 1649, Oct. 2020. https://doi.org/10.3390/sym12101649

[15] S. Olenik, H. S. Lee and F. Güder, "The future of near-field communication-based wireless sensing," *Nature Reviews Materials,* vol. 6, pp. 286–288, 2021. https://doi.org/10.1038/s41578-021-00299-8

[16] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education". *Smart Learning Environ*ments, vol. 5, no. 1, Jan. 2018. https://doi.org/10.1186/s40561-017-0050-x

[17] L. Liu, W. Zhang, and C. Han, "A survey for the application of blockchain technology in the media," *Peer-to-Peer Netw. Appl*., vol.14, pp. 3143–3165, 2021. https://doi.org/10.1007/s12083-021-01168-5

[18] H. T. M Gamage, H. D. Weerasinghe, and N. G. J Dias, "A survey on blockchain technology concepts, applications, and issues," *SN Computer Science,* vol. 1, no. 114, 2020. https://doi.org/10.1007/s42979-020-00123-0

[19] N. P Krylova and E. N. Levashov, "The prospects of the blockchain technology in the information society," *Autom. Doc. Math. Linguist.,* vol. 55, pp. 8–16, 2021. https://doi.org/10.3103/S0005105521010052

[20] A. Khatoon, "A blockchain-based smart contract system for healthcare management", *Electronics,* vol. 9, no. 1, p. 94, Jan. 2020. https://doi.org/10.3390/electronics9010094

[21] A. B. Haque, B. Naqvi, A. K. M. N. Islam, and S. Hyrynsalmi, "Towards a GDPR-compliant blockchain-based COVID vaccination passport," *Applied Science,* vol. 11, no. 13, p. 6132, Jul. 2021. https://doi.org/10.3390/app11136132

[22] H. R. Hasan et al., "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," in *IEEE Access*, vol. 8, 2020, pp. 222093–222108. https://doi.org/10.1109/ACCESS.2020.3043350

[23] K. Christodoulou, P. Christodoulou, Z. Zinonos, E. G. Carayannis, and S. A. Chatzichristofis, "Health information exchange with blockchain amid Covid-19-like pandemics," in *16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2020, pp. 412-417. https://doi.org/10.1109/DCOSS49796.2020.00071

[24] Y. Zhang, Y. Liu, and C. Chi, "BID-HCP: blockchain identifier based health certificate passport system," in *Lecture Notes in Computer Science,* vol. 12653, Cyberspace Safety and Security, Cheng J., Tang X., Liu X. (eds). Springer, Cham. https://doi.org/10.1007/978-3-030-73671-2_18

[25] A. S. Anjum, "A blockchain-based approach to prevent hidden contagion of Covid-19," *Compiler*, vol. 9, no. 2, pp. 71–84, 2020. https://doi.org/10.28989/compiler.v9i2.787

[26] J. Thatcher, R. Wright, H. Sun, T. Zagenczyk, and R. Klein, "Mindfulness in information technology use: Definitions, distinctions, and a new measure," *MIS Quarterly: Management Information Systems*, vol. 42, pp. 831–847, 2018. https://doi.org/10.25300/misq/2018/11881

[27] S. S.Hasan, N. H.Sultan, and F. A. Barbhuiya, "Cloud data provenance using IPFS and blockchain technology," in *Proceedings of the Seventh International Workshop on Security in Cloud Computing*, Auckland, New Zealand, 7–12 July 2019, pp. 5–12. https://doi.org/10.1145/3327962.3331457

Fredrick Ishengoma is a Lecturer at the University of Dodoma, College of Informatics and Virtual Education (CIVE), Department of Information Systems and Technology (IST). He holds a Master degree in Computer and Information Engineering (CIE) from Daegu University, South Korea, and a Bachelor degree in Information and Communication Technology Management (ICTM) from Mzumbe University, Tanzania. His research interests include blockchain technology, social dimensions of ICT, and ICT4D.
E-mail: ishengomaf@gmail.com