**qi23\_07:** Transparency, security and immutability of electoral process in Ghana using classical and quantum blockchain technology

**Authors**: Peter Nimbe, Emmanuel Adjei Domfeh, Tayyab Yahya, Emmanuel Tapany Junior, Isaac Batun, Nicodemus Songose Awarayi, Jacob Mensah, Yousra Ishraq, Richard Asiamah

**Abstract:** The electoral process in Ghana has been susceptible to errors as a result of many human elements, calculations, and non-vigilance from one level of the electoral process to another. In this project, we seek to design and implement a blockchain with quantum encryption for the parliamentary and presidential election results submission process in Ghana. Despite the potential applicability of blockchain technology in the whole electoral process, the primary focus of this project is on the election results submission after the close of polls. The objectives of the project include; (1) optimizing the results submission and collation process at the polling station, constituency, regional and national levels, and (2) ensuring the security and integrity of data, pink sheets, and other relevant documents using quantum cryptographic techniques.

**Keywords:** Quantum Blockchain, Electoral Process, Security, Transparency, Immutability, Integrity, Credibility

1. **Introduction**

**1.1 Quantum Blockchain Technology for National Elections Management**

Quantum blockchain technology represents a convergence of quantum computing and blockchain, holding the potential to revolutionize various sectors, including the critical area of national elections management. By combining the cryptographic security of blockchains with the computational power of quantum computers, quantum blockchain technology offers enhanced security, efficiency, and transparency for managing national elections (Azhar & Iqbal, 2019; Bonneau et al, 2015; Dang & Qin, 2020; Govindaraj & Prasad, 2019).

***1.1.1 Enhanced Security***:

Traditional blockchain systems rely on cryptographic methods that could be vulnerable to quantum attacks once large-scale, fault-tolerant quantum computers become available. Quantum blockchain technology employs quantum-resistant cryptographic algorithms, such as lattice-based cryptography, which are immune to quantum attacks. This ensures that the integrity of election data, voter information, and results remains intact (Azhar & Iqbal, 2019; Bonneau et al, 2015; Dang & Qin, 2020; Govindaraj & Prasad, 2019).

***1.1.2 Verifiable Voting***:

Quantum blockchain can enhance the transparency and verifiability of the voting process. Each vote cast can be recorded on a quantum blockchain, ensuring that once added, the information cannot be altered due to the inherent immutability of blockchain. Quantum entanglement can be used to create distributed, tamper-evident records of each vote, making it practically impossible to manipulate results without detection (Azhar & Iqbal, 2019; Bonneau et al, 2015; Dang & Qin, 2020; Govindaraj & Prasad, 2019).

***1.1.3. Privacy and Anonymity***:

Privacy in voting is a crucial aspect. Quantum blockchain can enable verifiable voting without compromising voter privacy. Quantum key distribution (QKD) protocols provide secure methods for distributing cryptographic keys, allowing voters to encrypt their ballots and verify their integrity while keeping their selections private (Azhar & Iqbal, 2019; Bonneau et al, 2015; Dang & Qin, 2020; Govindaraj & Prasad, 2019).

***1.1.4. Fraud Prevention***

Quantum blockchain can play a significant role in preventing voter fraud. By utilizing quantum entanglement for creating unique and non-replicable voter IDs or quantum signatures, the system can ensure that only valid voters participate and vote once, reducing the potential for fraudulent activities (Azhar & Iqbal, 2019; Bonneau et al, 2015; Dang & Qin, 2020; Govindaraj & Prasad, 2019).

***1.15. Decentralization and Trust***

Blockchain's decentralized nature can contribute to building trust in the election process. Quantum blockchain, with its robust security features, can further enhance trust by offering a system that is resistant to both classical and quantum attacks (Azhar & Iqbal, 2019; Bonneau et al, 2015; Dang & Qin, 2020; Govindaraj & Prasad, 2019).

**1.2 History of Ghana’s Elections During the Democratic Era**

The Fourth Republic of Ghana began in 1992 after a period of military rule. Since then, Ghana has held regular elections every four years, marked by the transition of power between different political parties. Ghana experienced its first multi-party elections in 1992 under the new constitution. The National Democratic Congress (NDC) and the New Patriotic Party (NPP) emerged as the major political parties (Ayee & Debrah, 2020; Gyimah-Boadi & Shapiro, 2008). Elections are the cornerstone of any democratic society, providing citizens with the opportunity to express their preferences and shape the future of their nation (Norris, 2014). In the Ghanaian context, elections have played a pivotal role in the country's democratic development since its independence in 1957 (Gaiman-Boadi, 2018). Over the years, Ghana has made significant strides in strengthening its electoral processes, but challenges persist in the collation, monitoring, and evaluation of election results (Gyimah-Boadi, 2018; Osei et al., 2020).

