Counterfactual Quantum Byzantine Consensus for Human-Centric Metaverse

Saw Nang Paing, Jason William Setiawan, Muhammad Asad Ullah, Fakhar Zaman, Trung Q. Duong, *Fellow, IEEE*, Octavia A. Dobre, *Fellow, IEEE*, and Hyundong Shin, *Fellow, IEEE*

***Abstract*—Quantum Byzantine fault tolerance (BFT) consensus is a secure and reliable mechanism that enables network nodes to reach an agreement even in the presence of faulty nodes, by using distributed private correlated lists. It plays a crucial role in developing the blockchain-based Metaverse to ensure its integrity and security. In this paper, we propose a counterfactual quantum BFT (CQ-BFT) protocol for a multipartite network using *counterfactual unitary telecomputation* with the chained quantum Zeno gates. This consensus protocol achieves an agreement among the parties without the passage of any physical particles through the quantum channel. Due to the unique properties of counterfactual communication, we demonstrate that the CQ-BFT protocol can operate in the absence of a shared phase reference and provide a quantum layer of security and robustness against dephasing noise, fulfilling the stringent requirements of blockchain technology. In addition, we analyze the performance tradeoff of the CQ-BFT protocol in terms of the three pillars of blockchain—i.e., security, scalability, and decentralization. The human-centric Metaverse could leverage high degrees of security, noise resilience, and fault tolerance of the CQ-BFT protocol to enhance its underlying network infrastructure. This protocol leads to more robust and immersive virtual environments that prioritize the needs and experiences of Metaverse users.**

***Index Terms*—Blockchain, Byzantine consensus, counterfactual quantum communication, Metaverse, private list distributions.**

I. Introduction

METAVERSE, the convergence of physical and digital realities towards the virtual world, has recently become of great interest in the technological industry and research community [1]. The emergence of the Metaverse has been facilitated by the rapid advancements of blockchain, augmented reality, virtual reality, the Internet of Things, and distributed computing [2]. Recently, Facebook Inc. has rebranded itself as "Meta" to accelerate the realization of the Metaverse. This transformation aims to create an immersive environment where people can surpass their own personal and career growth expectations. Initially, the concept of Metaverse was focused on the convergence of physical and digital realities with less realizing the needs and interests of human beings. Later, the concept of a human-centric Metaverse has been introduced, which emphasizes the concerns of human beings. The ultimate goal is to enhance and enrich human lives with meaningful customized experiences. By prioritizing the human aspect, the human-centric Metaverse aims to create a user-centered virtual realm that provides valuable experiences and opportunities [3].

The potential benefits of the human-centric Metaverse are vast and significant [4], [5]. One of the most prominent benefits is the democratization of access to information and services. The Metaverse can provide an open and inclusive virtual space where individuals from diverse backgrounds can connect and engage with each other, leading to increased diversity, inclusivity, and social harmony [6]. Another significant benefit is the potential to improve mental health and well-being by providing a space for people to connect with others, participate in engaging activities, and escape from the stresses of the physical world [7]. Additionally, the Metaverse can enable new forms of economic activity and innovation by creating new opportunities for digital goods and services, virtual real estate, and blockchain-based transactions such as virtual theme parks, telesurgery, and cryptocurrency [2], [8]–[10].

To realize the human-centric metaverse, it is essential to decentralize digital platforms and address several challenges. One of the biggest challenges is ensuring the security and privacy of user data within the Metaverse. As users increasingly engage with the virtual world, their personal data and digital identities become more vulnerable to cyber threats, making it imperative to establish robust security measures [11]. Although blockchain is not the sole determining factor, it plays a significant role in shaping the evolution of the Metaverse with a primary focus on decentralization, security, and transparency. These characteristics make blockchain the underlying technology that transforms the human-centric Metaverse, creating a user-centered equitable environment [12]. However, the scalability of the underlying blockchain technology must be addressed to ensure that the Metaverse can handle the massive amounts of data generated by user activity [13]. Finally, environmental factors such as background noise

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (NRF-2019R1A2C2007037, NRF-2022R1A4A3033401) and by the MSIT (Ministry of Science and ICT), Korea, under the Convergence security core talent training business support program (IITP-2023-RS-2023-00266615) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). The work of T. Q. Duong was supported in part by the U.K. Royal Academy of Engineering (RAEng) under the RAEng Research Chair and Senior Research Fellowship scheme Grant RCSRF2021\11\41. The work of O. A. Dobre was supported in part by the Natural Sciences and Engineering Research Council of Canada (NSERC), through its Discovery program. *(Corresponding author: Hyundong Shin.)*

S. N. Paing, J. W. Setiawan, M. A. Ullah, F. Zaman, and H. Shin are with the Department of Electronics and Information Convergence Engineering, Kyung Hee University, 1732 Deogyeong-daero, Giheung-gu, Yongin-si, Gyeonggi-do 17104 Korea (e-mail: hshin@khu.ac.kr). S. N. Paing and J. W. Setiawan contributed equally to this paper.

