Conference: 6th Asia Conference on Machine Learning and Computing (ACMLC 2024, in Bangkok, Thailand) (www.acmlc.org), April 2024

Web 3.0 and Quantum Security: A Long-Distance Free-Space and Implementation of QSDC for Global Web 3.0 Networks

Yew Kee Wong*
Hong Kong Chu Hai College
Hong Kong, China
yewkeewong.eric@gmail.com

Yifan Zhou*
BASIS International School Guangzhou
Guangzhou, China
yifan.zhou11882-bigz@basischina.com

Xinlin Zhou*
BASIS International School Guangzhou
Guangzhou, China
xinlin.zhou13495-bigz@basischina.com

Zi Yan Li*
BASIS International School Guangzhou
Guangzhou, China
ziyan.li11716-bigz@basischina.com

Yan Shing Liang*
BASIS International School Guangzhou
Guangzhou, China
yanshing.liang40486-bigz@basischina.com

***Abstract*—With the advent of Web 3.0, the swift advancement of technology confronts an imminent threat from quantum computing. Security protocols safeguarding the integrity of Web 2.0 and Web 3.0 are growing more susceptible to both quantum attacks and sophisticated classical threats. The article introduces long-distance free-space quantum secure direct communication (LDFS QSDC) as a method to safeguard against security breaches in both quantum and classical contexts. Differing from techniques like quantum key distribution (QKD), LDFS QSDC surpasses constraints by facilitating encrypted data transmission sans key exchanges, thus diminishing the inherent weaknesses of key-based systems. The distinctiveness of this attribute, coupled with its quantum mechanics base, protects against quantum computer assaults and advanced non-quantum dangers, harmonizing seamlessly with the untrustworthy tenets of the Web 3.0 age. The focus of our study is the incorporation of LDFS QSDC into network infrastructures, highlighting its efficacy for extended-range communication via memory DL04 protocol, quantum-aware low-density parity check (LDPC), and pointing, acquisition, and tracking (PAT) technologies. Utilizing this method not only bolsters the security of worldwide Web 3.0 networks but also guarantees their endurance in a time where quantum and sophisticated classical threats exist simultaneously. Consequently, LDFS QSDC stands out as a robust security solution, well-suited for Web 3.0 systems amidst the constantly evolving digital environment.**

***Index Terms*—Quantum Cryptography, Web 3.0, Quantum Secure Direct Communication, Long-Distance Free-Space Quantum Secure Direct Communication, Quantum Security**

I. Introduction

The emergence of the Web 3.0 era has brought about significant changes in the way we interact with the Internet and its applications. Web 3.0 is defined by a decentralized, distributed, and user-focused approach giving users control over their data, identity, and privacy. This also sets the stage for various economic exchanges, including direct transactions among peers, smart contracts, and digital assets.

In a globalized environment, the importance of security is paramount for networks, as diverse nodes and users can exhibit different degrees of reliability and risk elements. The use of methods such as public key encryption and digital signatures is crucial to maintaining the secrecy, reliability, and genuineness of network transactions and data.

Nonetheless, these techniques are vulnerable to risks posed by quantum computers, which utilize quantum mechanics principles to address issues more effectively than traditional computers. With quantum computers, the hazard to the security of networks stems from the potential to disrupt current cryptographic systems and jeopardize the integrity of data [1] [2]. Even though there has been quantum-proof cryptography proposed such as lattice-based cryptography, multivariate cryptography, and hash-based cryptography, these methods, although quantum-proof, have been decrypted by classical methods such as lattice reduction algorithms for certain lattice-based schemes [3], differential cryptanalysis for some multi-

*Yew Kee Wong, Yifan Zhou, Xinlin Zhou, Zi Yan Li, and Yan Shing Liang share co-first authorship to this work.

TABLE I
COMPARISON OF TYPES OF QUANTUM SECURE COMMUNICATION PROTOCOLS

Category	**Type of Protocol**			
	LDFS QSDC	***DL04 Protocol***	***Memory-Free DL04***	***QKD***
Communication Distance	**Long-distance (intercontinental)**	Moderate distance	Moderate distance	Short to moderate distance
Security Level	High (no key exchange required)	High (key exchange involved)	High (key exchange involved)	**Very high (key exchange fundamental)**
Implementation Complexity	**Moderate (enhanced by PAT technologies)**	High (requires quantum memory)	**Moderate (no quantum memory required)**	High (requires sophisticated setup)
Suitability for Globalized Web 3.0	**Highly suitable**	Moderately suitable	Moderately suitable	Less suitable for global scale
Atmospheric Disturbances Resistance	**Strong (mitigated by adaptive optics)**	Moderate (susceptible to some atmospheric effects)	Moderate (susceptible to some atmospheric effects)	Weak (highly susceptible to atmospheric effects)

variate cryptography systems [4], and collision attacks on certain hash functions [5].

The existence of these security LDFSaws demands the ongoing development of cryptographic techniques to maintain a lead over both quantum and classical potential attackers. One promising approach is to leverage quantum communication, which uses quantum states, such as photons, to transmit and process information [6] [7]. Quantum communication offers the advantages of unconditional security and high efficiency as compared to classical communications [8] [9] [10].

Quantum communication holds promise as a technology that can enhance the security and performance of networks in the Web 3.0 era. However, there is a pressing need for a new protocol that can overcome the challenges associated with long-distance free-space quantum communication to uphold the globalization of Web 3.0 networks. In this paper, we propose LDFS QSDC as a potential solution.

Quantum secure direct communication distinguishes itself from quantum communication techniques such as QKD by enabling direct data transmission, thus obviating the necessity for a central key exchange. This direct transmission approach reduces vulnerability points and enhances security, which is crucial given the decentralized and trustless nature of Web 3.0 networks [11] [12]. Moreover, QSDC's compatibility with long-distance free-space communication seamlessly aligns with the nature of safe and discrete transactions in Web 3.0.

With conventional QSDC methods being more suited for short distances or within fiber channels, adaptations are needed when applied on a larger scale to resolve signal loss and difficulties in transmitting through free space environments [13] [14]. This is especially important for applications that involve transactions happening over substantial distances. Therefore, when comparing LDFS QSDC with methods of quantum direct communication, it stands out for its ability to enable reliable quantum communication over long distances in free space environments [13] [14].

LDFS QSDC, based on memory-free DL04 protocol [15] and enhanced with Quantum-Aware LDPC [16] coding scheme and PAT technologies [17], addresses the limitations of signal loss and transmission difficulties. The DL04 protocol's memory-free nature reduces the complexity of quantum state storage and management, making the system more practical and robust for real-world applications [15]. The addition of PAT technologies and quantum-aware LDPC coding scheme mitigates issues related to atmospheric turbulence and alignment errors, which are prominent in free-space quantum communication [16] [18]. Combined, these technologies enable lossless and secure long-distance free-space communication in the era of Web 3.0 networks [19].

In this paper, we will also explore an integration plan of LDFS QSDC into Web 3.0 infrastructures to address quantum threats while aligning with the decentralized ethos of Web 3.0. The technical integration of LDFS QSDC with Web 3.0 requires a novel approach. Web 3.0 protocols would need to be adapted to accommodate the direct transmission capabilities of LDFS QSDC. The

integration entails altering the transaction verification methods of Web 3.0 to incorporate processes that align with LDFS QSDC's quantum-secured data. Furthermore, it's vital that the ledger is capable of documenting and harmonizing transactions secured by quantum technology. This necessitates not only advancements in quantum communication technologies but also developments in Web 3.0 architecture that can support such integration.

The main contributions of this article are summarized as follows:

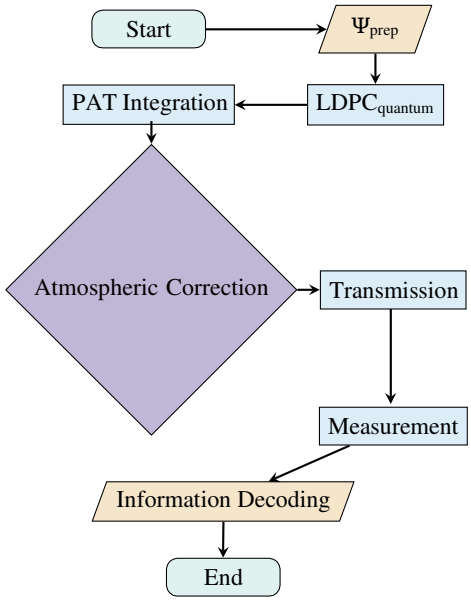
1) Introduction of a novel LDFS QSDC system designed for Web 3.0 networks.
2) Introduction of a detailed and practical roadmap to the implementation of LDFS QSDC into global communication networks.
3) Development and integration of Qauntum-Aware LDPC and PAT technology to enhance quantum communication reliability and efficiency.
4) Proposal of an Atmospheric Quantum Correction Algorithm (AQCA) aimed at mitigating atmospheric disturbances and improving security over long distances satellite communication.

We will first give an overview of our proposed LDFS QSDC system. Then, we will detail our innovative designs of Quantum-Aware LDPC, PAT Technologies, and Atmospheric Quantum Correction Algorithm. Finally, we will present our implementation plan for the LDFS QSDC and discuss the implications of our findings for global communication networks.

II. Long-Distance Free-Space QSDC Overview

This section introduces long-distance free-space quantum secure direct communication (QSDC), a sophisticated technique enabling secure data transfer across vast expanses in open space, eliminating the necessity for intermediary encryption key transmission. Our investigation delves into the ways in which advanced technologies can surmount existing constraints, rendering QSDC viable for widespread application both in the open air and across space through satellite communication. The following segment will elaborate on these advancements, emphasizing their capacity to transform secure communication worldwide.

Here is a LDFSowchart of LDFS QSDC:



The procedure begins with the preparation of the quantum state, indicating the initial step where quantum information is encoded for transmission. Following this, the process involves applying LDPC coding to enhance error correction capabilities, crucial for maintaining the integrity of quantum data over long distances. PAT technologies are integrated to ensure precise alignment and stabilization of the quantum signal, addressing challenges such as beam-wandering and atmospheric turbulence. An atmospheric correction step is then applied to mitigate effects like scattering and absorption that can degrade the quantum signal as it traverses the atmosphere. The corrected signal undergoes transmission, where it is sent across free space, potentially covering vast distances including satellite-to-ground communication paths. Upon reaching the destination, the quantum signal is measured—a critical phase where the encoded quantum information is detected and interpreted. Finally, the process concludes with information decoding, where the quantum data is translated back into classical information for use, marking the end of the LDFS QSDC transmission cycle. This systematic approach encapsulates the advanced technologies and strategies employed to overcome existing limitations of quantum communication, showcasing the potential for secure, direct data transfer across significant distances without the need for intermediary encryption keys.