**1.3 Electoral Challenges and Issues**

The integrity of election results is crucial for maintaining public trust, ensuring political stability, and upholding democratic principles (Lehoucq & Molina, 2002). However, the Ghanaian electoral system faces several challenges that can undermine trust among stakeholders (Ansah, 2016). These challenges include issues related to transparency, accountability, and the potential for fraud or manipulation during the collation, monitoring, and evaluation of election results (Gyimah-Boadi, 2018; Osei et al., 2020). Therefore, there is a need to explore innovative solutions that can enhance the credibility of the electoral process and build trust among stakeholders (Arhinful & Wali, 2019).

While Ghana's elections have generally been viewed as peaceful and credible, several challenges and issues have been identified over the years:

***1.3.1 Voter Registration***

Concerns have been raised about the accuracy and inclusiveness of the voter registration process, including issues related to the verification of voters' identity and the potential for voter fraud (Debrah, 2018; Prempeh & Gyimah, 2008).

***1.3.2 Electoral Violence***

Incidents of violence, intimidation, and conflicts have been reported during elections, particularly at the local level. These incidents pose a threat to the integrity and fairness of the electoral process (Debrah, 2018; Prempeh & Gyimah, 2008).

***1.3.3 Media Coverage***

Some concerns have been raised regarding media bias and imbalanced coverage favoring certain political parties, which can influence voters' perceptions and choices (Debrah, 2018; Prempeh & Gyimah, 2008).

***1.3.4 Campaign Finance***

Transparency and accountability in campaign financing have been identified as areas where improvements are needed to prevent undue influence and ensure a level playing field (Debrah, 2018; Prempeh & Gyimah, 2008).

***1.3.5 Legal Tussles***

Legal tussles over the results of the 2012 and 2020 presidential elections signaled that some aspects of Ghana's electoral system are susceptible to problems (Debrah, 2018; Prempeh & Gyimah, 2008).

**1.4 Electoral Management and Administration**

The Electoral Commission of Ghana plays a crucial role in organizing and overseeing elections. However, there have been concerns and gaps related to the management and administration of elections:

***1.4.1 Independence and Impartiality***

The Electoral Commission's independence and impartiality have been questioned at times, leading to allegations of bias and lack of trust in the electoral process (Quashigah, 2014; Achoribo, 2018).

***1.4.2 Legal Framework***

Some critics argue that Ghana's electoral laws and regulations need further improvement to address emerging challenges, ensure transparency, and enhance the accountability of electoral institutions (Quashigah, 2014; Achoribo, 2018).

***1.4.3 Civic Education***

Limited civic education and voter awareness programs have been cited as a gap, potentially leading to voter apathy, inadequate understanding of electoral processes, and lower voter turnout (Quashigah, 2014; Achoribo, 2018).

***1.4.3 Features of Ghana’s Electoral System***

Over the years, Ghana has employed certain methods and rules of counting votes or collations at the polling station, regional and national levels to ensure transparency and credibility of the polls through the active work of the electoral commission. Currently the nation has two major types of elections; 1) Presidential and 2) Parliamentary.  In Ghana, the presidential election is held every four years to elect the President who is the head of state and the Commander in Chief of the Armed Forces through the Majoritarian System (Two-Round System) (Electoral Commission, 2023).