T. Q. Duong is with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast BT7 1NN, UK (e-mail: trung.q.duong@qub.ac.uk).

O. A. Dobre is with Department of Electrical and Computer Engineering, Memorial University, 240 Prince Philip Dr., St. John's, NL A1B 3X5 Canada (e-mail: odobre@mun.ca).

or signal interference can introduce errors or disruptions in the communication channel within the Metaverse, reducing the efficiency of the communication and affecting the quality of the user experience and seamless interaction [14].

Recently, the unprecedented growth of quantum computing poses a serious threat to the classical blockchain and consequently, to the human-centric Metaverse [15]. Quantum cryptography, such as Shor's algorithm and Grover Search algorithm, can easily break some of the current security mechanisms used in classical blockchain technology [16]. To address these threats, blockchain must be equipped with post-quantum cryptography or transformed into a quantum blockchain [17]–[19]. Post-quantum cryptography uses mathematical algorithms that are believed to be secure even against quantum computing attacks. In the long run, a quantum blockchain is considered to be a secure solution for the next phase of the human-centric Metaverse.

In the Metaverse, the blockchain utilizes a consensus algorithm to maintain the consistency of its distributed ledger. However, node failure within the blockchain can compromise the integrity of the human-centric Metaverse and have negative consequences for users in the system. One of the best consensus algorithms for this purpose is the Byzantine fault tolerance (BFT) algorithm, as it can achieve consensus while tolerating failures caused by malicious or faulty nodes. However, existing classical BFT algorithms have two main issues: the 1/3 fault tolerance bound and the security vulnerabilities caused by classical cryptographic methods. By utilizing state-of-the-art quantum mechanics such as superposition, entanglement, and the no-cloning principle, quantum BFT (Q-BFT) can overcome the aforementioned problems by offering superior fault tolerance than its classical counterparts, achieving up to $1/2$ fault tolerance bound and a quantum layer of security [20]–[23].

In Q-BFT, nodes in the system communicate using quantum states and achieve consensus through a distributed private correlated list.[1] The private correlated list contains secret information that allows nodes to detect errors introduced by faulty or malicious nodes. Several variants of Q-BFT algorithm have been proposed, including those based on Aharonov quantum state [20], high-dimensional entangled states [24], [25], and single qudit state [21]. Although Q-BFT offers advantages, there is a concern that the private correlated list can be vulnerable to adversarial attack. Implementing a human-centric Metaverse in a noisy quantum environment is also challenging due to limitations such as decoherence and complexity. To address these issues, in this article, we develop a new type of Q-BFT protocol using the counterfactual communication paradigm for the human-centric Metaverse.

Counterfactual quantum communication is a new mode of communication that enables the transmission of information without the passage of any information-carrying particle through the channel [26], [27]. This concept arises from the convergence of two phenomena: interaction-free measurement, which allows one to infer the presence of an object without interacting with it; and chained quantum Zeno effect, which freezes a quantum state through a chain of continuous observation [28]–[30]. It has been used to enhance communication security in various applications, including key distribution, duplex coding and teleportation [27], [31]–[35]. Recent research has demonstrated that conventional quantum communication is no longer secure under counterfactual quantum attacks [36]. Hence, it has the potential to revolutionize the field of quantum communication by enabling the secure transmission of quantum information.

In this paper, we propose a counterfactual Q-BFT (CQ-BFT) protocol for a K-partite network where each party generates a correlated private list of length L through the counterfactual list distribution procedure. The main contributions of this paper are as follows: i) each party (say, Bob$_i$) in the network encodes the basis choice b_i and secret value s_i by applying counterfactual unitary telecomputation $\boldsymbol{V}$ and $\boldsymbol{U}$ respectively to accomplish the list distribution, ii) CQ-BFT can achieve a consensus with a fault tolerance bound of $1/2$, and iii) CQ-BFT offers enhanced security and robustness against dephasing noise, which are the fundamental requirements of the human-centric Metaverse. It is shown that the CQ-BFT protocol is not only secure against adversarial attacks but also prevents information from being disclosed to faulty parties.