A. State Preparation

The sender, Alice, prepares a sequence of single photons in one of the four time-bin states:

$$|T_0\rangle = |0\rangle, \quad |T_1\rangle = |1\rangle, \quad |T_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |T_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{1}$$

where $|0\rangle$ and $|1\rangle$ denote the early and late time bins, respectively [7]. Alice randomly chooses two bits, a_0 and a_1, to encode each photon. The encoding rule is as follows [20]:

$$(a_0, a_1) \rightarrow \begin{cases} |T_0\rangle, & \text{if } (a_0, a_1) = (0, 0), \\ |T_1\rangle, & \text{if } (a_0, a_1) = (0, 1), \\ |T_2\rangle, & \text{if } (a_0, a_1) = (1, 0), \\ |T_3\rangle, & \text{if } (a_0, a_1) = (1, 1). \end{cases} \quad (2)$$

Alice also randomly chooses another bit, a_2, to determine the phase of each photon. The phase modulation rule is as follows [11]:

$$a_2 \rightarrow \begin{cases} \phi = 0, & \text{if } a_2 = 0, \\ \phi = \pi, & \text{if } a_2 = 1. \end{cases} \quad (3)$$

Alice applies a phase modulator (PM) to each photon according to the value of a_2. The PM shifts the phase of the late time bin by ϕ, resulting in the following four phase states [11]:

$$|P_0\rangle = |0\rangle, \quad |P_1\rangle = |1\rangle, \quad |P_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle), \quad |P_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\phi}|1\rangle). \quad (4)$$

The phase states are related to the time-bin states by the following transformation [13]:

$$|P_i\rangle = \frac{1}{\sqrt{2}}(|T_i\rangle + e^{i\phi}|T_{i\oplus 2}\rangle), \quad (5)$$

where $\oplus$ denotes addition modulo 4. Alice records the values of a_0, a_1, and a_2 for each photon, and sends the photons to the receiver, Bob, through a free-space channel.

B. State Transmission

Photons traverse the free-space passage, leading to a range of disruptions including atmospheric disturbances, beam drift, scintillation, and ambient noise. Such disruptions impact the consistency and accuracy of quantum states, potentially leading to inaccuracies or losses in transmission. LDFS QSDC tackles these obstacles by utilizing a quantum-aware LDPC coding system, merging PAT technologies, and integrating an atmospheric quantum correction algorithm. In a research paper context, expanding on the techniques for long-distance free-space quantum secure direct communication with a focus on their synergy and suitability for Web 3.0 security:

1) Quantum-Aware LDPC: The LDPC coding system, represented by $\mathbf{x} = \mathbf{Hy} + \mathbf{n}$, where $\mathbf{H}$ is the parity-check matrix, plays a pivotal role in correcting errors inherent in quantum communication. This system is crucial for ensuring the integrity of each transaction in the Web 3.0 era [16].
2) PAT Technologies: PAT technologies align quantum signals and maintain a stable communication link, ensuring the continuous operation of decentralized Web 3.0 networks [17].
3) Atmospheric Quantum Correction Algorithms: These algorithms address disturbances like turbulence ($\Delta\Phi_{turbulence}$) to ensure the reliability of long-distance transmissions crucial for global Web 3.0 networks [6].

This combination of schemes and algorithms ensures a secure, reliable, and efficient quantum communication system, adhering to the requirements of the Web 3.0 era. The paper will proceed to discuss the design and integration of these methods in detail in the next section.

C. State Measurement

Bob receives the photons from Alice and measures them using an interferometer and a single-photon detector (SPD). The interferometer consists of a beam splitter (BS), two PMs, and two mirrors (M). The BS splits each photon into two paths, corresponding to the early and late time bins. The PMs shift the phases of the two paths by ϑ and $\vartheta + \pi$, respectively. The mirrors reLDFSect the photons to the BS, where they recombine and interfere. The SPD detects the photons at the output port of the BS.

The measurement outcome depends on the phase state of the photon and the phase difference ϑ between the two paths. The probability of detecting a photon at the output port is given by

$$P(\vartheta) = \frac{1}{2}(1 + \cos(\phi - 2\vartheta)), \quad (6)$$

where ϕ is the phase of the photon [20]. Bob randomly chooses the value of ϑ for each photon and records the detection results. Bob then announces the values of ϑ publicly and discards the results that correspond to $\vartheta = \frac{\pi}{4}$ or $\vartheta = \frac{3\pi}{4}$, since these values do not provide any information about the phase of the photon.

D. Information Extraction

Alice and Bob extract the information from the transmitted and measured photons, using the following steps:

1) Alice and Bob perform sifting, where they compare the values of a_2 and ϑ, and keep only the results that satisfy $a_2 \oplus \vartheta = 0$ or $a_2 \oplus \vartheta = 1$. This ensures that Bob's measurement basis is aligned with Alice's encoding basis and that the phase information is preserved [7].
2) Alice and Bob perform error correction, where they apply the error-correcting codes to correct the bit errors and phase errors in the sifted data. They also perform privacy amplification, applying a hash function to reduce the information leakage to Eve [22].

3) Alice and Bob perform information reconciliation, where they compare the values of a_0 and a_1, and extract the common bits as the final secret message. They also perform authentication, where they verify the integrity of the message using a secret key shared beforehand [23].

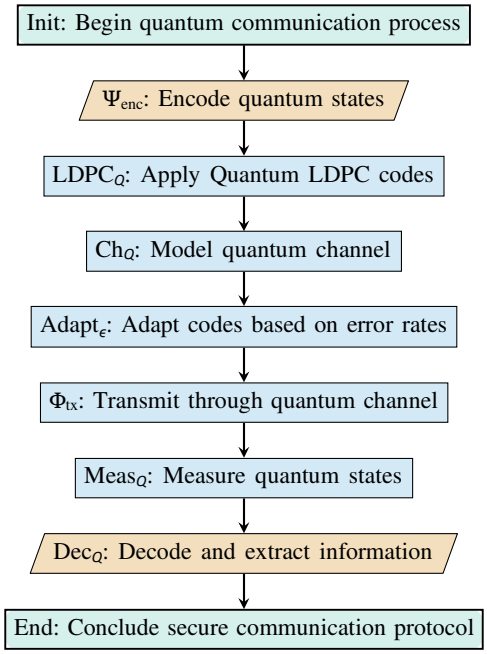
The LDFS QSDC protocol enables protected and immediate communication across extensive distances and open-air channels, eliminating the necessity for quantum memory or repeaters. LDFS QSDC's foundation, memory-free QSDC, has been experimentally demonstrated over a 19-km urban atmospheric channel and has the potential to be extended to satellite-based QSDC in the future [15].

III. Lossless and Secure Long-Distance Free-Space Transmission Techniques

This section delves into innovative techniques for the secure and loss-free transmission of data over extensive distances via air or space. The focus is on technologies that guarantee the transmission of data from one location to another remains unaltered and completely confidential, notwithstanding the hurdles of geographical separation and possible disruptions. Future dialogues will explore creative approaches that render forward-looking communication both practical and dependable.

A. Quantum-Aware LDPC Coding

In this subsection, we introduce an advanced error correction method that is vital for preserving the integrity of quantum communication across extensive distances. In this part, we describe the adaptation of low-density parity-check (LDPC) codes for quantum applications, outlining their architecture, execution, and advantages. Fundamental ideas involve modifying traditional LDPC codes for use in quantum protocols and improving error rectification while maintaining the security and consistency of quantum data. Key phases include developing LDPC codes resistant to quantum disturbances, fine-tuning them for quantum pathways, and amalgamating them into quantum communication frameworks to guarantee strong, protected transmission.



The LDFSowchart outlines the process of incorporating quantum-aware LDPC coding into a quantum communication protocol to ensure secure and reliable transmission of quantum information over long distances. The process begins with the initiation phase, marking the start of the quantum communication process. The next step involves encoding quantum states to prepare them for transmission. Following this preparation, quantum LDPC codes are applied to these quantum states to enhance error correction capabilities, crucial for mitigating errors that might occur during transmission through a quantum channel. The protocol then dynamically adapts these codes based on observed error rates, optimizing them for the specific characteristics of the quantum channel. Once the quantum states are encoded and the LDPC codes are optimized, the states are transmitted through the quantum channel. Upon reaching their destination, the quantum states are measured, and the encoded information is extracted through a decoding process, concluding with the secure communication protocol. This systematic approach ensures the integrity and security of quantum data, leveraging advanced error correction methods to maintain high fidelity in quantum communications.

1) Channel and Measurement Model: Outlining the mathematical models used to describe the behavior and challenges of quantum communication channels and measurement processes.

Quantum Channel Model:

- Let P_{loss} represent the probability of photon loss in the quantum channel.
- Dark count probability is denoted as P_{dark}.
- Quantum Bit Error Rate (QBER) is represented by $QBER$.

- The quantum channel can be modeled as [6]:

$$C_Q = \alpha \cdot P_{loss} + \beta \cdot P_{dark} + \gamma \cdot QBER \quad (7)$$

where α, β, γ are weighting factors for each component.

Quantum Measurement Model:

- Measurements in quantum communication are subject to basis mismatch and detector inefficiencies.
- Let $P_{mismatch}$ denote the probability of basis mismatch.
- The effective measurement model, M_Q, can be expressed as [24]:

$$M_Q = (1 - P_{mismatch}) \cdot (\text{Detector Efficiency}) \quad (8)$$

2) LDPC Code Parameter Optimization: Explores the optimization of LDPC codes for quantum communication, aiming to improve error correction and data integrity by refining degree distribution and introducing an optimization strategy for minimizing QBER. Discusses dynamic channel adaptation through machine learning, allowing for real-time adjustments to enhance the reliability of quantum communication systems.

Degree Distribution Optimization:

- *Extended Definition and Impact:* The degree distribution of an LDPC code, represented by the polynomials $\lambda(x)$ for variable nodes and $\rho(x)$ for check nodes, fundamentally determines the code's performance in terms of error correction efficiency and rate. These polynomials dictate how bits are interconnected within the LDPC graph.
- *Technical Enhancement:* A more comprehensive optimization function that not only maximizes mutual information I(X; Y) and minimizes QBER but also considers the decoding threshold and the code rate. The optimization can integrate more complex constraints related to the noise model of the quantum channel.
- *New Mathematical Formulation:*
  Optimization Goal:

$$\max \; I(X;Y) - \lambda(\text{QBER}) - \delta(\text{Code Rate}) \quad (9)$$

Subject to:

$$\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}, \quad \rho(x) = \sum_{i=2}^{d_c} \rho_i x^{i-1} \quad (10)$$

Here, δ represents the additional constraint related to the code rate.

Channel Adaptation:

- *Machine Learning Prediction and Iterative Update Algorithm:* A dynamic adaptation mechanism in which LDPC codes adjust to the present state of the channel and also forecast outcomes based on the patterns of channel behavior. In this proposal, we introduce machine learning and an iterative update algorithm designed to predict upcoming alterations in the quantum channel and modify the LDPC code parameters, guided by immediate feedback from the quantum communication system.
  1) Initialization: Set initial LDPC code parameters based on average channel conditions.
  2) Real-time Feedback Loop:
     * Collect real-time CQ data.
     * Adjust LDPC parameters for immediate channel conditions.
  3) Predictive Adjustment:
     * Use the ML model to predict short-term future CQ.
     * Preemptively adjust LDPC parameters based on predictions.
  4) Iterative Update:
     * Continuously repeat steps 2 and 3.
     * Employ a decay factor to balance between recent adjustments and new predictions.
- *Mathematical Representation:*
  - Let P_t represent LDPC parameters at time t.
  - $CQ_{real}(t)$ and $CQ_{pred}(t+1)$ represent real-time and predicted CQ metrics.
  - Update function:

$$P_{t+1} = f(P_t, CQ_{real}(t), CQ_{pred}(t+1)) \quad (11)$$

  - Where f is a function that calculates new parameters considering both current and predicted CQ [25].
- *Pseudocode:*

```
import numpy as np
from keras.models import Sequential
from keras.layers import LSTM, Dense

# LSTM Model for Channel Prediction
def build_lstm_model(input_shape):
model = Sequential()
model.add(LSTM(50, return_sequences=True,
    input_shape=input_shape))
model.add(LSTM(50))
model.add(Dense(1))
model.compile(optimizer='adam', loss='mse')
return model


# Update LDPC Parameters
def update_ldpc_parameters(current_params,
    current_cq, predicted_cq):
# Algorithm to update LDPC parameters based
    on current and predicted CQ
# Example: Adjust code rate based on SNR
snr_threshold = 10
if current_cq['SNR'] < snr_threshold or
    predicted_cq['SNR'] < snr_threshold:
new_params = adjust_code_rate(current_params,
    decrease=True)
```

```
else:
new_params = adjust_code_rate(current_params,
    decrease=False)
return new_params

# Main Loop for Iterative Update
def iterative_update_loop(initial_params,
    model, channel_data):
params = initial_params
for t in range(len(channel_data)-1):
current_cq = get_current_cq(channel_data, t)
predicted_cq =
    model.predict(channel_data[t:t+1])
params = update_ldpc_parameters(params,
    current_cq, predicted_cq)
# Update the LDPC codes with new params
return params
```

3) Adaptive Decoding Algorithm with Graph Neural Network Enhanced Belief Propagation and Adaptive Iteration: Introduces a GNN-enhanced adaptive decoding algorithm for quantum communication, improving LDPC code decoding by adapting to channel changes and enhancing security with decoy states for eavesdropping detection and privacy amplification methods to secure final keys, significantly increasing transmission reliability and protection.

