Novel Long Distance Free Space Quantum Secure Direct Communication for Web 3.0 Networks

Yifan Zhou *, Xinlin Zhou , Zi Yan Li , Yew Kee Wong , Yan Shing Liang

Posted Date: 9 September 2024

doi: 10.20944/preprints202409.0656.v1

Keywords: Quantum Cryptography; Web 3.0; Quantum Secure Direct Communication; Long-Distance Free-Space Quantum Secure Direct Communication; Quantum Security

 doi:10.20944/preprints202409.0656.v1

Article

Novel Long Distance Free Space Quantum Secure Direct Communication for Web 3.0 Networks

Yifan Zhou [1,*], Xinlin Zhou [2] Zi Yan Li [2], Yew Kee Wong [3] and Yan Shing Liang [4]

[1] University of California, Los Angeles Los Angeles, USA
[2] BASIS International School Guangzhou Guangzhou, China; xinlin.zhou13495-bigz@basischina.com (X.Z.); ziyan.li11716-bigz@basischina.com (Z.Y.L.)
[3] Hong Kong Chu Hai College Hong Kong, China; ericwong@chuhai.edu.hk
[4] New York University New York, USA; yanshing.liang40486-bigz@basischina.com
* Correspondence: yzhou05@ucla.edu

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 our novel long-distance free-space quantum secure direct communication (LF QSDC) as a method to safeguard against security breaches in both quantum and classical contexts. Differing from techniques like quantum key distribution (QKD), LF 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 technical design and incorporation of LF QSDC into web 3.0 network infrastructures, highlighting its efficacy for extended-range communication. LF QSDC is based on the memory DL04 protocol and enhanced with our novel Quantum-Aware Low-Density Parity Check (LDPC), Pointing, Acquisition, and Tracking (PAT) technologies, and Atmospheric Quantum Correction Algorithm (AQCA). Utilizing this method not only bolsters the security of worldwide Web 3.0 networks but also guarantees their endurance in a time when quantum and sophisticated classical threats exist simultaneously. Consequently, LF QSDC stands out as a robust security solution, well-suited for Web 3.0 systems amidst the constantly evolving digital environment.

Keywords: quantum cryptography; Web 3.0; quantum secure direct communication; long-distance free-space quantum secure direct communication; quantum security

1. Introduction

The advent of Web 3.0 has dramatically transformed internet usage and application interaction, characterized by a decentralized, distributed, and user-centric approach. This paradigm shift empowers users with unprecedented control over their data, identity, and privacy. In the context of our globalized digital ecosystem, securing these networks is crucial, given the varied reliability and risk profiles across nodes and users. Traditional security mechanisms, including public key encryption and digital signatures, play a pivotal role in ensuring the confidentiality, integrity, and authenticity of network transactions and data. However, the emergence of quantum computing, leveraging principles of quantum mechanics, presents a formidable challenge to these cryptographic defenses, threatening to compromise data integrity by breaking current encryption methods [1,2].

 doi:10.20944/preprints202409.0656.v1

Table 1. Comparison of Types of Quantum Secure Communication Protocols.

Category	**Type of Protocol**			
	LF QSDC	***DL04 Protocol***	***Memory-Free DL04***	***QKD***
Communication Distance	**Long-distance (intercontinental)**	Moderate distance	Moderate distance	Moderate distance
Security Level	**High (no key exchange required)**	**High (can transmit secure messages without key exchange)**	**High (can transmit secure messages without key exchange)**	**High (key exchange fundamental)**
Implementation Complexity	Moderate (enhanced by PAT technologies)	High (requires quantum memory)	Moderate (no quantum memory required)	**Low (proven by ample experimentation)**
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)

The advent of the Web 3.0 period has led to major transformations in our engagement with the Internet and its various applications. The essence of Web 3.0 lies in its decentralized, distributed, and user-centric structure, empowering users to manage their data, identity, and privacy. This scenario also paves the way for diverse economic interactions, encompassing direct peer transactions, intelligent transactions, and digital assets.

Nevertheless, the practical application of quantum communication, particularly in long-distance free-space contexts, faces significant hurdles that must be overcome to fully realize the globalization of Web 3.0 networks. Current quantum communication techniques such as QKD are unable to achieve practical secure satellite-based long-distance direct data transmission yet.

In the evolution of satellite-based QKD, significant strides have been made since the launch of the Micius satellite in 2017, demonstrating secure quantum key transmission over intercontinental distances [3,5,6]. These advancements include ground-to-satellite quantum teleportation [3], air-to-ground quantum communication [4], and satellite-based entanglement distribution [5]. However, challenges such as substantial signal loss, atmospheric interference, and the need for precise alignment and tracking remain [4–6].

Zhou et al. addressed some of these issues with device-independent QSDC protocols [7]. Zhang et al. demonstrated QSDC over 100 km, highlighting its scalability [8]. Liu et al. discussed the infrastructure needed for global QSDC networks, including numerous satellites and ground stations [9]. Zhou et al. emphasized the importance of integrating quantum repeaters to extend QSDC's reach [10]. And more works by many scientists continue to advance the field of QSDC[11–13]

Despite many advancements, practical deployment of satellite-based QSDC still faces significant hurdles, requiring continued research and development to achieve scalable, secure quantum communication networks[14].

Challenges with QKD for Global Scale Communication: QKD systems experience significant signal loss and attenuation over long distances, limiting practical distances without quantum repeaters to a few hundred kilometers. Atmospheric disturbances further exacerbate signal degradation in free-space QKD, making it highly susceptible to environmental factors. For instance, substantial signal loss and atmospheric interference hinder the efficiency of QKD in long-distance communications

Extending QKD reach beyond terrestrial limits with satellites introduces additional challenges, including precise satellite alignment and significant signal loss during transmission. Implementing a global QKD network requires substantial infrastructure, including numerous satellites and ground stations, and the integration of quantum repeaters. The high cost and complexity of this infrastructure pose barriers to widespread adoption

 doi:10.20944/preprints202409.0656.v1

Advantages of QSDC for Global Scale Communication In contrast, QSDC protocols, particularly our solution LF QSDC, offer more practical solutions for global communication. QSDC allows direct transmission of secure messages without prior key exchange, reducing communication complexity and eliminating intermediate key management. Additionally, QSDC protocols incorporate eavesdropping detection through quantum state disturbance, ensuring real-time detection of interference. Technologies like Quantum-Aware Low-Density Parity-Check (LDPC) coding, Pointing, Acquisition, and Tracking (PAT) systems, and Atmospheric Quantum Correction Algorithms (AQCA) improve LF QSDC reliability over long distances. These technologies address key challenges in satellite-based free-space communication, ensuring precise alignment and minimizing signal loss due to atmospheric disturbances. LF QSDC's reliance on advanced error correction and adaptive technologies reduces the need for extensive infrastructure compared to QKD, making it more scalable and cost-effective. By leveraging existing satellite and communication infrastructure with minimal modifications, LF QSDC can be integrated seamlessly into current systems.