The remaining sections of the paper are organized as follows. Section II covers the privacy and security protection for the human-centric Metaverse. Section III briefly introduces BFT, reviews the qudit list distribution, and designs our counterfactual consensus protocol (CQ-BFT). Section IV addresses the security of CQ-BFT along with numerical examples. Section V analyzes noise robustness, scalability, and decentralization of the CQ-BFT protocol with the comparison of the known quantum consensus protocols. Finally, we provide a brief conclusion in Section VI.

II. Privacy and Security in the Metaverse

Metaverse concepts such as virtual assets, currency, and properties allow a massive amount of users to generate their own creative content and perform Metaverse activities exclusively. With emerging technologies and new concepts of virtual technologies, the Metaverse, which is comprised of multiple smaller subsystems, becomes vulnerable to various kinds of attacks as new virtual concepts open up to unseen security and privacy issues [37]. To ensure the continuity of Metaverse, it is crucial to tackle potential security and privacy issues.

Within the Metaverse, each user is represented by a virtual avatar and interacts with others. To access the virtual world, users employ various Metaverse gadgets, including AR/VR headsets, haptic glasses, wrist-based bands, and IoT sensors. Since these gadgets serve as a gateway to the Metaverse, an eavesdropper can get control of these physical Metaverse gadgets through cyber means, imposing cyber-physical threats by manipulating other users. Moreover, recent advancements in artificial intelligence (AI) have made it challenging to distinguish between a human and a bot. The eavesdropper can steal someone's identity and create a deep fake using AI. This opens new security problems such as virtual property theft, ownership disputes, and fraudulent transactions, as the

[1] To distribute a private correlated list, each node in the network shares correlated data in the form of lists. The list held by each node is known only to itself and enables to detect the presence of malicious users in the network.

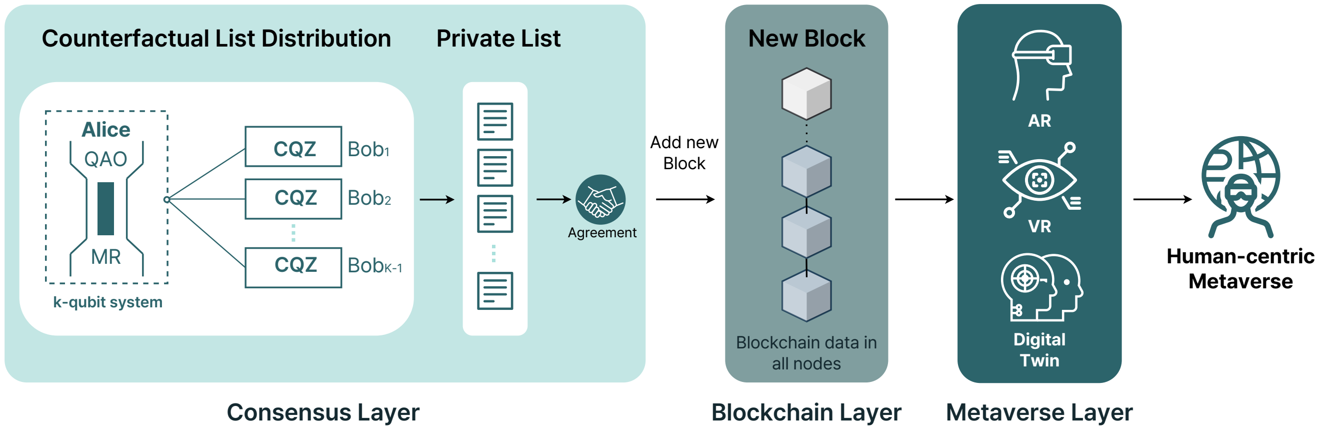


Fig. 1. A counterfactual list distribution for the consensus layer to reach an agreement among Metaverse users where QAO stands for a quantum absorptive object, MR for a mirror, and CQZ for the chained quantum Zeno effect. This counterfactual consensus provides quantum-safe security and privacy for the distributed ledger system. The consensus layer is responsible for validating and agreeing on transactions before adding them to the blockchain layer to provide a decentralized and tamper-resistant ledger for the Metaverse layer where users can trade digital assets and interact with others in the virtual environment.

Metaverse allows users to own and trade virtual objects such as virtual real estate and currency. In addition, Metaverse data may include sensitive private information as well as essential personal information of users. As an open platform with multiple third parties or stakeholders involved, the Metaverse also opens up vulnerabilities for personal data misuse or abuse.