Standard BP Equation [25]:

$$m_{i\to j}^{(t+1)} = 2\tanh^{-1}\left(\prod_{k\in N(i)\setminus j}\tanh\left(\frac{m_{k\to i}^{(t)}}{2}\right)\right) \quad (12)$$

Modification with GNN:
Adjust messages $m_{i\to j}^{(t)}$ using a GNN. The GNN predicts the likelihood of error in each node's message, inLDFSuencing the BP update rule.

GNN Model Design:

- Input: Messages from each node, current iteration number, and additional features like channel conditions.
- Architecture: Utilize a GNN architecture capable of handling graph-structured data. Layers can include Graph Convolutional Networks (GCN) or Graph Attention Networks (GAT).
- Output: Adjusted messages and probability of error for each node.

Adaptive Iteration:

- Dynamically Adjust Iterations: Based on channel conditions and convergence rate, the number of iterations, T, is adapted.
- Stopping Criterion: Utilize error patterns and rate of convergence to determine when to stop the iterations.

Mathematical Representation:

- Let $m_{i\_j}^{(t)}$ be the message from node i to node j at iteration t.
- GNN output inLDFSuences the update rule:

$$m_{i\to j}^{(t+1)} = GNN(m_{i\to j}^{(t)}, \text{features})$$

- Adaptive iteration count T based on GNN feedback and channel conditions.

Pseudocode:

```
import torch
import torch.nn as nn
import torch.nn.functional as F
from torch_geometric.nn import GCNConv, GATConv

class GNNModel(nn.Module):
    """
    Define GNN model structure for enhancing BP
        decoding.
    Can use either GCN or GAT layers based on
        architecture choice.
    """
    def___init__(self, input_dim, hidden_dim,
        output_dim):
        super(GNNModel, self).__init__()
        # Example with GCN layers, can be
            replaced with GAT for attention
            mechanism
        self.conv1 = GCNConv(input_dim,
            hidden_dim)
        self.conv2 = GCNConv(hidden_dim,
            output_dim)

    def forward(self, x, edge_index):
        # x represents node features, edge_index
            represents graph structure
        x = F.relu(self.conv1(x, edge_index))
        x = self.conv2(x, edge_index)
        return x

def enhanced_bp(messages, gnn_model, edge_index,
    num_iterations):
    """
    Enhanced BP using GNN for adjusting messages.
    Iteratively updates messages based on GNN
        predictions.
    """
    for t in range(num_iterations):
        # Convert messages to tensor for GNN input
        messages_tensor = torch.tensor(messages,
            dtype=torch.LDFSoat)
        # Update messages using GNN output
        adjusted_messages =
            gnn_model(messages_tensor, edge_index)
        # Convert adjusted messages back to numpy
            array for next iteration
        messages =
            adjusted_messages.detach().numpy()
    return messages

def adaptive_decoding_algorithm(messages,
    channel_conditions, edge_index):
    """
    Main decoding function that uses adaptive
        iteration based on channel conditions.
    Utilizes GNN model to adjust messages and
        improve decoding.
    """
    # Initialize GNN model
```

```
    input_dim = messages.shape[1]  # Assuming
        messages is a 2D array: num_nodes x
        message_dim
    hidden_dim = 64  # Example hidden dimension
    output_dim = input_dim  # Output dimension
        matches input for message adjustment
    gnn_model = GNNModel(input_dim, hidden_dim,
        output_dim)

    # Determine the number of iterations based on
        channel conditions
    T = determine_iterations(channel_conditions)

    # Perform enhanced BP with adaptive iterations
    adjusted_messages = enhanced_bp(messages,
        gnn_model, edge_index, T)

    # Decode the adjusted messages to extract
        information
    decoded_info = decode(adjusted_messages)
    return decoded_info

def determine_iterations(channel_conditions):
    """
    Determine the number of iterations for BP
        based on channel conditions.
    Placeholder function - implement logic based
        on specific channel conditions.
    """
    # Example: adjust iterations based on SNR or
        QBER thresholds
    if channel_conditions['SNR'] > 10:
        return 10  # Fewer iterations for high SNR
    else:
        return 20  # More iterations for low SNR

# Example usage
# Assuming 'messages' is a numpy array of
    messages, 'channel_conditions' is a dict
# containing channel condition metrics, and
    'edge_index' is a tensor defining graph
    structure
# decoded_info =
    adaptive_decoding_algorithm(messages,
    channel_conditions, edge_index)
```

4) Security Enhancement Techniques: Discusses enhancing quantum communication security through the decoy state method, which estimates channel parameters and detects eavesdropping by analyzing detection rates, and privacy amplification, which secures the decoded key by applying a hash function to reduce its length based on QBER and eavesdropping risks.

Decoy State Method:

- Employ decoy states with varying intensities to estimate channel parameters.
- Use statistical methods to analyze the difference in detection rates between signal and decoy states to estimate P_{loss} and detect eavesdropping.
- The estimation can be formulated as solving a set of linear inequalities derived from decoy state intensities and detection rates [20]. The general form of these linear inequalities can be represented as follows:

For a set of decoy states with different intensities μ_i (where i indexes the different decoy states), and corresponding detection rates Y_i, the inequalities can be structured to estimate the parameters like photon loss (P_{loss}) and single-photon detection rates Y_1. The estimation typically aims to bind the yield of the single-photon states Y_1 and the quantum bit error rate (QBER) for single-photon states.

The set of inequalities:

1) $Y_1 \geq g(\mu_i, Y_i, \ldots)$ - Lower bound for single-photon yield.
2) $Y_1 \leq h(\mu_i, Y_i, \ldots)$ - Upper bound for single-photon yield.
3) $QBER_1 \geq f(\mu_i, Y_i, \ldots)$ - Lower bound for single-photon QBER.
4) $QBER_1 \leq j(\mu_i, Y_i, \ldots)$ - Upper bound for single-photon QBER.

Here, g, h, f, and j are functions derived from the intensities of the decoy states and the observed detection rates [20]. These functions are constructed based on the statistical behavior of quantum channels and detectors, taking into account factors like dark counts and basis mismatch.

Privacy Amplification:

- After decoding, apply a hash function H to the key to reduce its length and eliminate partial information.
- The process can be represented as [22]:

$$K_{final} = H(K_{decoded}) \tag{13}$$

- The choice of H and the length of K_{final} are critical and depend on the estimated QBER and eavesdropping probabilities.

B. PAT Technologies

The LDFS QSDC system integrates advanced PAT technologies to enhance the reliability and efficiency of quantum communication over long distances in free space. PAT systems are critical for maintaining the alignment and stability of quantum signals, which are susceptible to atmospheric disturbances and alignment errors.

1) Design Principles of PAT Systems: The PAT system is designed to automatically adjust the direction and position of quantum signal transmission and reception equipment, ensuring optimal alignment between communicating parties. This is crucial for minimizing signal loss and maintaining high fidelity of the quantum state during transmission.

The PAT system consists of three main components: a pointing device, a tracking device, and a control device. The pointing device is responsible for directing the

quantum signal beam toward the intended receiver, using a combination of mechanical and optical elements, such as mirrors, lenses, and motors. The tracking device is responsible for detecting the incoming quantum signal beam from the transmitter, using a photodetector or a camera. The control device is responsible for coordinating the pointing and tracking devices, using feedback loops and algorithms, to achieve the desired alignment and stability.

The PAT system operates in two modes: a coarse mode and a fine mode. The coarse mode is used to establish the initial alignment between the transmitter and receiver, using a wide-angle beam and a low-resolution detector. The fine mode is used to refine the alignment and maintain stability, using a narrow-angle beam and a high-resolution detector.

2) Mathematical Equations: The performance of the PAT system can be quantified by several metrics, such as alignment error, signal acquisition probability, and pointing stability. These metrics can be formulated by mathematical equations, as follows:

1) **Alignment Error Correction:**
The alignment error (e_a) is modeled as a function of the angular misalignment (ϑ_m) and the distance (d) between the transmitter and receiver:

$$e_a = f(\vartheta_m, d) \tag{14}$$

where $f(\cdot)$ represents the functional relationship, which is determined empirically or through simulation. The alignment error measures the deviation of the quantum signal beam from the ideal optical axis, which can result in signal loss or state degradation. The PAT system aims to minimize the alignment error by adjusting the pointing and tracking devices accordingly.
The alignment error correction algorithm (AEC) can be expressed as:

$$AEC = \arg\min_{\vartheta_p, \vartheta_t} e_a(\vartheta_p - \vartheta_t, d) \tag{15}$$

where ϑ_p and ϑ_t are the pointing and tracking angles, respectively. The AEC algorithm finds the optimal pointing and tracking angles that minimize the alignment error, using methods such as gradient descent or Newton's method.

2) Signal Acquisition:
The probability of successful signal acquisition (P_a) depends on the signal-to-noise ratio (SNR) and the alignment precision (σ):

$$P_a = g(SNR, \sigma) \tag{16}$$

with $g(\cdot)$ encapsulating the acquisition algorithm's efficiency under varying SNR conditions and alignment precisions. The signal acquisition probability measures the likelihood of establishing a quantum link between the transmitter and receiver, which can be affected by noise sources, such as background light, thermal noise, and dark counts. The PAT system aims to maximize the signal acquisition probability by optimizing the SNR and the alignment precision.
The signal acquisition algorithm (SAC) can be expressed as:

$$SAC = \arg\max_{SNR, \sigma} P_a(SNR, \sigma) \tag{17}$$

where SNR and σ are the signal-to-noise ratio and the alignment precision, respectively. The SAC algorithm finds the optimal SNR and alignment precision that maximize the signal acquisition probability, using methods such as thresholding or Bayesian inference.