Ghana’s parliamentary election is a single-member constituency election held every four years to elect representatives to the National Assembly (Parliament). Members are elected using the ***First Past The Post*** (FPTP) system (Electoral Commission, 2023). Ghana’s Electoral System has the following features:

* Universal adult suffrage for citizens who are 18 years or older, continuous registration of voters
* Non-compulsory/voluntary participation in registration of electors and voting
* Where you register is where you vote
* Secret ballot
* Regulation of political parties by Electoral Commission (EC)
* Political parties as corporate entities
* Partisan politics at national level elections
* Non-partisan politics at local level elections
* Presidential and parliamentary elections held on the same day
* No minimum voter turnout required for presidential and parliamentary elections
* Presidential election requires the winner to obtain more than 50% of valid votes cast
* A run-off election is required in case no winner emerges on the first ballot in the presidential election
* Simple majority/First-past-the-post (FPTP) electoral formula determines the winner in the parliamentary election
* Permanent Election Management Body (EMB), EC (Electoral Commission, 2023)

**1. 4 Project Significance**

This project is very important as it contributes to national peace (trickling down to global peace), ensures transparency and good governance. In a peaceful society, there is a promise of sustained or continued growth of the economy. Specifically, it

* Ensures transparent, secure, and credible elections in Ghana
* Helps achieves Sustainable Development Goal (SDGs) established by the United Nations
  + SDG 9 – Industry, Innovation and Infrastructure
  + SDG 16 – Peace, Justice and Strong Institutions (United Nations, n.d.)

**1.5 Project Objectives**

In this project, we seek to propose a framework for a classical blockchain with quantum encryption for parliamentary and presidential election results submission process in Ghana. Despite the potential applicability of blockchain technology in the whole electoral process, the primary focus of this project is on the election results submission after close of polls.

* Optimizing the results submission and collation process at the polling station, constituency, regional and national levels
* Ensuring the transparency, security, integrity, credibility and immutability of data, pink sheets and other relevant documents.

1. **Method**

The project comprises of 4 major aspects:

* Blockchain for electoral results submission
  + Participants: *Polling Agents*, *Polling Assistants*, *Verification Officers*, *EC Officials*
* Quantum Encryption of data
* Data Compression of documents and files

**2.1 Blockchain for electoral results submission**

In the designing of the blockchain, the following tools are utilized

* Neutral blockchain technology known as Ethereum
* Solidity Programming Language for the blockchain development
* SDLC approach to system development (Planning, Defining, Designing, Building, Testing, Deployment)

**2.1.1 Election System Architecture**

The election system architecture consists of 2 principal parts; Frontend and Backend

***Frontend***: Comprises HTML, CSS and JavaScript web interface for data entry or input. This also serves as the layer where data retrieval is done as well as collated results.

***Backend***: Comprises the distributed database ledger where encrypted data and documents will be stored.

A framework of the frontend architecture with electoral information details is shown below in Figure 2.1.

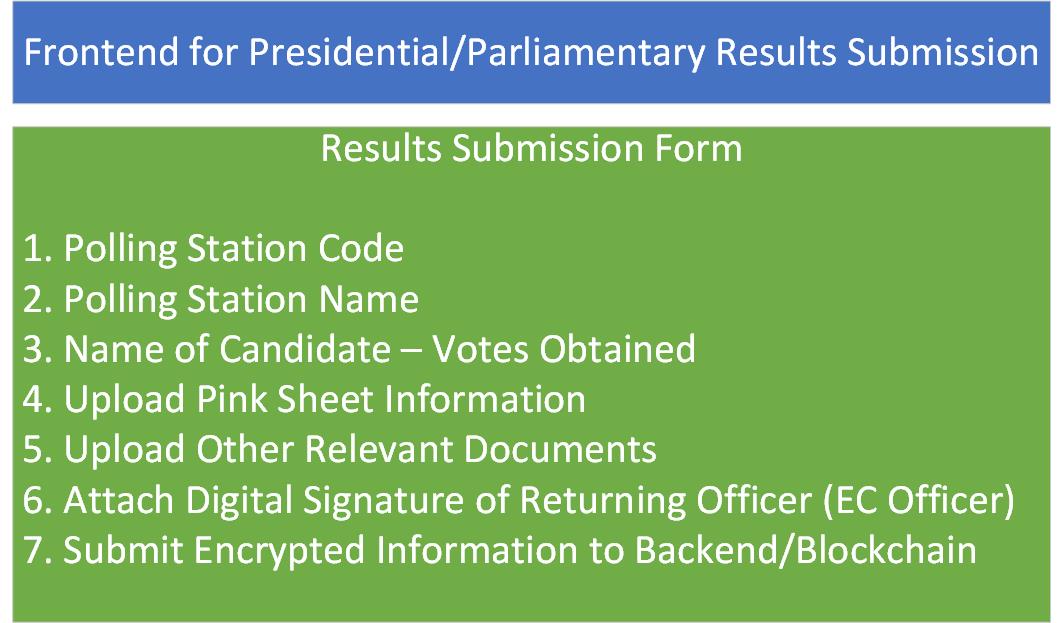


Figure 2.1: Frontend Architecture

After the encrypted data is submitted to the blockchain or backend, it can be queried so as to get results of the various candidates. Some actors or participants on the blockchain network also has Read-only access to the information in the blockchain as shown in Figure 2.2