Thus, while QKD has laid the groundwork for secure quantum communication, its limitations in signal loss, infrastructure requirements, and susceptibility to environmental factors make it less suitable for global-scale applications. QSDC protocols, particularly LF QSDC, present a more robust and practical solution for long-distance secure communication, offering enhanced security, scalability, and cost-effectiveness.

To address the challenge of a practical, secure, and long-distance quantum communication protocol, this research proposes a novel protocol, LF QSDC. LF QSDC is based on memory-free DL04 protocol [15] and incorporates our novel lossless transmission system which includes a Quantum-Aware LDPC coding scheme, PAT technologies, and AQCA.

Recent advancements in QSDC and supporting fields have shown significant theoretical and experimental progress, enhancing the feasibility of direct quantum communications[16–21]. Noteworthy developments include the realization of QSDC over 100 km using time-bin and phase quantum states underlines the scalability of these technologies[10].

The memory-free DL04 protocol contributes to these advancements by facilitating secure quantum communication without the need for a shared secret key and bypassing the necessity for quantum memory. This protocol ensures the integrity of quantum communication through immediate state preparation and encoding, followed by direct transmission to the receiver. This process is detailed as follows[10]:

1. **Quantum State Preparation:** Bob prepares qubits in one of the four initial states: $\{|0\rangle, |1\rangle\}$ (polarization states) or $\{|+\rangle, |-\rangle\}$ (phase states), forming the basis of the communication.
2. **Initial Transmission to Alice:** Bob sends these qubits to Alice via the quantum channel.
3. **Eavesdropping Detection:** Alice randomly selects some received qubits for immediate measurement in basis X or Z. The results are communicated to Bob through the classical service channel. Bob then verifies if the measured qubits match the initially prepared states. Any discrepancy indicates potential eavesdropping by Eve, causing the process to terminate if the error rate (e_e) exceeds a predefined threshold. Otherwise, Alice and Bob proceed to estimate the secrecy capacity (C_s).
4. **Message Encoding:** Alice encodes the message bits (M_k) into codewords (C_{nc}) using a predetermined coding scheme.
5. **Photon Modulation:** Alice modulates the remaining qubits by applying either the identity operator (I) or the unitary operator (U) based on the bit values '0' or '1' of C_{nc}. These modulated photons are then stored in a quantum memory.
6. **Return Transmission to Bob:** The modulated photons are sent back to Bob through the same quantum channel.
7. **Demodulation and Decoding:** Bob demodulates the received photons to retrieve the codewords (C'_{nc}), then decodes these to extract the original message (Y_k).

Key Features and Advantages

 doi:10.20944/preprints202409.0656.v1

- **Eavesdropping Detection:** The immediate measurement of randomly selected qubits allows Alice and Bob to detect any interference by Eve, leveraging the fundamental principles of quantum mechanics where any measurement alters the quantum state.
- **Quantum Memory Utilization:** Unlike protocols that operate memory-free, DL04 requires quantum memory, ensuring qubits are stored securely between initial transmission and modulation. This aids in maintaining the integrity and sequence of transmitted qubits.
- **Secrecy Capacity Estimation:** The protocol allows for precise estimation of the secrecy capacity (C_s), which is crucial for determining the security of the communication channel.
- **Two-Way Transmission:** The bidirectional flow of qubits between Alice and Bob enhances the robustness of the protocol by providing an additional layer for detecting and mitigating eavesdropping attempts.

The memory-free DL04 protocol that FL QSDC employs reduces the complexity of quantum state storage and management, making the system more practical and robust for real-world applications [15] as shown in Table I. Our novel 1uantum-aware LDPC coding scheme, PAT technologies, and AQCA mitigate issues related to atmospheric turbulence and alignment errors, which are prominent in satellite-based free-space quantum communication. Our innovative features are based on the developments of these works [22–27].

This paper delves into a strategy for incorporating LF QSDC into Web 3.0 frameworks to combat quantum dangers, in harmony with the decentralized nature of Web 3.0. Integrating LF QSDC technically with Web 3.0 demands an innovative method. It's necessary to modify Web 3.0 protocols to integrate LF QSDC's direct transmission features. This demands progress in quantum communication technologies and the evolution of Web 3.0 architecture to facilitate such integration.

The main contributions of this article are summarized as follows:

1. Introduction of a novel LF QSDC system designed for Web 3.0 networks.
2. Introduction of a detailed and practical road map to the implementation of LF QSDC into global communication networks.
3. Development and optimization of a quantum-aware LDPC and PAT technology to enhance quantum communication reliability and efficiency.
4. Proposal of a novel AQCA aimed at mitigating atmospheric disturbances and improving security over long distances satellite communication.

We will first give an overview of our proposed LF QSDC system. Then, we will detail our innovative designs of quantum-aware LDPC, PAT technologies, and atmospheric quantum correction algorithms. Finally, we will present our implementation plan for the LF QSDC and discuss the implications of our findings for global communication networks.

2. Long-Distance Free-Space QSDC Overview

This section introduces long-distance free-space quantum secure direct communication (QSDC). Our investigation delves into how advanced technologies can surmount existing constraints, rendering QSDC viable for widespread application both in the open air and across space through satellite communication. The process initiates by setting up the quantum state, marking the first phase in encoding quantum information 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. 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, sending it across free space, potentially covering vast distances including satellite-to-ground communication paths. Upon reaching the destination, the quantum signal is measured in a critical phase where the encoded quantum information is detected and interpreted.

 doi:10.20944/preprints202409.0656.v1

Finally, the process concludes with information decoding, where the quantum data is translated back into classical information for use.