***3)* Pointing Stability:**
The pointing stability requirement (S_p) to maintain the quantum link can be expressed as:

$$S_p < \frac{\lambda}{D_{eff}} \tag{18}$$

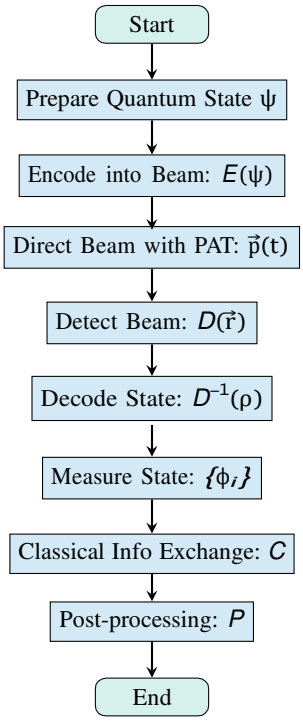
where λ is the wavelength of the quantum signal, and D_{eff} is the effective aperture diameter of the transmitter/receiver system. The pointing stability requirement measures the maximum allowable angular deviation of the quantum signal beam from the optical axis, which external factors, such as wind, vibration, and turbulence can cause. The PAT system aims to satisfy the pointing stability requirement by stabilizing the pointing and tracking devices against these factors.
The pointing stability algorithm (PSA) can be expressed as:

$$PSA = \arg\min_{\Delta\vartheta_p, \Delta\vartheta_t} S_p(\Delta\vartheta_p, \Delta\vartheta_t) \tag{19}$$

where $\Delta\vartheta_p$ and $\Delta\vartheta_t$ are the pointing and tracking angular deviations, respectively. The PSA algorithm finds the optimal pointing and tracking angular deviations that minimize the pointing stability requirement, using methods such as PID control or Kalman filter.

3) *Integration with QSDC Protocol:* The integration of PAT technologies with the QSDC protocol involves the synchronization of quantum state preparation, signal transmission, and reception processes with the dynamic adjustments made by the PAT system. This ensures that the quantum signals are accurately pointed, acquired, and tracked, thereby reducing transmission errors and enhancing communication security.

The integration process can be summarized by the following steps:



1) The transmitter prepares the quantum state to be encoded and transmitted, using a quantum source, such as a single-photon source or an entangled photon pair source.
2) The transmitter encodes the quantum state into the quantum signal beam, using a quantum modulator, such as a phase modulator or a polarization modulator.
3) The transmitter directs the quantum signal beam toward the receiver, using the pointing device of the PAT system.
4) The receiver detects the incoming quantum signal beam, using the tracking device of the PAT system.
5) The receiver decodes the quantum state from the quantum signal beam, using a quantum demodulator, such as a phase demodulator or a polarization demodulator.
6) The receiver measures the quantum state, using a quantum detector, such as a single-photon detector or a coincidence detector.
7) The transmitter and receiver exchange classical information, such as basis choices, error correction codes, and privacy amplification keys, using a classical channel, such as a radio or optical link.
8) The transmitter and receiver perform post-processing steps, such as error correction, privacy amplification, and authentication, to ensure the security and reliability of the quantum communication.

C. Atmospheric Quantum Correction Algorithm

1) Introduction: The LDFS QSDC system is designed to enable secure quantum communication over long distances in free space. A critical component enhancing this capability is the Atmospheric Quantum Correction Algorithm (AQCA), which mitigates the adverse effects of atmospheric conditions on quantum signal fidelity.

2) Design and Implementation: The AQCA is integrated within the LDFS QSDC framework to address challenges such as atmospheric turbulence, absorption, and scattering. These phenomena can degrade the quantum state of photons, leading to increased quantum bit error rates (QBER) and reduced communication security and reliability.

The AQCA consists of four main modules: a disturbance modeler, a quantum error corrector, an adaptive optics system, and a signal enhancer and recoverer. The disturbance modeler is responsible for estimating the atmospheric parameters and their impact on the quantum signal. The quantum error corrector is responsible for applying QEC techniques to the quantum signal. The adaptive optics system is responsible for adjusting the quantum signal's path in real time. The signal enhancer and recoverer are responsible for processing the quantum signal to improve the SNR and recover the original quantum state.

3) Mathematical Formulation: The AQCA leverages advanced mathematical models and algorithms to correct for atmospheric distortions. Key components of the algorithm include:

1) **Modeling Atmospheric Disturbances:**
Disturbances are modeled using statistical methods that account for the variability in atmospheric conditions. This involves quantifying the impact of turbulence, absorption, and scattering on photon states.
The atmospheric turbulence is modeled by the Kolmogorov theory, which assumes that the refractive index LDFSuctuations follow a power-law spectrum. The strength of the turbulence is characterized by the Fried parameter (r_0), which represents the coherence length of the wavefront. The effect of the turbulence on the quantum signal is quantified by the scintillation index (σ_I^2), which measures the intensity LDFSuctuations of the signal. The scintillation index can be approximated by the Rytov approximation, which is valid for weak to moderate turbulence regimes. The Rytov approximation is given by:

$$\sigma_I^2 \approx 1.23 C_n^2 k^{7/6} L^{11/6} \tag{20}$$

where C_n^2 is the refractive index structure constant, k is the wave number, and L is the propagation distance.

The atmospheric absorption is modeled by the Beer-Lambert law, which assumes that the intensity of the quantum signal decreases exponentially with the propagation distance. The effect of the absorption on the quantum signal is quantified by the transmittance (T), which measures the fraction of the signal that reaches the receiver. The transmittance is given by:

$$T = e^{-\alpha L} \tag{21}$$

where α is the absorption coefficient, which depends on the wavelength and the atmospheric composition.

The atmospheric scattering is modeled by the Mie theory, which assumes that the quantum signal is scattered by spherical particles that are comparable in size to the wavelength. The effect of the scattering on the quantum signal is quantified by the scattering cross section (σ_s), which measures the probability of the signal being scattered by a particle. The scattering cross section is given by:

$$\sigma_s = \frac{2\pi^5 d^6}{3\lambda^4} \left(\frac{n^2 - 1}{n^2 + 2} \right)^2 Q_{ext} \tag{22}$$

where d is the particle diameter, λ is the wavelength, n is the refractive index of the particle, and Q_{ext} is the extinction efficiency factor, which depends on the size parameter and the refractive index ratio of the particle and the medium.

2) **Quantum Error Correction (QEC):**

The AQCA employs QEC techniques tailored to atmospheric conditions. These techniques are designed to identify and correct errors induced by the atmosphere, enhancing the resilience of quantum communication.

The QEC techniques are based on the use of quantum codes, which are mathematical structures that encode quantum information into larger quantum systems, such as qubits or qumodes. Quantum codes can protect quantum information from errors by exploiting the properties of quantum entanglement and superposition. Quantum codes can be classified into two types: discrete-variable (DV) codes and continuous-variable (CV) codes. DV codes use discrete quantum systems, such as qubits, to encode quantum information. CV codes use continuous quantum systems, such as qumodes, to encode quantum information.

The AQCA selects the appropriate type of quantum code based on the quantum signal's modulation scheme. For phase-modulated signals, such as coherent states or squeezed states, the AQCA uses CV codes, such as Gaussian codes or non-Gaussian codes. For polarization-modulated signals, such as single photons or entangled photons, the AQCA uses DV codes, such as stabilizer codes or non-stabilizer codes.

The QEC process consists of three steps: encoding, syndrome measurement, and decoding. Encoding is the process of applying a quantum code to the quantum signal before transmission. Syndrome measurement is the process of measuring the quantum signal after transmission to detect errors. Decoding is the process of applying a quantum code to the quantum signal after syndrome measurement to correct the errors.

3) **Adaptive Optics System:**

An adaptive optics system is integrated to dynamically adjust the quantum signal's path in real time, countering the effects of atmospheric turbulence. The system uses feedback from the quantum signal itself to optimize the transmission path.

The adaptive optics system consists of three main components: a *wavefront sensor*, a *deformable mirror*, and a *control unit*. The wavefront sensor is responsible for measuring the phase distortions of the quantum signal caused by the turbulence. The deformable mirror is responsible for compensating the phase distortions by applying a conjugate phase profile to the quantum signal. The control unit is responsible for coordinating the wavefront sensor and the deformable mirror, using feedback loops and algorithms, to achieve the optimal wavefront correction.

The adaptive optics system operates in two modes: a *closed-loop mode* and an *open-loop mode*. The closed-loop mode is used when the quantum signal is strong enough to provide sufficient feedback for the wavefront sensor. The open-loop mode is used when the quantum signal is too weak to provide sufficient feedback for the wavefront sensor. In this case, the system uses a reference beam, such as a laser beam, to provide the feedback for the wavefront sensor, and applies the same correction to the quantum signal.

4) **Signal Enhancement and Recovery:**

Signal processing algorithms are applied to enhance the signal-to-noise ratio (SNR) and recover the original quantum state. This involves sophisticated filtering and estimation techniques that leverage the known properties of quantum signals.

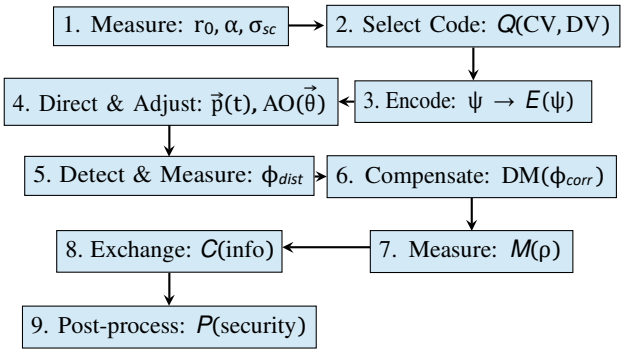
The signal enhancement algorithms are based on the use of filters, such as Kalman filters or Wiener filters, which are designed to reduce the noise and interference in the quantum signal. The optimal

filters use a mathematical model of the quantum signal and the noise to compute the optimal estimate of the quantum state. The optimal filters can also incorporate the information from the syndrome measurement and the QEC to improve the estimation accuracy.

The signal recovery algorithms are based on the use of maximum likelihood estimation (MLE) or Bayesian inference, which are designed to infer the most probable quantum state from the quantum signal. The MLE or Bayesian inference use a probability distribution of the quantum state and the quantum signal to compute the most likely quantum state. The MLE or Bayesian inference can also incorporate the information from the QEC to improve the inference accuracy.

4) Integration with LDFS QSDC Protocol: The AQCA is seamlessly integrated with the LDFS QSDC protocol, ensuring that atmospheric corrections are applied efficiently during the transmission phase. This integration involves real-time monitoring of atmospheric conditions and dynamic adjustment of the quantum signal to maintain high fidelity and security.