A high-level view of the framework of the backend architecture (blockchain) is shown below in Figure 2.2

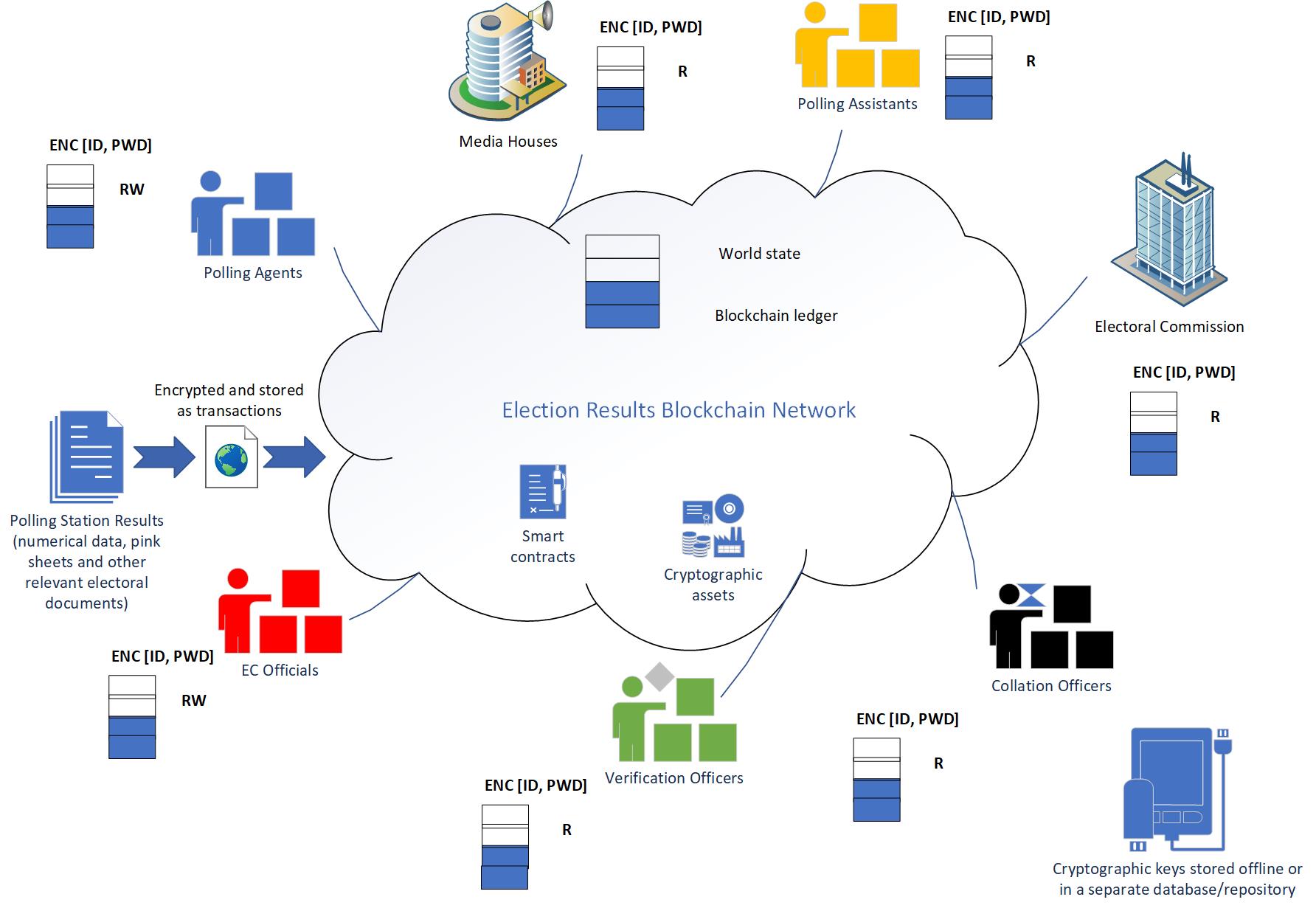


Figure 2.2: High-Level View of Backend Architecture