Figure 1 shows the overview of LF QSDC:

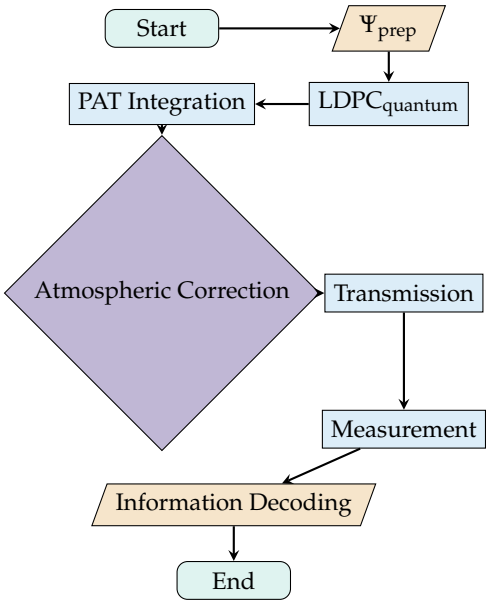

Figure 1. Flowchart showing the overview of FL QSDC

2.1. Quantum State Preparation and Encoding

The LF QSDC protocol starts with Alice preparing and encoding quantum states in a highly structured manner. She uses two parameters, a_0 and a_1, to determine the quantum state based on the required information:

2.1.1. Basis Determination (a_0):

- If $a_0 = 0$, the basis is computational, with states $\{|0\rangle, |1\rangle\}$.
- If $a_0 = 1$, the basis is superpositional, where a_1 further dictates the specific state:
  - $a_1 = 0$: State becomes $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$
  - $a_1 = 1$: State becomes $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$

Alice also selects a third parameter, a_2, which applies a phase shift to the encoded states:

- If $a_2 = 0$, the phase states remain as initially encoded.
- If $a_2 = 1$, the phase states are swapped:
  - $|0\rangle + |1\rangle$ becomes $|0\rangle - |1\rangle$ and vice versa.

These encoded quantum states are then transmitted to Bob, who has a crucial role in their measurement.

2.2. Measurement Protocols and Two-Way Communication

Upon receiving the quantum states, Bob's task is to measure them accurately, which requires selecting the appropriate basis for measurement based on preliminary information shared by Alice. Bob randomly selects a measurement basis, theta (θ), which dictates his measurement strategy:

- If $\theta = 0$, he measures in the basis:

$$\{|0\rangle, |1\rangle\} \tag{1}$$

 doi:10.20944/preprints202409.0656.v1

- If $\theta = 1$, he measures in the basis:

$$\left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\} \tag{2}$$

After measurement, Bob announces his choice of θ and the results of his measurements. Alice and Bob then jointly analyze the outcomes to check if θ aligns with a_2 ($a_2 \oplus \theta = 0$ or 1), ensuring the correct basis was used and the transmission was secure. This process embodies the two-way communication required by the DL04 protocol, where feedback from Bob influences potential retransmissions by Alice or adjustments in the encoding strategy to correct any discrepancies or enhance security.

2.3. Integration of Advanced Quantum Technologies

The effective transmission of quantum states over long distances is fraught with potential disturbances such as atmospheric turbulence, scattering, and absorption. To mitigate these effects and enhance the fidelity of the quantum channel, the following technologies are integrated into our LF QSDC protocol:

1. **Quantum-Aware LDPC Coding:** Specifically designed for quantum information, these codes correct errors that occur during the quantum state transmission, thus ensuring that the integrity and secrecy of the data are maintained even over long distances.
2. **Pointing, Acquisition, and Tracking (PAT) Systems:** These technologies are critical for maintaining the alignment of the quantum communication link, especially in dynamic environments such as satellite communications, where precision pointing is crucial for successful data transmission.
3. **Atmospheric Quantum Correction Algorithms:** These algorithms are designed to compensate for the quantum signal degradation caused by the atmosphere. By correcting errors induced by atmospheric turbulence, these algorithms significantly improve the reliability and stability of the quantum channel.

2.4. Security Checking Process

To ensure the security of the QSDC protocol, a detailed security checking process is implemented. After the initial transmission and measurement phases, a verification step is conducted where Alice and Bob compare a subset of their data to check for any discrepancies. This process includes the following steps:

1. **Error Rate Estimation:** Alice and Bob share a portion of their measurement results to estimate the quantum bit error rate (QBER). If the QBER exceeds a predefined threshold, the communication is deemed insecure, and the process is aborted.
2. **Entanglement Verification:** By verifying the entanglement of the transmitted quantum states, Alice and Bob can ensure that no eavesdropping has occurred. This involves comparing the measurement results to check for correlations consistent with the expected entangled states.
3. **Classical Post-Processing:** Any discrepancies identified during the verification steps are corrected through classical post-processing techniques, such as error correction and privacy amplification. This ensures that the final shared data is secure and free from eavesdropping.

By incorporating these security measures, the LF QSDC protocol ensures the secure transmission of quantum information over long distances, making it suitable for practical applications in free-space and satellite-based communication systems.

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

This section delves into our innovative techniques for the secure and loss-free transmission of data over extensive distances via air or space.

 doi:10.20944/preprints202409.0656.v1

3.1. Quantum-Aware LDPC Coding

3.1.1. LDPC Code Parameter Optimization

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 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:
  $$\max\big(I(X;Y) - \lambda(\text{QBER}) - \delta(\text{Code Rate})\big) \tag{3}$$
  Subject to:
  $$\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}, \quad \rho(x) = \sum_{i=2}^{d_c} \rho_i x^{i-1} \tag{4}$$
  Here, δ represents the additional constraint related to the code rate.

Channel Adaptation:

- *Machine Learning Prediction and Iterative Update Algorithm:* a 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.

- *Pseudocode:*

```
# 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:
```

 doi:10.20944/preprints202409.0656.v1


```
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
```

3.1.2. Adaptive Decoding Algorithm with Graph Neural Network Enhanced Belief Propagation and Adaptive Iteration

We propose 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 fi- nal keys, significantly increasing transmission reliability and protection.

Standard BP Equation:

$$m_{i\to j}^{(t+1)} = 2\tanh^{-1}\left(\prod_{k\in N(i)\setminus j}\tanh\left(\frac{m_{k\to i}^{(t)}}{2}\right)\right) \tag{5}$$

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

$$m_{i\to j}^{(t+1)} = GNN(m_{i\to j'}^{(t)}, \text{features}) \tag{6}$$

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

Pseudocode:

 doi:10.20944/preprints202409.0656.v1


```
class GNNModel(torch.nn.Module):
    #Graph Neural Network model using GCN layers.
    def __init__(self, input_dim, hidden_dim, output_dim):
        super().__init__()
        self.conv1 = GCNConv(input_dim, hidden_dim) # First GCN layer
        self.conv2 = GCNConv(hidden_dim, output_dim) # Second GCN layer

    def forward(self, x, edge_index):
        x = F.relu(self.conv1(x, edge_index)) # Activation function
        return self.conv2(x, edge_index) # Output layer

def enhanced_bp(messages, gnn_model, edge_index, num_iterations):
    #Enhanced BP decoding with GNN model.
    for _ in range(num_iterations):
        messages_tensor = torch.tensor(messages, dtype=torch.float) # Messages to tensor
        messages = gnn_model(messages_tensor, edge_index).detach().numpy() # GNN model output
    return messages

def adaptive_decoding_algorithm(messages, channel_conditions, edge_index):
    #Adaptive decoding based on channel conditions.
    input_dim, hidden_dim, output_dim = messages.shape[1], 64, messages.shape[1]
    gnn_model = GNNModel(input_dim, hidden_dim, output_dim)
    T = 10 if channel_conditions['SNR'] > 10 else 20 # Iterations based on SNR
    adjusted_messages = enhanced_bp(messages, gnn_model, edge_index, T) # Decode with GNN
    return decode(adjusted_messages) # Final decoding
```

3.1.3. Security Enhancement Techniques

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.