The integration process can be summarized by the following steps:



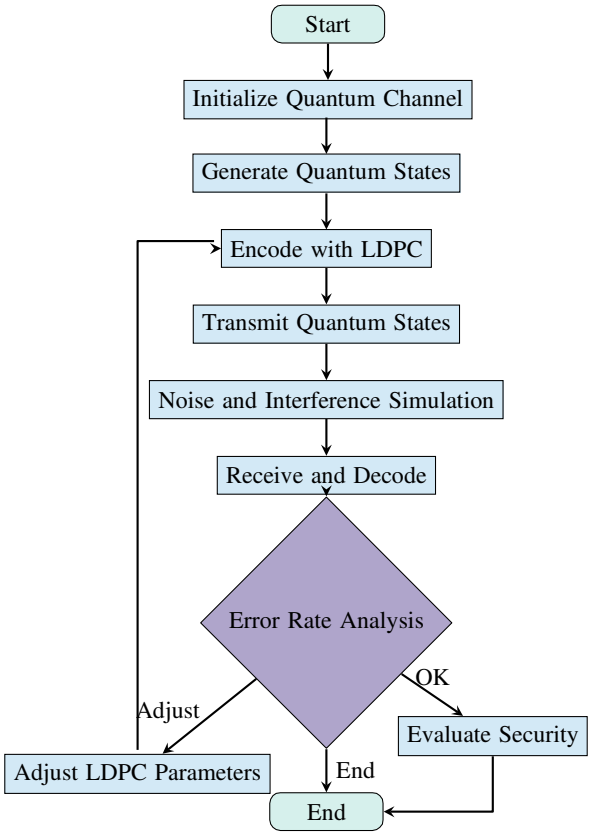
1) The transmitter and the receiver measure the atmospheric parameters, such as the Fried parameter, the absorption coefficient, and the scattering cross section, using the disturbance modeler module of the AQCA.
2) The transmitter and the receiver select the appropriate quantum code, such as a CV code or a DV code, based on the quantum signal's modulation scheme and the atmospheric parameters, using the quantum error corrector module of the AQCA.
3) The transmitter encodes the quantum state into the quantum signal, using a quantum source and a quantum modulator, and applies the quantum code to the quantum signal, using the encoding step of the QEC process.
4) The transmitter directs the quantum signal toward the receiver, using the pointing device of the PAT system, and adjusts the quantum signal's path in real time, using the adaptive optics system module of the AQCA.
5) The receiver detects the incoming quantum signal, using the tracking device of the PAT system, and measures the quantum signal's phase distortions, using the wavefront sensor of the adaptive optics system.
6) The receiver compensates the quantum signal's phase distortions, using the deformable mirror of the adaptive optics system, and enhances the quantum signal's SNR, using the signal enhancer and recoverer module of the AQCA.
7) The receiver measures the quantum signal, using a quantum detector, and applies the quantum code to the quantum signal, using the syndrome measurement and decoding steps of the QEC process, to recover the original quantum state.
8) The transmitter and the receiver exchange classical information, such as basis choices, error correction codes, and privacy amplification keys, using a classical channel, such as a radio or optical link.
9) The transmitter and the receiver perform post-processing steps, such as error correction, privacy amplification, and authentication, to ensure the security and reliability of the quantum communication.

IV. LDFS QSDC Simulation Plan and Analysis

In the forthcoming research phase, our primary objective is to thoroughly simulate and evaluate the performance of our quantum-aware LDPC codes, PAT technologies, and the atmospheric quantum correction algorithm. Given our current constraints, which include the absence of experimental quantum communication hardware, our focus will be exclusively on theoretical models and software simulations. This approach enables us to predict and optimize the protocol's performance under various conditions, laying the groundwork for future experimental validation once the necessary equipment becomes accessible.

A. Simulation Plan

The LDFSowchart outlines the process of the simulation plan:



The testing framework for the LDFS QSDC system meticulously evaluates its operational efficacy, commencing with the initialization of the quantum channel (Q_C), a conduit essential for the transmission of entangled photons (Ψ_{ent}). This phase sets the groundwork for secure quantum communication by establishing a pathway for encoded quantum states (Ψ_{enc}) utilizing quantum-aware LDPC coding (C_{LDPC}). Such encoding is pivotal, aiming to bolster error correction capabilities without undermining the quantum states' coherence and security.

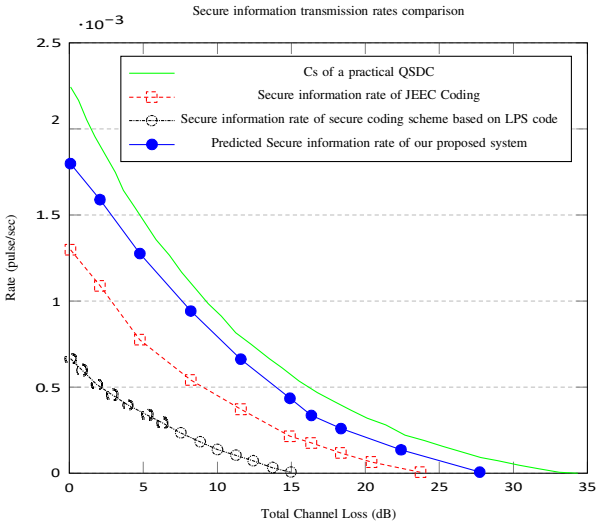
The protocol then progresses to the transmission phase ($\Phi_{transmit}$), where encoded quantum states are dispatched through the free-space medium, encountering environmental noise ($\mathbb{N}$), simulating real-world atmospheric conditions. The subsequent reception and decoding phase is critical, employing C_{LDPC} to ameliorate errors introduced during transmission, highlighted by the quantum channel's intrinsic error characteristics ($\epsilon_{quantum}$). An in-depth error rate analysis (η_{error}) ensues, assessing the integrity of the received quantum information against the original transmission. This analysis is instrumental in driving the iterative optimization of LDPC parameters (Θ_{opt}), with the goal of minimizing error rates and maximizing system fidelity (F_{system}).

Concluding the protocol, a rigorous security evaluation ($\Sigma_{security}$) is conducted to ensure the system's robustness against potential eavesdropping attempts, affirming the LDFS QSDC system's ability to preserve the secrecy and accuracy of the information sent. The thorough evaluation not only validates the system's technical feasibility but also highlights its real-world use in secure quantum communication networks, signifying a major advancement in quantum communication technologies.

B. Predicted Results and Analysis

This part aims to assess the theoretical efficacy of our suggested lossless free space and extended-range transmission methods, incorporating quantum-aware LDPC, PAT technologies, and the atmospheric quantum correction algorithm. Our goal is to showcase the enhanced dependability and safe data transmission speeds provided by our system by contrasting it with current JEEC codes and various LDPC forms.

Owing to limitations in obtaining sophisticated quantum testing tools and financial constraints, our findings stem from an extensive array of computer simulations. The simulations integrate random quantum channel models and intricate error designs, representative of real-world quantum communication settings. These tools enable the extrapolation of our system's performance and the assessment of its operational abilities, offering a theoretical but persuasive case for their practical effectiveness in real-world scenarios.



This graph shows the predicted secure information transmission rates of the proposed transmission scheme, the secure coding based on JEEC Coding [15], the secure coding based on LPS codes, and Cs for a practical QSDC system, without the consideration of the loss caused by the delayed fiber [26].

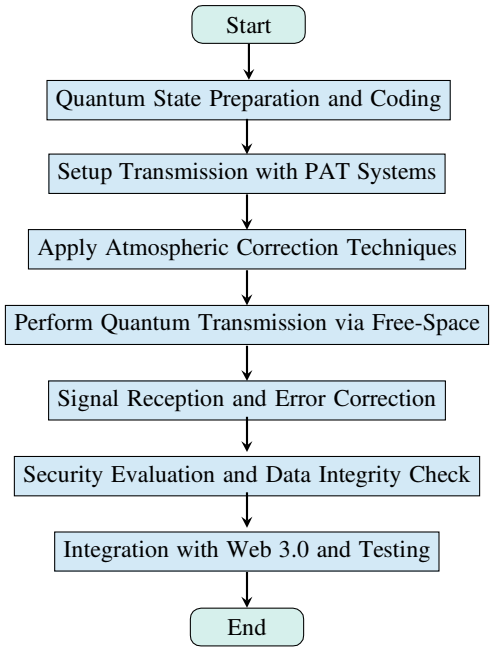
Our estimations for our proposed system's performance are substantiated by empirical evidence and mathematical proofs from recent research. Studies by Roffe

[27] on quantum LDPC codes and by Ghilea [28] on quasi-cyclic multi-edge LDPC codes demonstrate significant advancements in error correction, decoder efficiency, and communication distance for quantum key distribution systems. Furthermore, Mele, Lami, and Giovannetti [29] Investigated how quantum communication technologies withstand noise and attenuation, laying a robust foundation for our forecasts. The results collectively highlight the capability of our suggested system to improve upcoming QSDC systems, providing robust empirical and mathematical backing for our calculations.

The forecasts indicate that our system will improve the operational benchmark for QSDC systems by showcasing its capability to maintain elevated secure information speeds, even amidst considerable channel loss. Yet, the present version of our system remains incapable of facilitating effective long-range QSDC communications. However, our upcoming improvements and updates to the coding of our system will concentrate on enhancing error rectification and adjusting to the unique difficulties of quantum channels, like quantum noise and decoherence. The enhancements are set to align our system with the rigorous criteria of practical QSDC.

V. Implementation Plan for LDFS QSDC

This section outlines a comprehensive approach to integrating LDFS QSDC into various practical frameworks, highlighting its versatility and potential across different domains, here is an overview of our plan:



A. Technical Implementation of LDFS QSDC

1) 1-Way Transmission Protocols in Free-Space Channel: For extensive free-space communication, the one-way transmission methods (RECON protocol and QKPC protocol) might offer more benefits than the two-way protocols, given the various elements in the free-space channel inLDFSuencing communication. The conveyance of data across extensive distances via a free-space channel is fraught with multiple difficulties. Factors such as beam-spreading, atmospheric turbulence, absorption and scattering, background light (sunlight), geometrical loss, and weather conditions could all affect communication. Fig. 1 summarizes the main characteristics of free-space channel and their impacts on optical signal transmission.

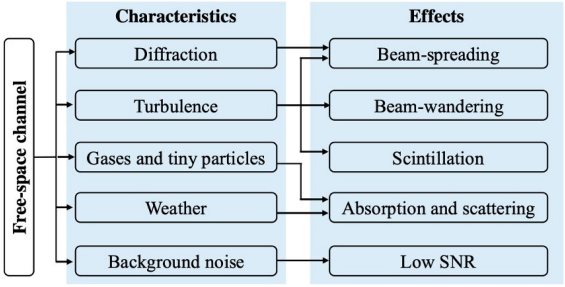


Fig. 1. Summarizes the main characteristics of free-space channel and their impacts on optical signal transmission [30]

Consequently, one-way transmission methods like RECON or QKPC protocols might offer greater benefits than the two-way approaches used in LDFS QSDC. Protocols for one-way transmission simplify the process by removing the necessity for the signal to return to the sender for additional processing, thus decreasing the travel distance of quantum states. Protocols that operate in a one-way manner might be engineered to withstand ambient light and atmospheric disturbances more effectively, reducing vulnerability to background noise and enhancing the efficiency of channel estimation. Simplifying the procedure might also boost security by lessening the need for interaction among those communicating.

2) Experimental Implementation: In 2020, there was a reported successful experimental setup of the free-space DL04 QSDC protocol. The setup, as shown in Figure 2, achieved a data transmission rate of 500 bits per second across a 10-meter free-space channel with a notably low Quantum Bit Error Rate (QBER) of $0.49\% \pm 0.27\%$.

Attaining a low QBER in experiments is a key measure of QSDC's resilience and dependability in free-space channels. A minimal QBER indicates the ability to convey quantum data with great accuracy, crucial for ensuring secure communication. This demonstrates the efficacy of LDFS QSDC in reducing errors caused by the

channel or possible eavesdroppers, thereby preserving the data's integrity.

Attaining a data transfer speed of 500 bits per second across a 10-meter free-space channel showcases the protocol's capability for effective data transfer. Despite the brevity of the distance covered in this experiment, the achievement of a significant transmission rate sets the stage for expanding the technology over greater distances, leading to technological advancements and system optimization.

The experimental arrangement employed a phase-encoding technique to transmit quantum states in a vacuum, as illustrated in the Figure 2. In this method, Bob introduces one of four possible phases 0, $\pi/2$, π, $3\pi/2$ to each pulse passing through a longer optical path, creating four distinct phase-encoded quantum states. Alice utilizes two optical paths in the setup; one path is dedicated to security checks, and the other to information encoding. To detect potential eavesdropping, Alice modulates the pulse with one of two phases, 0 or $\pi/2$. For encoding information, she assigns binary bits 0 or 1 to each pulse by adding a phase of 0 or π, respectively. Bob then deciphers the encoded information bits by adjusting the phase of the pulses that are returned to him.