The blockchain transaction process is shown below in Figure 2.3

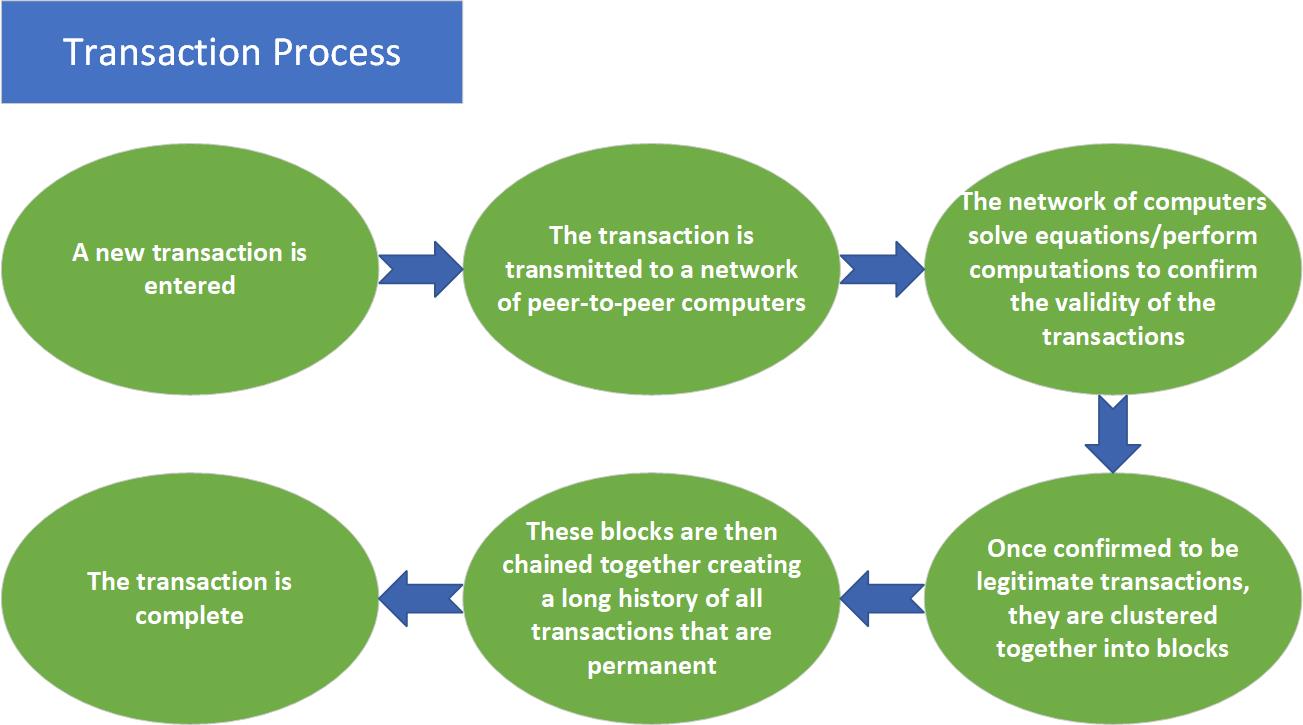


Figure 2.3: Blockchain Transaction Process

A low-level view of the framework of the backend architecture (blockchain) is shown below in Figure 2.4