Privacy Amplification:

- After decoding, apply a hash function H to the key to reduce its length and eliminate partial information[28,29].
- The process can be represented as:

$$K_{final} = H(K_{decoded}) \tag{7}$$

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

3.2. PAT Technologies

3.2.1. Design

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

 doi:10.20944/preprints202409.0656.v1

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.

3.2.2. Performance Evaluation and Optimization Algorithms

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:

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:

$$e_a = f(\theta_m, d) \tag{8}$$

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:

$$AEC = \arg\min_{\theta_p, \theta_t} e_a(\theta_p - \theta_t, d) \tag{9}$$

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.

Signal Acquisition:

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

$$P_a = g(SNR, \sigma) \tag{10}$$

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:

$$SAC = \arg\max_{SNR, \sigma} P_a(SNR, \sigma) \tag{11}$$

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.

Pointing Stability:

 doi:10.20944/preprints202409.0656.v1

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

$$S_p < \frac{\lambda}{D_{eff}} \tag{12}$$

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:

$$PSA = \arg \min_{\Delta\theta_p, \Delta\theta_t} S_p(\Delta\theta_p, \Delta\theta_t) \tag{13}$$

where $\Delta\theta_p$ and $\Delta\theta_t$ 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.

3.3. Atmospheric Quantum Correction Algorithm

3.3.1. Design

AQCA is integrated within the LF 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.

3.3.2. Mathematical Formulation

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

Modeling Atmospheric Disturbances:

The Kolmogorov theory models the atmospheric turbulence. 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 fluctuations 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:

$$\sigma_I^2 \approx 1.23 C_n^2 k^{7/6} L^{11/6} \tag{14}$$

The atmospheric absorption is modeled by the Beer-Lambert law. 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:

$$T = e^{-\alpha L} \tag{15}$$

 doi:10.20944/preprints202409.0656.v1

The Mie theory models atmospheric scattering. 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:

$$\sigma_s = \frac{2\pi^5 d^6}{3\lambda^4} \left(\frac{n^2 - 1}{n^2 + 2} \right)^2 Q_{ext} \tag{16}$$

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 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.

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.

3.4. Integration with LF 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.

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.

 doi:10.20944/preprints202409.0656.v1

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.

4. LF 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.

4.1. Simulation Plan

Figure 2 outlines the process of the simulation plan:

 doi:10.20944/preprints202409.0656.v1

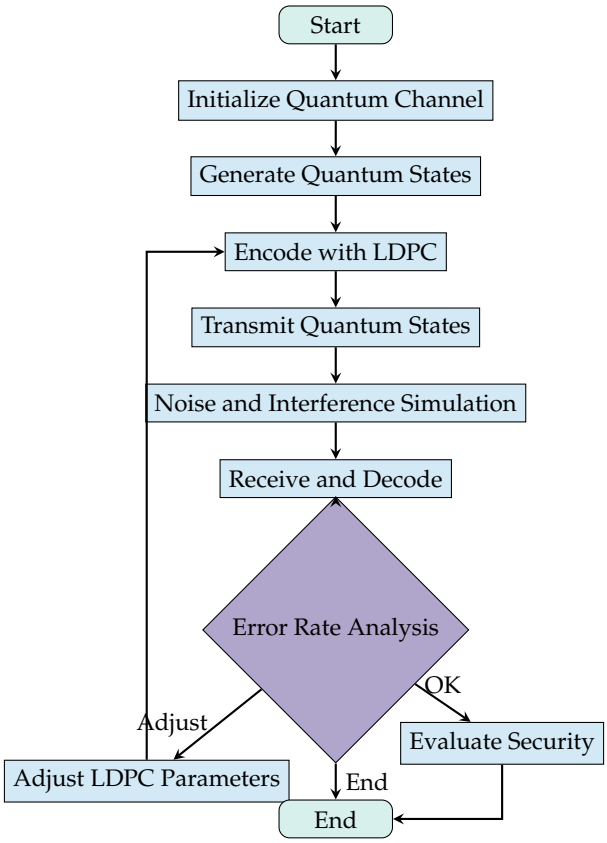

Figure 2. Flowchart outlining the overview of our simulation plan

The testing framework for the LF QSDC system meticulously evaluates its operational efficacy, commencing with the initialization of the quantum channel ($\mathcal{Q}_C$), 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 (Φ_{transmit}), where encoded quantum states are dispatched through the free-space medium, encountering environmental noise ($\mathcal{N}$), 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 ($\epsilon_{\text{quantum}}$). 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 (Σ_{security}) is conducted to ensure the system's robustness against potential eavesdropping attempts, affirming the LF QSDC system's ability to preserve the secrecy and accuracy of the information sent.

4.2. 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.

Figure 3 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 [32].

 doi:10.20944/preprints202409.0656.v1

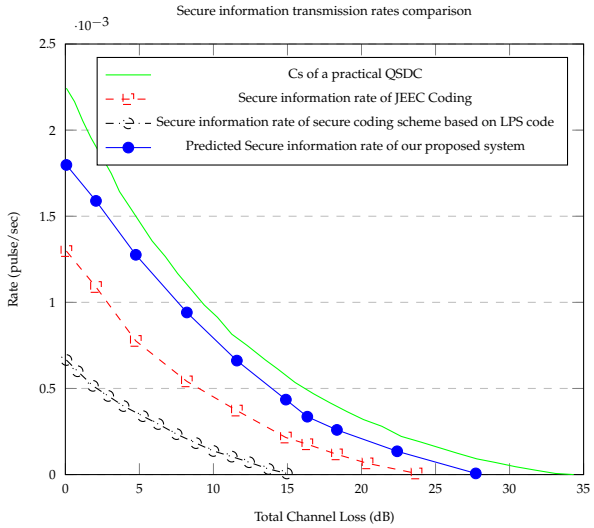

Figure 3. Graph showcasing the predicted secure information transmission rates of the proposed transmission scheme, the secure coding based on JEEC Coding, the secure coding based on LPS codes, and Cs for a practical QSDC system, without the consideration of the loss caused by the delayed fiber

Our estimations for our proposed system's performance are substantiated by empirical evidence and mathematical proofs from recent research such as works by Hu et al. and Babar et al. and[30,31]. Specifically, studies by Roffe [33] on quantum LDPC codes and by Ghilea [34] 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 [35] 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.