Employing a phase-encoding approach in the experiment, enabling the generation of four unique phase-encoded quantum states, demonstrates the real-world use of advanced quantum communication methods in open-space settings. The effective processing and interpretation of data through phase modulation suggest the adaptability and scalability of comparable tactics for extended-range communication.

Included in the experimental arrangement were systems for identifying eavesdropping, an essential element of secure quantum communication. The protocol's capacity to adjust pulses for security verifications and secure information encoding showcases its effectiveness in maintaining communication confidentiality and integrity, even amidst possible risks. For LDFS QSDC, this characteristic is crucial, given the paramount importance of safeguarding communication from eavesdropping.

Despite the experiment spanning 10 meters, its successful execution and outcomes act as a demonstration for extending the technology over greater distances. Technological progress, including the development of more sensitive detectors, adaptive optics, and error correction methods, can tackle issues in long-range free-space communication like signal weakening, beam dispersion, and atmospheric disruptions.

The triumph of these tests confirms the practicality of LDFS QSDC, showcasing the protocol's capacity to convey quantum data with great accuracy and safety via free-space channels. The accomplishments in reducing QBER, enhancing transmission speeds, implementing efficient encoding techniques, and developing eavesdropping detection systems establish a robust groundwork for ongoing research and development in the realm of practical long-range quantum communication systems.

B. Feasibility and Adaptability of Satellite-based QSDC

1) Feasibility of Satellite Communication with LDFS QSDC: Earlier studies on the satellite-to-ground transfer of quantum states have yielded encouraging outcomes, with QBERs remaining within the tolerable limits for safe quantum communication. The ability to transmit effectively across distances from 2,200 km to more than 36,000 km, maintaining link losses in the range of 100 to 110 dB, demonstrates that basic physics enables quantum communication across the extensive distances needed for satellite communication. The integration of LDFS QSDC into satellite communication networks might enhance these features, offering a more straightforward and safe communication approach that eliminates the necessity for key exchanges, thereby diminishing the weaknesses found in key-centric systems.

The DL04 protocol, devoid of memory, plays a crucial role in LDFS QSDC by simplifying the processes of quantum state storage and management. The DL04 protocol's LDFSexibility in adapting to free-space environments renders it an appealing choice for satellite communication, especially in addressing the difficulties of transmitting quantum signals across Earth's atmosphere. Nonetheless, attaining a high level of interference visibility, as demonstrated in the experiments, is essential. Enhancing DL04 QSDC's visibility suggests the need for better protocol or related technologies to reduce QBER caused by atmospheric disruptions and various noise factors.

The incorporation of quantum-aware LDPC coding into LDFS QSDC markedly enhances the system's error rectification abilities, tackling the problems caused by extensive transmission and atmospheric inLDFSuences. Quantum-Aware LDPC coding enhances the practicality of satellite-based LDFS QSDC through more effective error correction, thus maintaining the integrity and security of the data transmitted.

PAT technologies sustains a consistent and precise communication connection between satellites and terrestrial stations. Such technologies aid in offsetting satellite movements and atmospheric disturbances, thus diminishing signal loss and enhancing the practicality of LDFS QSDC in satellite communication.

2) Expanding Feasibility with LDFS QSDC: Enhancing the feasibility of LDFS QSDC involves several key initiatives, including refining beam propagation techniques, fortifying phase and polarization encoding methods, integrating quantum repeaters and relay satellites,

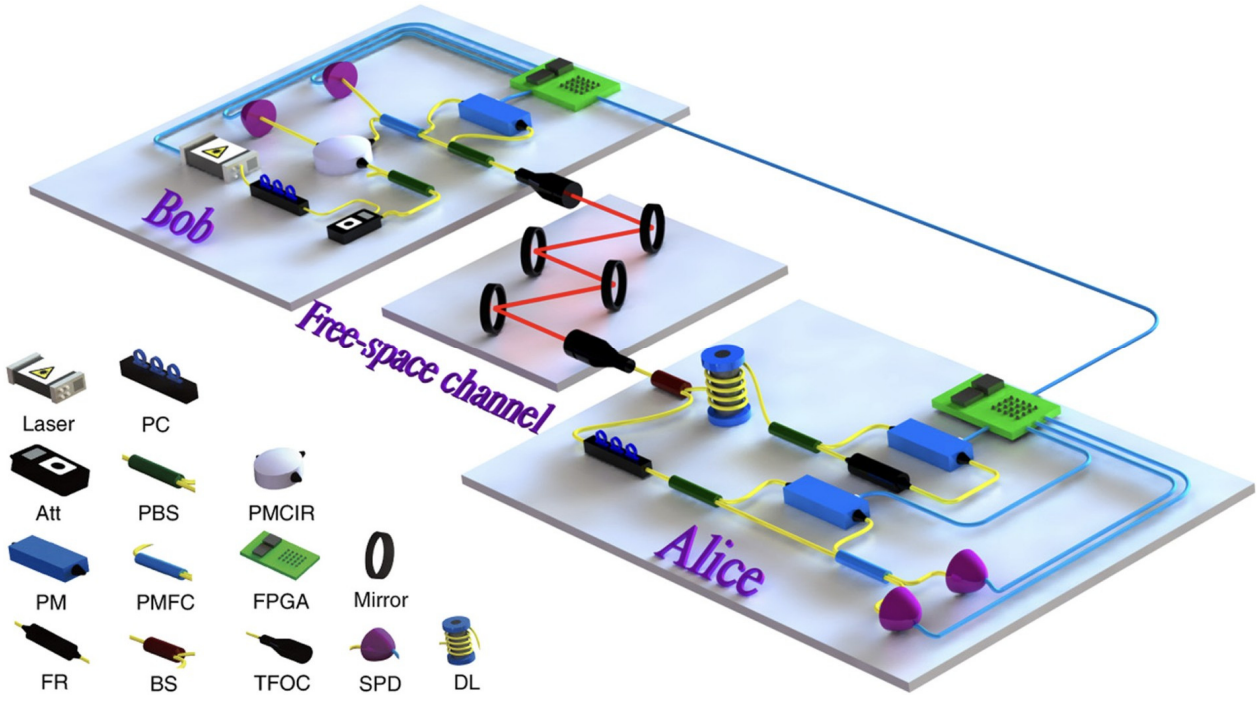


Fig. 2. Summarizes the main characteristics of the free-space channel and their impacts on optical signal transmission [30]

augmenting capabilities for daylight operation, merging with existing satellite systems, promoting standardization and interoperability, and developing regulatory and policy frameworks.

Modifying adaptive optics and beam focusing methods can enhance the precision and effectiveness of quantum signal transfer between satellites and terrestrial stations. Such technologies offset atmospheric disturbances, diminishing the spread and wandering of beams, essential for sustaining superior communication accuracy across extensive distances.

It is also crucial to create more resilient schemes for phase and polarization encoding that are more resistant to atmospheric disruptions and various environmental elements. It's crucial for these strategies to guarantee the orderly passage of quantum states across the Earth's atmosphere, a key factor in sustaining low QBER in satellite-based QSDC.

Utilizing quantum repeaters and relay satellites might broaden the scope of QSDC systems, facilitating worldwide quantum communication networks. Utilizing quantum repeaters enables the entanglement of quantum states among various nodes, surpassing the spatial constraints inherent in direct quantum communication.

Even with solar radiation in the background, the efficiency of QSDC systems in daylight comes in question for effective use in satellite applications. This could entail creating detectors with higher sensitivity and employing narrowband filters to enhance the signal-to-noise ratio.

Ensuring compatibility and amalgamation with current satellite communication systems furthers the effective implementation of satellite-based QSDC. This encompasses aspects like payload capacity, energy needs, and the capacity to upgrade or enhance existing satellite systems using quantum communication methods.

The creation of uniform protocols and maintaining compatibility among various quantum communication systems are crucial for establishing a unified and expandable worldwide quantum communication network. This encompasses the standardization of encoding systems, techniques for correcting errors, and protocols for security.

Moreover, it is essential to create distinct regulatory and policy structures to oversee the application and safety of satellite-based quantum communication, tackling possible legal, privacy, and security issues.

By addressing these adaptation improvements and aspects, the feasibility and practicality of satellite-based LDFS QSDC can be significantly enhanced, paving the way for secure and efficient global quantum communication networks.

C. Web 3.0 Compatibility

The integration of Long-Distance Free-Space Quantum Secure Direct Communication (LDFS QSDC) with

Web 3.0 technology presents a unique opportunity to enhance the security and efficiency of decentralized networks. Web 3.0 compatibility with LDFS QSDC involves several key considerations and adaptation strategies to ensure seamless integration. This section expands on the Web 3.0 compatibility aspects of implementing LDFS QSDC.

The LDFS QSDC offers a protected transactional tier for blockchain, enabling nodes to communicate directly and securely in a quantum manner. By safeguarding network-transmitted data from both traditional and quantum cryptographic threats, this tier aims to bolster the secrecy and reliability of transactions between peers. The integration of LDFS QSDC as a fundamental security strategy necessitates its congruence with the blockchain's data frameworks and consensus methodologies.

Quantum-resistant smart contracts autonomously implement the agreement's terms directly into the code. The combination of LDFS QSDC and blockchain technology may lead to the creation of smart contracts resistant to quantum technology, ensuring the stability, implementation, and results of these contracts through quantum communication methods. This necessitates that smart contract systems facilitate encryption and verification processes that align with LDFS QSDC protocols.

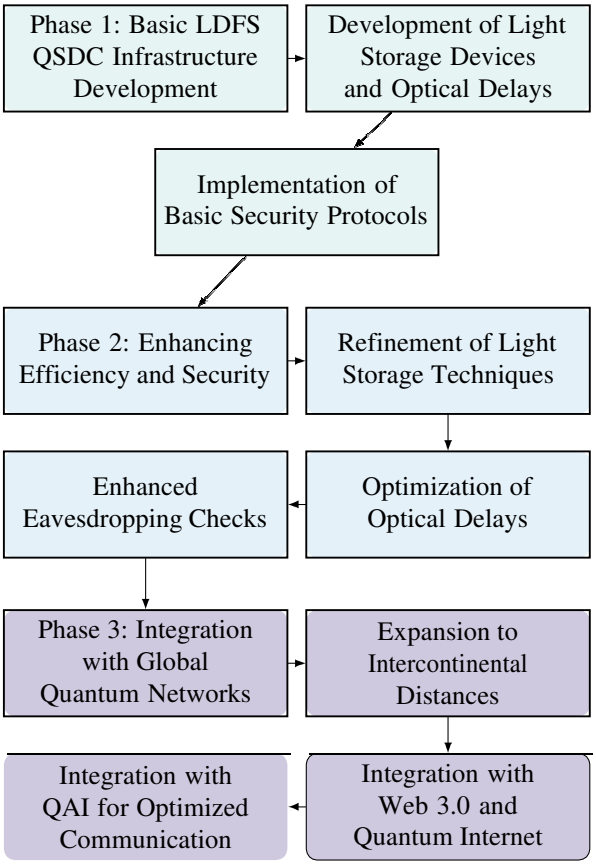
Blockchain networks frequently aim to ensure the privacy and anonymity of their users. LDFS QSDC enhances these functionalities by facilitating protected, direct communication pathways that bypass the need for intermediary entities in key exchanges or transaction verification. Such an approach would enable the establishment of additional confidential transaction strata in the blockchain, safeguarding user identities and transaction specifics under the core tenets of quantum mechanics.