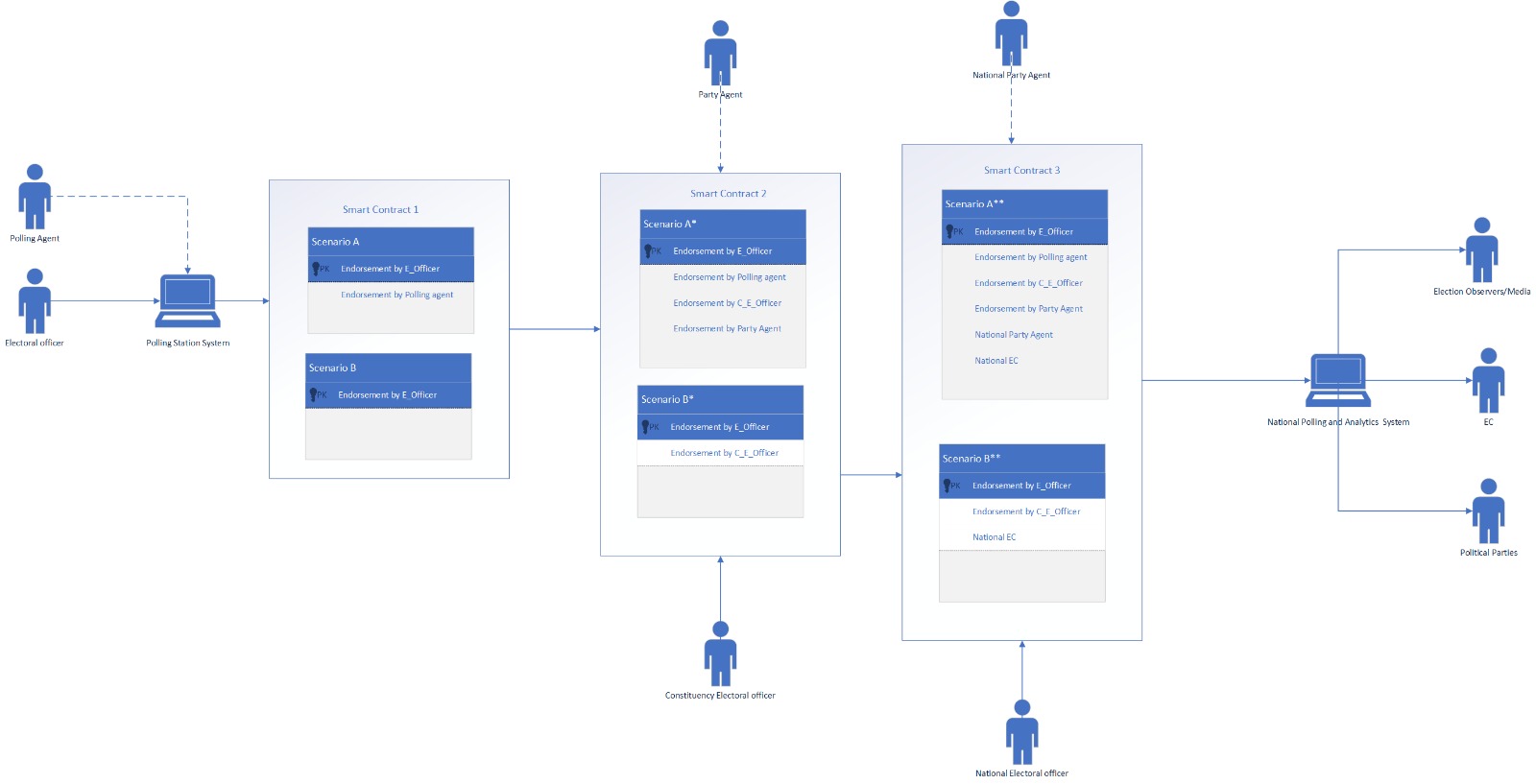
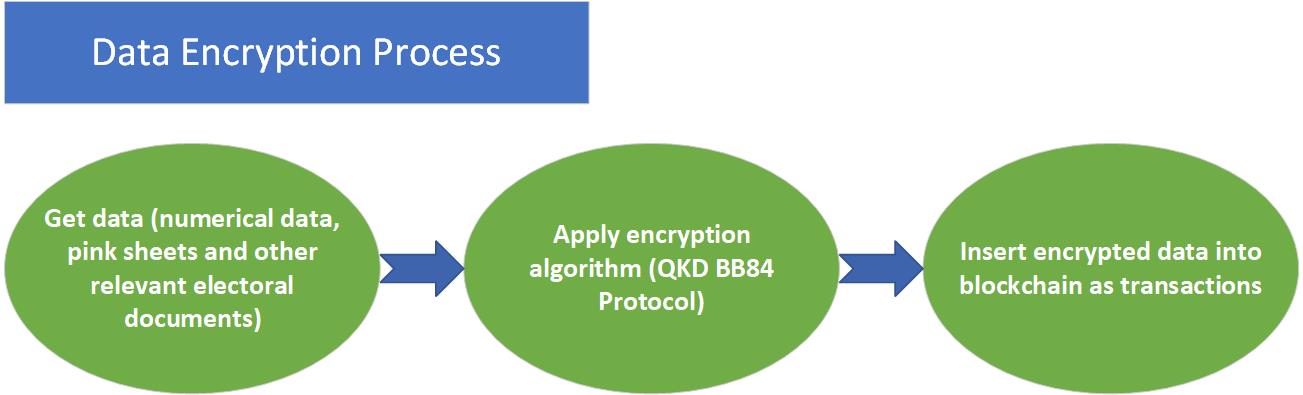