5. Implementation Plan for LF QSDC

5.1. Technical Implementation of LF QSDC

5.1.1. 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 influencing communication [36]. 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 [37–39]. Figure 4 summarizes the main characteristics of the free-space channel and their impacts on optical signal transmission.

 doi:10.20944/preprints202409.0656.v1

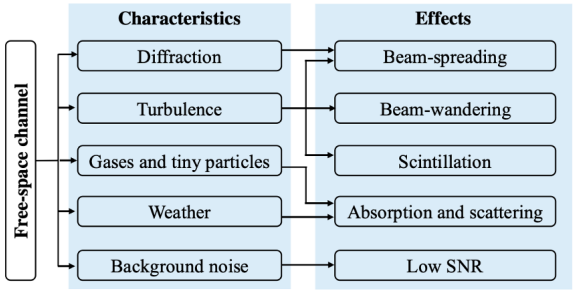

Figure 4. Summarizes the main characteristics of free-space channel and their impacts on optical signal transmission[62]

Consequently, one-way transmission methods like RE-CON or QKPC protocols might offer greater benefits than the two-way approaches used in LF QSDC [40]. 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 [41,42].

5.1.2. Experimental Implementation

In 2020, there was a reported successful experimental setup of the free-space DL04 QSDC protocol. The setup, as shown in Figure 5, 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 $0.49\% \pm 0.27\%$[62].

Attaining a low QBER in experiments is a key measure of QSDC's resilience and dependability in free-space channels [44]. A minimal QBER indicates the ability to convey quantum data with great accuracy, crucial for ensuring secure communication demonstrated by both works in QSDC and QKD [45–47]. 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 [62].

The experimental arrangement employed a phase encoding technique to transmit quantum states in a vacuum. 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. 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 [64].

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[62]. For LF QSDC, this characteristic is crucial, given the paramount importance of safeguarding communication from eavesdropping.

Included in the experimental arrangement were also systems for identifying eavesdropping, an essential element of secure quantum communication. A protocol's capacity to adjust pulses for security verifications and secure information encoding showcases its effectiveness in maintaining communication confidentiality and integrity is crucial and achieveavle, even amidst possible risks as demonstrated by this experiment and Pan et al.[43].

The success of these experiments confirms the practicality of LF QSDC, showcasing the protocol's capacity to convey quantum data with great accuracy and safety via free-space channels.

 doi:10.20944/preprints202409.0656.v1

5.2. Feasibility and Adaptability of Satellite-based QSDC

5.2.1. Feasibility of Satellite Communication with LF 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[48–50]. 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[50].

The DL04 protocol, devoid of memory, plays a crucial role in LF QSDC by simplifying the processes of quantum state storage and management [19]. The DL04 protocol's LF flexibility 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. The incorporation of quantum-aware LDPC coding into LF QSDC markedly enhances the system's error rectification abilities, tackling the problems caused by extensive transmission and atmospheric influences [51–53]. Furthermore, the use of PAT technologies helps sustain a consistent and precise communication connection between satellites and terrestrial stations [54].

5.2.2. Expanding Feasibility with LF QSDC

Enhancing the feasibility of LF QSDC involves comprehensive advancements across various technical and regulatory dimensions. Key initiatives include refining beam propagation and encoding methods to counter atmospheric disturbances and environmental disruptions as shown in Figure 5, ensuring high communication accuracy and low Quantum Bit Error Rate (QBER) across vast distances [55,56]. Additionally, integrating quantum repeaters and relay satellites expands the scope of QSDC, enabling a global quantum communication network that overcomes spatial limitations inherent in direct quantum communication [57]. Improvements in daylight operation capabilities through advanced detectors and narrowband filters are crucial for QSDC's effectiveness in satellite applications, addressing challenges posed by solar radiation [58].

Further, merging QSDC systems with existing satellite communication infrastructures requires addressing payload capacity, energy needs, and upgrade compatibility, ensuring effective implementation of quantum communication methods [59]. Promoting standardization and interoperability among quantum communication systems through uniform protocols and error-correcting techniques is essential for establishing a scalable and unified global network [60]. Developing regulatory and policy frameworks is also critical for overseeing the application and ensuring the security and privacy of satellite-based quantum communication, addressing potential legal and security issues [61]. These collective efforts will significantly enhance the practicality of satellite-based LF QSDC, paving the way for a secure and efficient global quantum communication network.

5.3. Web 3.0 Compatibility

The integration of LF QSDC with Web 3.0 technologies marks a pivotal advancement in securing decentralized networks through quantum communication methods. This collaboration aims to create a secure transactional layer within Web 3.0, enabling nodes to directly and securely exchange data, thereby enhancing transaction secrecy and reliability against both conventional and quantum cryptographic threats [62–64]. Furthermore, the adaptation of LF QSDC within Web 3.0 involves developing quantum-resistant smart contracts, ensuring their execution and outcomes are secured through quantum communication, thus requiring smart contract systems to support encryption and verification processes compatible with LF QSDC protocols [65–67].

Additionally, LF QSDC contributes to Web 3.0's goals of user privacy and anonymity by establishing secure, direct communication channels that eliminate the need for intermediaries in key

 doi:10.20944/preprints202409.0656.v1

exchanges or transaction verifications. This approach not only strengthens confidentiality within the network but also introduces an additional layer of transaction security based on quantum mechanics, offering a robust defense against potential quantum cryptographic attacks [68].