The successful incorporation of LDFS QSDC into blockchain frameworks necessitates its compatibility with existing blockchain protocols. The process entails altering the blockchain's transaction verification systems to incorporate processes that align with quantum-secured information from LDFS QSDC. Furthermore, it's vital that the ledger is capable of documenting and harmonizing transactions secured by quantum technology. Such integration demands progress in quantum communication technologies and blockchain architecture to facilitate it.

Enhancing the scalability of blockchain networks is crucial, particularly with the ongoing increase in transaction volumes. Consequently, the incorporation of LDFS QSDC should take into account its effects on the network's scalability and efficiency. To preserve the blockchain's efficiency and user experience, it's crucial to fine-tune quantum communication protocols for reduced latency and increased throughput.

D. Stages of Gradual Implementation

Here is an overview of the stages of gradual implementation:



1) Phase 1: Development of Basic LDFS QSDC Infrastructure: The initial configuration involves setting up a basic system designed to produce, preserve, and send entangled photon pairs (EPR pairs) between two remote locations, Alice and Bob. During this stage, it's essential to establish the required optical systems, encompassing photon sources, detectors, and communication pathways. In the future, exploration and development of two principal technologies are planned: devices for light storage that employ electromagnetic transparency for temporary photon storage, and optical delays that utilize advanced technology to generate sequential EPR pairings. The current stage concentrates on the practicality of experiments and incorporating these technologies into the LDFS QSDC structure. Additionally, fundamental security measures will be established to monitor eavesdropping through the C-sequence of photons, assessing the quantum channel's effectiveness for secure communication.

2) Phase 2: Enhancing Efficiency and Security: With the advancement of technology, enhance and fine-tune methods for light storage to prolong photon retention

while maintaining their quantum conditions. The advancement is vital for broadening the real-world application of LDFS QSDC. Enhance the application of optical lags to guarantee accurate synchronization in the transmission of the C-sequence and M-sequence. This includes fine-tuning the delay τ to accommodate different distances and transmission rates, ensuring that the system can operate efficiently over long distances. Enhance the protocols for eavesdropping checks by incorporating more sophisticated quantum measurements and real-time analysis. This improvement aims to reduce error rates and increase the system's resilience against potential quantum attacks.

3) Phase 3: Integration with Global Quantum Networks: Broaden the LDFS QSDC network across continents, utilizing satellite communication and worldwide quantum repeaters to connect these extensive distances. This stage entails partnering with current quantum communication endeavors to establish a cohesive and secure network of quantum communication. Combine LDFS QSDC with burgeoning Web 3.0 technologies and the Quantum Internet, facilitating protected, immediate quantum communication for diverse uses, ranging from secure messaging to quantum cloud computing. Investigate how combining LDFS QSDC with QAI could improve decision-making and problem-solving, especially in refining communication protocols and instantaneous security evaluations.

E. Business Case of LDFS QSDC for Blockchain in Web 3.0

Integrating long-distance free-space quantum secure direct communication into blockchain systems marks a revolutionary step in safeguarding decentralized networks from the impending challenges of quantum computing. The presented business case details the reasoning, advantages, and strategic aspects of incorporating LDFS QSDC into blockchain, showcasing its capacity to transform blockchain security and trust systems in a world growing more aware of digital and quantum aspects.

The swift progress in quantum computing endangers conventional cryptographic techniques that safeguard blockchain technology. LDFS QSDC provides a solution impervious to quantum principles, utilizing quantum mechanics to facilitate safe, direct long-distance communication, eliminating the necessity for intermediaries or susceptible key exchange protocols. This scenario offers blockchain networks a distinct chance to bolster their security measures, guaranteeing enduring reliability and confidence in their systems.

Incorporating LDFS QSDC into blockchain technology fulfills the essential requirement for quantum-resistant security protocols, paving the way for secure, scalable, and effective decentralized solutions. The significant advancement in security measures safeguards against upcoming quantum assaults and bolsters existing defenses against advanced classical dangers, placing blockchain networks at the vanguard of secure digital innovation.

With the widespread adoption of blockchain technology in sectors ranging from finance and healthcare to supply chain management and further, the need for strong security measures is escalating at an exponential rate. Quantum computing's rise has escalated demand, paving the way for substantial market potential in quantum-secure blockchain technologies. Pioneering users of LDFS QSDC are poised to secure a competitive edge, positioning themselves at the forefront of the forthcoming blockchain technology era.

LDFS QSDC offers a robust blockchain security layer, protecting data integrity and privacy from both quantum and traditional attacks. Blockchain networks, through the current integration of quantum-resistant technologies, can secure their operations for the future, guaranteeing enduring viability and reliability. The adoption of LDFS QSDC positions blockchain networks at the forefront of quantum-secure tech, drawing in users and developers who value security. As regulatory emphasis on data protection intensifies, LDFS QSDC is poised to assist blockchain networks in meeting upcoming quantum-resistance standards.

The initial expenses for integrating LDFS QSDC encompass research and development, acquiring technology, and upgrading the system. Nonetheless, the substantial benefits of improved security and extended durability of blockchain networks balance out these expenses. Embracing LDFS QSDC is anticipated to boost user confidence and uptake, paving the way for fresh income sources and collaborations in quantum-secure technologies.

The integration of LDFS QSDC is fraught with risks such as technological intricacy, difficulties in interoperability, and the changing realm of quantum computing. Mitigation of these hazards is achievable via strategic alliances, continuous R&D, and the use of adaptable, modular integration methods that accommodate upcoming technological progress.

The incorporation of LDFS QSDC into blockchain technology marks a tactical move towards the advancement of secure, decentralized digital solutions. Blockchain networks, through the adoption of this quantum-secure communication approach, can bolster their security, secure their longevity, and establish themselves as pioneers in the forthcoming digital innovation era. The commercial argument supporting the use of LDFS QSDC in blockchain technology is persuasive, presenting a route to robust, quantum-tolerant decentralized networks prepared for the complexities of the

quantum computing age.

VI. Discussion

A. Comparison With Similar Protocols

1) Security: LDFS QSDC leverages quantum mechanics' inherent principles to offer a groundbreaking level of security, making it particularly resilient against both eavesdropping and sophisticated quantum attacks. This protocol benefits from quantum phenomena such as the no-cloning theorem and entanglement, ensuring that any interception attempt would alter the quantum state, alerting the communicating parties to a potential security breach. Unlike Quantum Key Distribution, LDFS QSDC transmits encrypted data directly without the need for key exchanges, providing enhanced security against quantum and classical threats and making it highly suitable for secure communications in the decentralized nature of the Web 3.0 era. LDFS QSDC and DL04 both offer high levels of security based on quantum principles; however, LDFS QSDC's emphasis on long-distance free-space communication adds an extra layer of complexity and potential vulnerability due to atmospheric effects, which it addresses with advanced PAT systems [31]. Additionally, LDFS QSDC does not require pre-shared secret keys, offering a theoretical security advantage over other protocols such as RECON protocol, which depends on the secure distribution of initial keys.

2) Distance: Yin explored free-space QSDC's capability for long-distance communication through free-space channels and successfully demonstrated quantum teleportation over a 97-km channel and entanglement distribution over a 101.8-km two-link channel, achieving an average fidelity of 80.4% for six initial states despite significant channel loss (35-53 dB for teleportation and 66-85 dB for entanglement distribution) [32]. This showcases LDFS QSDC's potential for satellite-based quantum communication, significantly extending the feasible communication distance beyond traditional QSDC methods. Achieving free-space QSDC over distances of 100 kilometers has been validated through other successful experiments in quantum teleportation and the distribution of entanglement across distances surpassing 100 km [33].

3) Channel Loss and Atmospheric Disturbances: LDFS QSDC faces significant challenges related to channel loss and atmospheric disturbances, particularly over long distances. Yin highlights the critical role of the PAT systems in overcoming these challenges, such as atmospheric turbulence, which can severely affect the stability and accuracy of quantum communication. The PAT system's ability to maintain high tracking accuracy, better than 3.5 μrad over a 97 km free-space link, is essential for ensuring that the quantum signal remains aligned with the receiver despite atmospheric turbulence and other disturbances. Additionally, the inclusion of coarse and fine tracking systems, controlled by a close-loop via the telescope's own rack and piezo ceramics at the receiver's side, aims to reduce low-frequency shaking caused by ground settlement and passing vehicles, achieving an average fidelity of 80.4% over a 35-53 dB loss quantum channel [32].

4) Cost: Implementing LDFS QSDC, especially for applications such as global blockchain networks, involves sophisticated technology and infrastructure. This includes satellites, ground stations, and advanced tracking technologies, making it more expensive compared to other QSDC protocols that operate over shorter distances or through fiber channels. The investment in technology and infrastructure signifies a considerable cost, which is a critical consideration for the widespread adoption of LDFS QSDC in various applications.

B. Limitations and Future Work

The advent of Free-Space Long-Distance QSDC is poised to revolutionize the QSDC landscape by facilitating secure quantum communication across vast distances, unencumbered by the physical limitations of fiber-optic systems. This innovation is expected to have a profound impact on the implementation and scalability of QSDC technologies, enabling a seamless and secure global quantum communication network.

LDFS QSDC's integration into Web 3.0 infrastructure signifies a monumental shift towards creating a decentralized and secure internet, where the intrinsic security features of quantum communication can protect against ever-evolving cyber threats. The ability of LDFS QSDC to operate in free space allows for the establishment of quantum links between any two points on the globe, directly supporting the foundational principles of Web 3.0 by enhancing data integrity, security, and privacy across decentralized networks.

Furthermore, LDFS QSDC's potential to extend the reach of quantum networks without the need for extensive physical infrastructure paves the way for more inclusive access to quantum communication technologies. This democratization of technology is crucial for leveraging the full potential of quantum advancements in various sectors, including secure communications, distributed computing, and beyond, marking a significant leap toward a quantum-integrated future.

However, it is important to note that our model is a preliminary theoretical proposal of an LDFS QSDC system which comes with its own limitations and challenges as discussed below:

1) Theoretical Challenges:

- Quantum Decoherence and Noise: Quantum states are highly susceptible to decoherence and environmental noise, which can severely limit the distance