Figure 2.4: High-Level View of Backend Architecture

**2.2 Quantum Encryption and Decryption of data**

Pertaining to the data encryption and data compression of data, files and documents, the QKD BB84 protocol is utilized. The reason why the BB84 protocol has been adopted is because it is more resistant to quantum attacks. QKD uses entanglement, which is a quantum phenomenon that is very difficult to attack. QKD allows for the secure exchange of cryptographic keys, which can be used for subsequent encryption and decryption of voting data. QKD protocols can detect the presence of an eavesdropper attempting to intercept the quantum communication, ensuring the integrity of the voting process. QKD protocols are designed to be secure against quantum attacks, providing long-term security even with the advent of quantum computers. QKD protocols rely on the use of quantum randomness, ensuring the generation of secure cryptographic keys. QKD protocols have been successfully demonstrated over long distances, making it suitable for large-scale online voting systems. QKD protocols allow for the generation of cryptographic keys offline, reducing the risk of key compromise during the online voting process.



**2.3 Data Compression of documents and files**

Lempel Ziv universal lossless data compression algorithm created by Abraham Lempel and Jacob Ziv is used to reduce the file and image sizes in bits. The election documents or files include scanned copies of pink sheets, numerical data of presidential and parliamentary elections etc. before they are submitted into the blockchain network.

1. **Results**

**3.1 General Steps & Algorithms for Quantum Encryption (BB84 protocol)**

The general steps to implementing the BB84 protocol for encryption and decryption of electoral information using Qiskit:

* ***Implement the quantum operations***: Write code to prepare, encode, and measure qubits based on the BB84 protocol. This would involve creating quantum circuits for qubit preparation, encoding, and measurement.
* ***Implement error correction and privacy amplification***: Implement error correction codes (such as the binary repetition code or the bit-flip code) and privacy amplification techniques to correct errors and distill a secure final key.
* ***Integrate classical communication***: Set up a classical communication channel between Alice and Bob to exchange information about bases used and to perform error correction and privacy amplification.
* ***Implement encryption and decryption***: Once a secure key is generated, use standard cryptographic algorithms (such as AES, RSA, etc.) to encrypt and decrypt the text or files.

***3.2* Qiskit Code for IBM Quantum Experience Implementation of BB84 Protocol**

from qiskit import QuantumCircuit, Aer, execute

from qiskit.visualization import plot\_histogram

import random

# Function to create a random bit string of given length

def random\_bitstring(length):

return ''.join(str(random.randint(0, 1)) for \_ in range(length))

# Create a quantum circuit for BB84 protocol

def bb84\_circuit(bits):

n = len(bits)

qr = QuantumRegister(n, name='q')

cr = ClassicalRegister(n, name='c')

circuit = QuantumCircuit(qr, cr, name='BB84')

for i, bit in enumerate(bits):

if bit == '1':

circuit.x(qr[i])

# Apply Hadamard gate to create superposition

circuit.h(qr[i])

return circuit

# Simulate the BB84 protocol

def bb84\_protocol():

alice\_bits = random\_bitstring(10) # Alice generates random bits

circuit\_alice = bb84\_circuit(alice\_bits)

# Bob measures the qubits

bob\_basis = random\_bitstring(10)

circuit\_bob = bb84\_circuit(bob\_basis)

circuit\_bob.measure(circuit\_bob.qregs[0], circuit\_bob.cregs[0])

backend = Aer.get\_backend('qasm\_simulator')

shots = 1024

job = execute([circuit\_alice, circuit\_bob], backend=backend, shots=shots)

results = job.result().get\_counts()

return alice\_bits, bob\_basis, results

# Run the BB84 protocol

alice\_bits, bob\_basis, results = bb84\_protocol()

print("Alice's bits:", alice\_bits)

print("Bob's basis:", bob\_basis)

print("Measurement results:", results)

# Filter out the measurement results where Alice and Bob used different bases

filtered\_results = {key: val for key, val in results.items() if key[0] == key[1]}

print("Filtered results:", filtered\_results)

# Display histogram of the filtered results

plot\_histogram(filtered\_results)

NB: This code is not the complete code. This is just an aspect of the whole code.