For LF QSDC's successful integration into Web 3.0, it must align with existing protocols, modifying transaction verification systems to accommodate quantum-secured information and ensuring the ledger supports and accurately documents quantum-secured transactions [69–71]. Additionally, considering the increasing transaction volumes on Web 3.0 networks,

5.4. Stages of Gradual Implementation

Figure 6 summarizes the overview of the stages of gradual implementation:

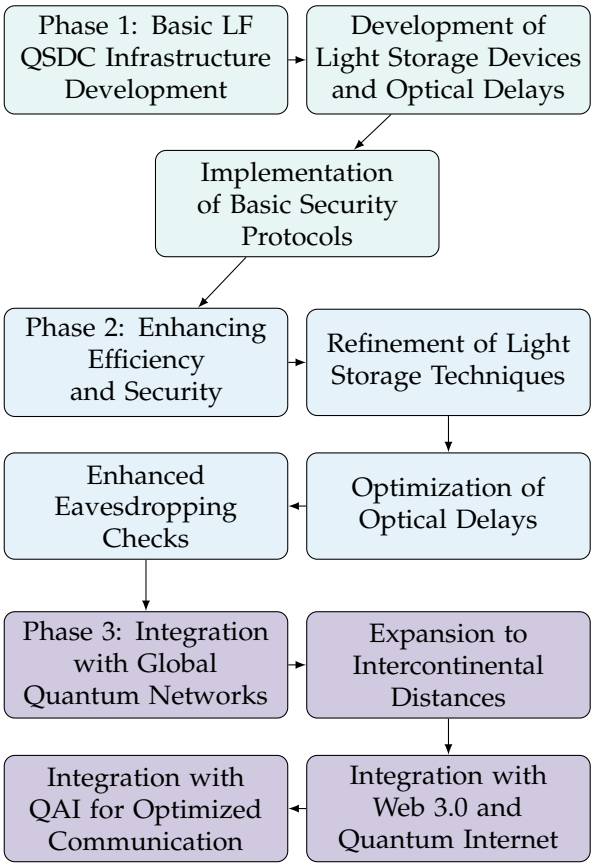

Figure 6. Flowchart showing the overview of the stages of gradual implementation

5.4.1. Phase 1: Development of Basic LF QSDC Infrastructure

The initial configuration focuses on establishing a basic system to create, store, and transmit entangled photon pairs between two locations, Alice and Bob, requiring optical systems like photon sources, detectors, and communication channels. Future efforts will explore light storage devices using electromagnetic transparency and optical delays for sequential EPR pair production, aiming to integrate these technologies into LF QSDC and set up security measures to detect eavesdropping and evaluate secure communication efficiency.

5.4.2. 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 LF QSDC. Enhance the application of optical lags to guarantee accurate

 doi:10.20944/preprints202409.0656.v1

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.

5.4.3. Phase 3: Integration with Global Quantum Networks

This stage entails partnering with current quantum communication endeavors to establish a cohesive and secure network of quantum communication. Combine LF 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.

5.5. Business Case of LF QSDC in The Web 3.0 Era

Integrating LF QSDC with Web 3.0 represents a significant advancement in securing decentralized networks against quantum computing threats, emphasizing its transformative potential for Web 3.0's security and trust mechanisms in an increasingly digital and quantum-aware world [56]. This integration addresses the vulnerabilities of traditional cryptographic methods to quantum computing by offering a quantum mechanics-based solution for secure, direct communication over long distances without intermediaries, significantly enhancing Web 3.0's security posture and ensuring sustained trust and reliability [62].

The necessity for quantum-resistant security protocols in Web 3.0 is increasingly critical, with LF QSDC fulfilling this requirement by providing a secure, scalable, and efficient framework. This advancement not only protects against future quantum threats but also reinforces defenses against sophisticated conventional attacks, positioning Web 3.0 networks at the cutting edge of secure digital technology. The integration of LF QSDC into Web 3.0 is especially pertinent as the adoption of Web 3.0 expands across various sectors, highlighting the growing demand for robust security solutions in the face of quantum computing's rise and offering a competitive advantage to early adopters [62].

However, integrating LF QSDC into Web 3.0 comes with challenges, including technological complexity and interoperability issues. Strategic partnerships, ongoing research and development, and adaptable integration strategies are essential for mitigating these risks and staying abreast of quantum computing advancements. Despite initial costs related to research, technology acquisition, and system upgrades, the long-term benefits of enhanced security and network durability justify the investment, promising increased user confidence and new opportunities in quantum-secure technologies [62]. The strategic incorporation of LF QSDC into Web 3.0 not only fortifies network security but also positions Web 3.0 networks as leaders in the next era of digital innovation, ready for the challenges of the quantum computing age.

6. Discussion

6.1. Comparison With Similar Protocols

6.1.1. Security

LF 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, LF 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

 doi:10.20944/preprints202409.0656.v1

nature of the Web 3.0 era. LF QSDC and DL04 both offer high levels of security based on quantum principles; however, LF 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 [72,73]. Additionally, LF 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.

6.1.2. 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)[74]. This showcases LF 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[8,75].

6.1.3. Channel Loss and Atmospheric Disturbances

LF 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[74].

6.1.4. Cost

Implementing LF QSDC, especially for applications such as global Web 3.0 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 LF QSDC in various applications.

6.2. 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.

LF 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 LF 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.

 doi:10.20944/preprints202409.0656.v1

Furthermore, LF 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 LF QSDC system which comes with its own limitations and challenges as discussed below:

6.2.1. Theoretical Challenges

- Quantum Decoherence and Noise: Quantum states are highly susceptible to decoherence and environmental noise, which can severely limit the distance over which LF QSDC can be effectively implemented.
- Security Proofs: Complete, universally accepted security proofs for LF QSDC under all potential attack scenarios are challenging to develop, raising concerns about its absolute security.

6.2.2. 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.

6.2.3. Implementation Challenges

- Infrastructure Development: Establishing a global LF 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.

6.2.4. Impact Considerations

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

7. Conclusions

This document delves into the integration of distant, free-space quantum secure direct communication in the digital age of Web 3.0, introducing a theoretical model aimed at enhancing the security aspects of the worldwide networking structure in the quantum age. This document highlights LF QSDC's capability to strengthen the Web 3.0 framework against various cryptographic dangers, including quantum and classical, by utilizing direct quantum communication, bypassing traditional key exchange methods.

LF QSDC's core is based on the memory-free DL04 protocol, implemented by merging quantum-aware, low-density parity-check codes, sophisticated pointing, acquisition, and tracking technologies, along with algorithms for atmospheric quantum correction. These factors play a crucial role in overcoming current environmental and technical challenges that hinder the effective

 doi:10.20944/preprints202409.0656.v1

use of quantum communication technologies, especially in the realm of long-distance free-space communication. Additionally, we suggest a strategic plan that includes the development of quantum communication technologies, integrating them with the current Web 3.0 framework, and overcoming environmental and technical hurdles to ensure a secure and efficient data transmission channel.