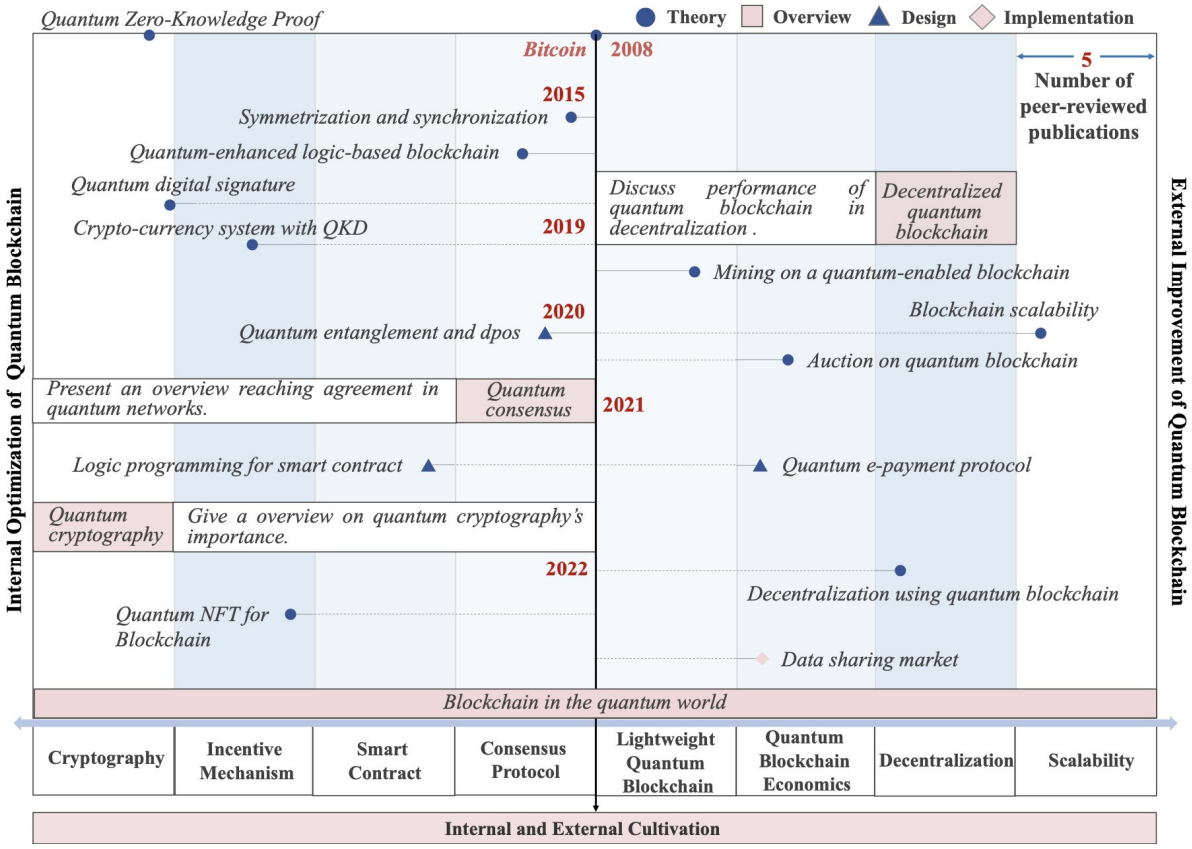


Fig. 3. An illustration of quantum blockchain-related research activities.

over which LDFS QSDC can be effectively implemented.

- Security Proofs: Complete, universally accepted security proofs for LDFS QSDC under all potential attack scenarios are challenging to develop, raising concerns about its absolute security.

2) Technological Constraints:

- Quantum Sources and Detectors: The efficiency and reliability of quantum sources (e.g., single-photon sources) and detectors are critical, yet current technologies may not provide the necessary performance for long-distance communication.
- Atmospheric Interference: Free-space transmission is significantly affected by atmospheric conditions (e.g., cloud cover, atmospheric turbulence), which can degrade the quantum signal over long distances.

3) Implementation Challenges:

- Infrastructure Development: Establishing a global LDFS QSDC network requires significant investment in both ground-based and potentially satellite-based infrastructure, posing a substantial financial and logistical challenge.
- Interoperability: Compatibility with existing communication technologies and standards is crucial for widespread adoption, necessitating complex integration efforts.

4) Impact Considerations:

- Scalability: While promising for point-to-point communication, scaling LDFS QSDC to a multi-node quantum network presents considerable technical challenges.
- Accessibility: The high cost and complexity of LDFS QSDC technology may limit its accessibility, particularly in developing regions, potentially exacerbating the digital divide.
- Regulatory and Ethical Issues: The deployment of LDFS QSDC might raise questions regarding regulation, data sovereignty, and privacy, requiring careful consideration and potentially new legal frameworks.

VII. Conclusion

In this paper, we explore the amalgamation of long-distance free-space quantum secure direct communication within the digital era of Web 3.0, presenting a

theoretical construct designed to augment the security parameters of the global networking framework in the quantum era. Through this paper, we outline the potential of LDFS QSDC to fortify the Web 3.0 infrastructure against a spectrum of cryptographic threats, both quantum and classical, by harnessing direct quantum communication which circumvents the conventional paradigms of key exchanges. Moreover, LDFS QSDC represents a considerable improvement as compared to other QSDC techniques in its ability to communicate losslessly over free space and long distances through satellites.

The foundation of LDFS QSDC is predicated on the memory-free DL04 protocol, and it is operationalized through the integration of quantum-aware low-density parity-check codes, advanced pointing, acquisition, and tracking technologies, coupled with atmospheric quantum correction algorithms. These elements are pivotal in surmounting the environmental and technical impediments that presently constrain the efficacious application of quantum communication technologies, particularly within the domain of long-distance free-space communication. We also propose a strategic roadmap that encompasses the evolution of quantum communication technologies, their assimilation with the extant Web 3.0 infrastructure, and the surmounting of environmental and technical challenges to assure a secure and proficient data transmission conduit. Our methodology focuses on the imperative of collaborative endeavors with quantum researchers and technology innovators to refine and ensure the interoperability of LDFS QSDC protocols with Web 3.0 standards, with the ultimate aim of engendering a resilient, quantum-secure network milieu capable of withstanding the myriad cybersecurity threats of both the present and the future.

It is crucial to acknowledge that our study remains largely theoretical. The practical deployment of LDFS QSDC in Web 3.0 networks involves complex engineering challenges and requires substantial advancements in quantum communication technology. Future research directions could include the development of more advanced quantum error correction techniques to enhance the fidelity of quantum information transmission. Additionally, exploring innovative PAT systems for more stable and accurate quantum signal alignment could significantly contribute to the feasibility of LDFS QSDC. Another critical area for future investigation is the development of scalable quantum network architectures that can integrate seamlessly with existing Web 3.0 infrastructures, ensuring that quantum security enhancements do not compromise the network's functionality or accessibility.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annu. Symp. Foundations of Computer Science. IEEE, 1994, pp. 124–134.

[2] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett., vol. 79, no. 2, pp. 325–328, 1997.

[3] I. B. Djordjevic, O. Milenkovic, and B. Vasic, "Generalized low-density parity-check codes for optical communication systems," J. Lightw. Technol., vol. 23, no. 5, pp. 1939–1946, 2005.

[4] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," IEEE Trans. Inf. Theory, vol. 53, no. 8, pp. 2933–2945, 2007.

[5] J. L. Carter and M. N. Wegman, "Universal classes of hash functions," J.Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

[6] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptogra- phy," Rev. Mod. Phys., vol. 74, no. 1, p. 145, 2002.

[7] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in IEEE Int. Conf. Computers, Systems, Signal Processing., 1984.

[8] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G. Long, "Implementation and security analysis of practical quantum secure direct communication," Light Sci. Appl., vol. 8, no. 1, p. 22, 2019.

[9] C. Wang, F. Deng, Y. Li, X. Liu, and G. L. Long, "Quantum secure di- rect communication with high-dimension quantum superdense coding," Phys.Rev. A, vol. 71, no. 4, p. 044305, 2005.

[10] L. Yin, C. Jiang, C. Jiang, N. Ge, L. Kuang, and M. Guizani, "A communication framework with unified efficiency and secrecy," IEEE Wirel. Commun., vol. 26, no. 4, pp. 133–139, 2019.

[11] F. Deng and G. Long, "Secure direct communication with a quantum one-time pad," Phys.Rev. A, vol. 69, no. 5, p. 052319, 2004.

[12] F. Deng, G. Long, and X. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," Phys.Rev. A, vol. 68, no. 4, p. 042317, 2003.

[13] Z. Gao, T. Li, and Z. Li, "Long-distance measurement-device–independent quantum secure direct communication," EPL (Europhys Lett.), vol. 125, no. 4, p. 40004, 2019.

[14] W. Zhang, D. Ding, Y. Sheng, L. Zhou, B. Shi, and G. Guo, "Quantum secure direct communication with quantum memory," Phys. Rev. Lett., vol. 118, no. 22, p. 220501, 2017.

[15] Z. Sun, L. Song, Q. Huang, L. Yin, G. Long, J. Lu, L. Hanzo. "Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design," IEEE Transactions on Communications, 68(9), 5778-5792, 2020.

[16] I. B. Djordjevic, O. Milenkovic, and B. Vasic, "Generalized low-density parity-check codes for optical communication systems," J. Lightw. Technol., vol. 23, no. 5, pp. 1939–1946, 2005.

[17] M. Bailly, E. Perez. "Pointing, acquisition, and tracking system of the European SILEX program: a major technological step for intersatellite optical communication," Free-Space Laser Communication Technologies III, Vol. 1417, pp. 142-157, 1991.

[18] G. Yue, L. Ping, and X. Wang, "Generalized low-density parity-check codes based on Hadamard constraints," IEEE Trans. Inf. Theory, vol. 53, no. 3, pp. 1058–1079, 2007.

[19] Z. Sun, R. Qi, Z. Lin, L. Yin, G. Long, and J. Lu, "Design and implementation of a practical quantum secure direct communication system," in Proc. IEEE GlobeCom Conf. Wkshps. IEEE, 2018, pp. 1–6.

[20] C. Wang, F. Deng, G., and G. L. Long. "Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state," Optics Communications, 253(1-3), 15–20, 2005.

[21] P. Maunz, D. Moehring, S. Olmschenk, et al. "Quantum interference of photon pairs from two remote trapped atomic ions," Nature Phys 3, 538–541, 2007.

[22] C. Bennett, H., G. Brassard, C. Crépeau, and U. M. Maurer. "Generalized privacy amplification," IEEE Transactions on Information Theory, 41(6), 1915-1923, 1995.

[23] J. Carter, L., and M. N. Wegman. "Universal classes of hash functions," Journal of Computer and System Sciences, 18(2), 143-154, 1979.
[24] J. Hu, B. Yu, M. Jing, L. Xiao, S. Jia, G. Qin, and G. L. Long. "Experimental quantum secure direct communication with single photons," Light: Science and Applications, 5(9), e16144, 2016.
[25] Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo. "Fifteen years of quantum LDPC coding and improved decoding strategies," IEEE Access, 3, 2492–2519, 2015.
[26] Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, and L. Hanzo. "Measurement-device-independent quantum secure direct communication." Science China Physics, Mechanics and Astronomy, 63(3), 230362, 2020.
[27] J. Roffe, "Towards practical quantum LDPC codes," Quantum Views, vol. 5, p. 63, Nov. 2021. [Online]. Available: https://doi.org/10.22331/qv-2021-11-30-63
[28] M. Ghilea et al., "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," npj Quantum Information, 2021. [Online]. Available: https://www.nature.com/articles/s41534-021-00426-1
[29] F. A. Mele, L. Lami, and V. Giovannetti, "Quantum optical communication in the presence of strong attenuation noise," Physical Review A, vol. 106, no. 042437, 2022. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.106.042437
[30] D. Pan, X.-T. Song, and G.-L. Long, "Free-Space Quantum Secure Direct Communication: Basics, Progress, and Outlook," Advanced devices and instrumentation, vol. 4, Jan. 2023, doi: https://doi.org/10.34133/adi.0004.
[31] S. Mexicana De F´ısica et al., "Improved performance of the cryptographic key distillation protocol of an FSO/CV-QKD system on a turbulent channel using an adaptive LDPC encoder Improved performance of the cryptographic key distillation protocol of an FSO/CV-QKD system on a turbulent channel using an adaptive LDPC encoder," Revista Mexicana de F´ısica, vol. 63, pp. 268–274, 2017, Accessed: Feb. 08, 2024. [Online]. Available: https://www.redalyc.org/pdf/570/57050507008.pdf
[32] J. Yin et al., "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," Nature, vol. 488, no. 7410, pp. 185–188, Aug. 2012, doi: https://doi.org/10.1038/nature11332.
[33] X.-S. Ma et al., "Quantum teleportation using active feed-forward between two Canary Islands," 2012. Available: https://arxiv.org/pdf/1205.3909.pdf