**3.3 Algorithms for Data Compression (Lempel Ziv)**

Implementing a full Lempel-Ziv compression algorithm from scratch involves several steps, including reading and writing files, maintaining buffers, searching for repeated patterns, and encoding the output. Here's a basic Python implementation of the LZ77 compression algorithm for compressing files:

def lz77\_compress(input\_filename, output\_filename, window\_size, lookahead\_buffer\_size):

# Read the input data

with open(input\_filename, 'rb') as f:

input\_data = f.read()

compressed\_data = []

pos = 0

while pos < len(input\_data):

max\_length = min(lookahead\_buffer\_size, len(input\_data) - pos)

best\_match = (0, 0)

for length in range(1, max\_length + 1):

search\_start = max(0, pos - window\_size)

search\_end = pos

search\_window = input\_data[search\_start:search\_end]

candidate = input\_data[pos:pos + length]

match\_pos = search\_window.rfind(candidate)

if match\_pos != -1:

distance = pos - (search\_start + match\_pos)

best\_match = (distance, length)

compressed\_data.append(best\_match)

pos += best\_match[1]

# Write compressed data to the output file

with open(output\_filename, 'wb') as f:

for distance, length in compressed\_data:

f.write(bytes([distance, length]))

print("Compression completed.")

# Example usage

input\_filename = 'input.txt'

output\_filename = 'compressed.lz

**3.4 Comparison with Traditional Electoral Process**

The quantum blockchain approach offers decentralization, transparency, and security, which can improve the process for managing election results and increase trust. The traditional electoral process, on the other hand, is centralized and may have drawbacks in terms of speed, security, and openness. The decision between these strategies depends on a number of variables, such as technology preparedness, the regulatory landscape, and the requirement for increased confidence in the electoral process. The blockchain process optimizes the traditional process in that, there is no multiple results submission at various levels, hence a one-time submission and collation process. This reduces errors or mistakes that could potentially occur on the collation and multiple results submission processes. Nevertheless, it is without doubt that a quantum blockchain approach to elections result submission and management would significantly ensure transparency, fairness, credibility and immutability of the electoral process.

**4.0 Conclusion and Future Works**

The utilization of quantum blockchain technology for national elections management holds significant promise in addressing challenges related to security, transparency, and privacy. However, it's important to note that practical implementations and real-world applications of quantum blockchain are still in their early stages. This project is implementable and seeks to promote peace and innovation which are vital components of the Sustainable development goals established by the United Nations by aiding to conduct transparent and fair elections.

**References**

Achoribo, R. (2018). Electoral Reforms and Political Stability in Ghana. Journal of Political Sciences & Public Affairs, 6(3), 354.

Ayee, J. R. A., & Debrah, E. (Eds.). (2020). Election 2020 in Ghana: Democratic Consolidation or Stagnation? Friedrich-Ebert-Stiftung.

Azhar, S. M., & Iqbal, J. (2019). Quantum blockchain: A survey. Future Generation Computer Systems, 91, 641-658.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy (pp. 104-121). IEEE.

Dang, H., & Qin, S. J. (2020). Quantum Blockchain: A Comprehensive Review. IEEE Access, 8, 21966-21981.

Debrah, E. (2018). Political Financing in Ghana: Prospects and Challenges. Journal of African Elections, 17(2), 94-111.

Electoral Commission Ghana. (2023). Electoral System of Ghana. url: https://ec.gov.gh/electoral-system/

Govindaraj, T., & Prasad, S. (2019). A review on Quantum Blockchain. Journal of Physics: Conference Series, 1204(1), 012036.

Gyimah-Boadi, E., & Shapiro, I. (Eds.). (2008). Democracy in Ghana: The 1992 Elections. Oxford University Press.

Quashigah, E. T. (2014). The Electoral Commission and the Management of Elections in Ghana. Journal of African Elections, 13(1), 82-101.

Prempeh, H. K., & Gyimah-Boadi, E. (2008). The 2008 Elections and Prospects for Democratic Consolidation in Ghana. Journal of Democracy, 19(4), 103-117.

United Nations. What are the Sustainable Development Goals? (n.d). url: https://www.undp.org/sustainable-development-goals

Top of Form