Implementing LF QSDC in Web 3.0 networks presents intricate engineering hurdles and necessitates significant progress in quantum communication technology. Upcoming studies might focus on creating advanced quantum error correction methods to improve the accuracy of quantum data transmission. Furthermore, investigating cutting-edge PAT systems to enhance the stability and precision of quantum signal alignment might greatly aid in the practicality of LF QSDC. Developing scalable quantum network structures for effortless integration with current Web 3.0 systems is another vital field for future research, guaranteeing that quantum security improvements do not hinder the network's operational efficiency or accessibility.

8. Acknowledgement

Author Contributions: These authors contributed equally: Yew Kee Wong, Yifan Zhou, Xinlin Zhou, Yan Shing Liang, and Zi Yan Li.

Under the guidance of Yew Kee Wong, Yifan Zhou, Yan Shing Liang, Xinlin Zhou, and Zi Yan Li conducted the research with Yifan Zhou and Yan Shing Liang leading the methodology development. The original draft was primarily written by Yifan Zhou, with significant contributions from Xinlin Zhou, Zi Yan Li, and Yan Shing Liang. Xinlin Zhou also undertook the task of reviewing and editing the manuscript. Yew Kee Wong supervised the project, provided revisions, and managed project administration.

9. Data Availability

The datasets analyzed during the current study are available from the corresponding author on reasonable request.

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. J. G. Ren et al., "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70-73, Sept. 2017.
4. S. Nauerth et al., "Air-to-ground quantum communication," *Nature Photonics*, vol. 7, pp. 382-386, June 2013.
5. Q. Zhang et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140-1144, June 2017.
6. J. Yin et al., "Satellite-based quantum-secure time transfer," *Nature Communications*, vol. 11, no. 1, Article no. 4186, Aug. 2020.
7. L. Zhou, Y. B. Sheng, and G. L. Long, "Device-independent quantum secure direct communication against collective attacks," *Sci. Bull. (Beijing)*, vol. 65, no. 1, pp. 12-14, 2020.
8. H. Zhang et al., "Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states," *Light: Science & Applications*, vol. 11, no. 1, p. 83, 2022.
9. X. Liu, D. Luo, G. L. Lin, Z. H. Chen, C. F. Huang, S. Z. Li, C. X. Zhang, Z. R. Zhang, and K. J. Wei, "Fiber based quantum secure direct communication without active polarization compensation," Sci. China Phys. Mech. Astron., vol. 65, no. 12, p. 120311, 2022.
10. L. Zhou, B. W. Xu, W. Zhong, and Y. B. Sheng, "Device-independent quantum secure direct communication with single-photon sources," Phys. Rev. Appl., vol. 19, no. 1, p. 014036, 2023.
11. I. Paparelle, F. Mousavi, F. Scazza, A. Bassi, M. Paris, and A. Zavatta, "Practical quantum secure direct communication with squeezed states," arXiv:2306.14322, 2023.
12. Y. B. Sheng, L. Zhou, and G. L. Long, "One-step quantum secure direct communication," Sci. Bull. (Beijing), vol. 67, no. 4, p. 367, 2022.

13. L. Zhou and Y. B. Sheng, “One-step device-independent quantum secure direct communication,” Sci. China Phys. Mech. Astron., vol. 65, no. 5, p. 250311, 2022.
14. D. Pan et al., "The Evolution of Quantum Secure Direct Communication: On the Road to the Qinternet," in *IEEE Communications Surveys & Tutorials*, doi: 10.1109/COMST.2024.3367535
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*, vol. 68, no. 9, pp. 5778–5792, 2020.
16. 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.
17. 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.
18. L. Yin, C. Jiang, C. Jiang, N. Ge, L. Kuang, and M. Guizani, “A communication framework with unified efficiency and secrecy,” *IEEE Wireless Communications*, vol. 26, no. 4, pp. 133–139, 2019.
19. F. Deng and G. Long, “Secure direct communication with a quantum one-time pad,” *Phys. Rev. A*, vol. 69, no. 5, p. 052319, 2004.
20. 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.
21. Y. X. Xiao, L. Zhou, W. Zhong, M. M. Du, and Y. B. Sheng, “The hyperentanglement-based quantum secure direct communication protocol with single-photon measurement,” Quantum Inform. Process., vol. 22, no. 9, p. 339, 2023.
22. M. Bailly, E. Perez, “Pointing, acquisition, and tracking system of the European SILEX program: a major technological step for intersatellite optical communication,” in *Free-Space Laser Communication Technologies III*, vol. 1417, pp. 142-157, 1991.
23. I. B. Djordjevic, O. Milenkovic, and B. Vasic, “Generalized low-density parity-check codes for optical communication systems,” *J. Lightwave Technol.*, vol. 23, no. 5, pp. 1939–1946, 2005.
24. 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.
25. 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. Workshops*, IEEE, 2018, pp. 1–6.
26. C. Wang, F. Deng, G. Long, “Multi-step quantum secure direct communication using multi-particle Green–Horne–Zeilinger state,” *Optics Communications*, vol. 253, nos. 1-3, pp. 15–20, 2005.
27. P. Maunz, D. Moehring, S. Olmschenk, et al. “Quantum interference of photon pairs from two remote trapped atomic ions,” *Nature Phys*, vol. 3, pp. 538–541, 2007.
28. C. Bennett, H., G. Brassard, C. Crépeau, and U. M. Maurer. “Generalized privacy amplification,” *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915-1923, 1995.
29. J. Carter, L., and M. N. Wegman. “Universal classes of hash functions,” *J. Comput. Syst. Sci.*, vol. 18, no. 2, pp. 143-154, 1979.
30. 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*, vol. 5, no. 9, e16144, 2016.
31. Z. Babar, P. Botsinis, D. Alanis, S. X. Ng, and L. Hanzo. “Fifteen years of quantum LDPC coding and improved decoding strategies,” *IEEE Access*, vol. 3, pp. 2492–2519, 2015.
32. Z. Zhou, Y. Sheng, P. Niu, L. Yin, G. Long, and L. Hanzo. “Measurement-device-independent quantum secure direct communication,” *Science China Physics, Mechanics & Astronomy*, vol. 63, no. 3, 230362, 2020.
33. 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
34. 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
35. 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
36. S. Zafar and H. Khalid, “Free space optical networks: applications, challenges and research directions,” *Wireless Personal Communications*, vol.

37. H. Kaushal, V. K. Jain and S. Kar, "Free-space optical channel models," in Free Space Optical Communication, New Delhi, India: Springer, 2017, pp. 9-41.
38. A. M. Al-Kinani, A. A. Al-Habash, A. A. Al-Habash and A. A. Al-Habash, "A survey of hybrid free space optics communication networks to overcome atmospheric turbulence," Entropy, vol. 24, no. 11, p. 1573, 2022.
39. A. Avella et al., "Characterization of free-space quantum channels," arXiv preprint arXiv:1810.05700, 2018.
40. T. Ye, and Z. Ji, "Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states", arXiv preprint arXiv:2205.04631, 2021.
41. M.Xiao, and C. Ma, "Fault-tolerant quantum private comparison protocol", International Journal of Theoretical Physics, vol. 61, no. 1, p. 41, 2022.
42. J. Liu, Q. Wang, Y. Yang, and Q. Wen, "Quantum private comparison protocol based on high-dimensional quantum states", Quantum Information Processing, vol. 13, no. 11, pp. 2391-2404, 2014.
43. Pan D, Lin Z, Wu J, et al. Experimental free-space quantum secure direct communication and its security analysis[J]. Photonics Research, 2020, 8(9): 1522-1531.
44. R. Qi, Y. Zhang, S. Wang, H. Li, Z. Wang, S. Wang, X. Chen, and J.-W. Pan, "Experimental demonstration of free-space quantum secure direct communication with single photons", Light: Science and Applications, vol. 9, no. 1, p. 28, 2020.
45. G. Vallone et al., "Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels", arXiv preprint arXiv:1404.1272, 2014.
46. L.-C. Xu, H.-Y. Chen, N.-R. Zhou, and L.-H. Gong, "Multi-party semi-quantum secure direct communication protocol with cluster states", International Journal of Theoretical Physics, vol. 59, no. 6, pp. 2175-2186, 2020.
47. R. Qi et al., "Implementing a practical quantum secure direct communication system," Light: Science and Applications, vol. 8, no. 1, p. 21, 2019.
48. J.-G. Ren et al., "Ground-to-satellite quantum teleportation," Nature, vol. 549, no. 7670, pp. 70-73, 2017.
49. S.-K. Liao et al., "Satellite-to-ground quantum key distribution," Nature, vol. 549, no. 7670, pp. 43-47, 2017.
50. A. V. Khmelev et al., "Semi-Empirical Satellite-to-Ground Quantum Key Distribution Model for Realistic Receivers," Entropy, vol. 25, no. 4, p. 670, 2023.
51. P. Panteleev and G. Kalachev, "Degenerate Quantum LDPC Codes With Good Finite Length Performance," Quantum, vol. 5, p. 585, 2021.
52. P. Panteleev and G. Kalachev, "Layered Decoding of Quantum LDPC Codes," IEEE Transactions on Information Theory, vol. 66, no. 8, pp. 5198-5209, 2020.
53. J. Roffe, "Towards practical quantum LDPC codes," Quantum Views, vol. 5, p. 63, 2021.
54. M. T. Toledo, "Process Analytical Technology (PAT) - Enhance Quality and Efficiency," 2021. [Online].
55. J. Wang et al., "Direct and full-scale experimental verifications towards ground-satellite quantum key distribution," Nature Photonics, vol. 7, no. 5, pp. 387-393, 2013.
56. Z. Cao et al., "Continuous-Variable Quantum Secure Direct Communication Based on Gaussian Mapping," Physical Review Applied, vol. 16, no. 2, p. 024012, 2021.
57. S. Goswami and S. Dhara, "Satellite Relayed Global Quantum Communication without Quantum Memory," arXiv:2306.12421, 2021.
58. G. Long, H. Zhang "Practical quantum secure direct communication," 2020 Cross Strait Radio Science and Wireless Technology Conference (CSRSWTC). IEEE, 2020, 1-3.
59. V. E. Balasubramanian et al., "Quantum communication using satellites," Journal of Physics: Photonics, vol. 3, no. 3, p. 032001, 2021.
60. E. Perrier, "The Quantum Governance Stack: Models of Governance for Quantum Information Technologies," Digital Society, vol. 1, no. 1, p. 22, 2022.
61. M. Kop, "Establishing a Legal-Ethical Framework for Quantum Technology," Yale Journal of Law and Technology, vol. 23, no. 1, pp. 1-40, 2021.
62. 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.
63. F. Zhu et al., "Experimental long-distance quantum secure direct communication," arXiv:1710.07951, Oct. 2017.

64. S. Pirandola et al., "Advances in quantum cryptography," Adv. Opt. Photon., vol. 12, no. 4, pp. 1012–1236, Dec. 2020, doi: 10.1364/AOP.383547.
65. QANplatform, "Quantum-resistant security," [Online]. Available: https://learn.qanplatform.com/technology/technology-features/quantum-resistant-security.
66. J. Liu et al., "Quantum-secure blockchain with efficient verification based on quantum key distribution," Sci. Rep., vol. 10, Article 10677, Jul. 2020, doi: 10.1038/s41598-020-67612-3.
67. A. Kayal and S. Mandal, "Quantum secure direct communication using quantum key distribution and quantum encryption," in Proc. IEEE Int. Conf. Adv. Comput. Commun. Inform. (ICACCI), Bangalore, India, Sep. 2018, pp. 1566–1571, doi: 10.1109/ICACCI.2018.8554768.
68. Min-Jie W, Wei P. Quantum secure direct communication based on authentication[J]. Chinese Physics Letters, 2008, 25(11): 3860.
69. J. Wang et al., "Drone-based entanglement distribution towards mobile quantum networks," Natl. Sci. Rev., vol. 7, no. 5, pp. 921–930, May 2020, doi: 10.1093/nsr/nwz206.
70. H. Yin et al., "Long-distance and secure quantum key distribution over a free-space channel," Nat. Photon., vol. 15, pp. 41–45, Jan. 2021, doi: 10.1038/s41566-020-00713-5.
71. M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th ed. Cambridge, U.K.: Cambridge Univ. Press, 2010.
72. A. K. Patra and S. K. Jana, "A new quantum secure direct communication protocol using decoherence-free subspace," arXiv:2211.15941, Nov. 2021, [Online]. Available:
73. S. Mexicana De Física 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," Revista Mexicana de Física, vol. 63, pp. 268–274, 2017, Accessed: Feb. 08, 2024. [Online]. Available: https://www.redalyc.org/pdf/570/57050507008.pdf
74. J. Yin et al., "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels," Nature, vol. 488, no. 7410, pp. 185–188, 2012, doi: https://doi.org/10.1038/nature11332.
75. X.-S. Ma et al., "Quantum teleportation using active feed-forward between two Canary Islands," 2012, Accessed: Feb. 08, 2024. [Online]. Available: https://arxiv.org/pdf/1205.3909.pdf