The aforementioned security and privacy issues in the Metaverse can be solved using blockchain technology. Data structures in blockchains make it difficult for unauthorized parties to tamper with information, providing protection against cyber-physical attacks and identity management problems. The blockchain also keeps track of all transactions and ownership, offering more security protection against virtual property theft in the Metaverse. For privacy issues, blockchain's decentralized infrastructure can be used to store sensitive data along with cryptography tools to encrypt the data. This decentralization enables the Metaverse platform to protect user privacy, provide transparency to the data, and prevent any data misuse compared to centralized data storage.

Despite the potential benefits of blockchain technology in enhancing security and privacy, it is not a panacea for all related challenges [38]–[40]. Eavesdroppers and hackers are continually devising tactics to steal private information. For instance, external attackers can exploit vulnerabilities to gain unauthorized access, while malicious users with necessary privileges can introduce malicious consensus nodes or remove legitimate nodes to increase adversarial consensus power [40]. In addition, the evergrowing research and development of quantum computers impose a threat to the classical blockchain as classical cryptographic systems rely on the complexity of computational problems, and quantum computers can compromise their security. Due to the recent advancements in quantum computing, a transition from classical to quantum-based blockchain is needed.

At the core of quantum consensus for blockchains, the quantum network infrastructure must be designed to support its deployment in the blockchain infrastructure. However, challenges remain when integrating quantum consensus into blockchains. The most important challenge is to ensure the security and privacy of secret information. Recently, it has been shown that traditional quantum cryptography algorithms are susceptible to counterfactual attacks, which can break the security of these algorithms [36]. Another important challenge is the scalability of the quantum networks. As the size of the networks increases, it increases the complexity of entanglement distribution and the sensitivity of the quantum channel between remote parties. As shown in Fig. 1, the proposed CQ-BFT protocol enhance the security and privacy of the Metaverse, even in the presence of counterfactual quantum attacks [36], while accomplishing consensus without transmitting any particles carrying information through the quantum channel.

III. CQ-BFT Consensus

In this section, we develop a counterfactual protocol to securely distribute secret lists in a K-partite quantum network for BFT without transmitting any physical particle over the quantum channel.

A. *Byzantine Fault Tolerance*

For a distributed network, BFT is a method of achieving coordinated behavior among parties even in the presence of faulty or dishonest nodes [41]. The coordinated behavior is required for various tasks such as clock synchronization, secret sharing, or liar detection in a network [21], [42]. In general, the fault constitutes a crash, omission, or Byzantine attack at one or more network nodes. While the first two fault categories constitute the omission of all or a subset of messages, the Byzantine attack involves misleading information from the disloyal party to sabotage the coordination. The network has pairwise authenticated classical communication among the nodes. The network leader decides a message value $x \in \mathcal{X}$ from some finite domain $\mathcal{X}$. The leader then communicates its choice to each party with the help of pairwise communication channels. Then, the remaining nodes communicate

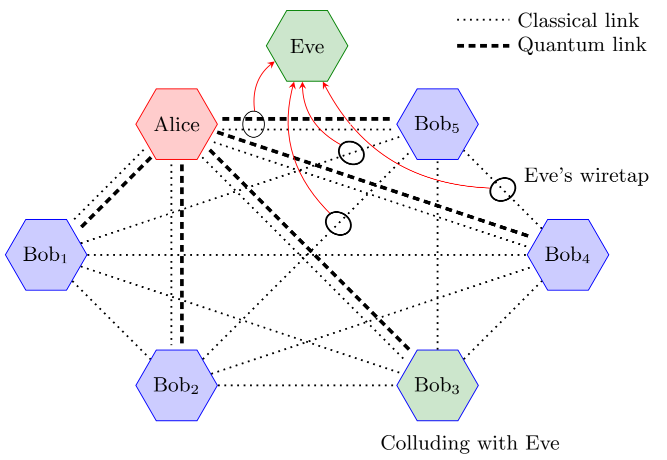


Fig. 2. A K-partite network for counterfactual secure BFT ($K = 6$). Alice shares a quantum channel with each of Bobs for the private list distribution. Pairwise classical channels exist between all the nodes in the network for BFT. An eavesdropper (Eve), either acting independently or in the direction of the malicious nodes (e.g., Bob$_3$), aims to sabotage the list distribution procedure.

to verify the message content mutually. The network is said to have achieved BFT if all legitimate nodes have verified and acknowledged the shared message x. Detectable BFT is a relaxed version of BFT, which introduces the possibility of aborting the protocol in the absence of a consensus. The BFT has been used in consensus protocols for blockchains [43]. For this purpose, one of the nodes acts as the central node (or sender) for each run of the BFT in a decentralized network.

The BFT consensus requires each party to have a private list suitably correlated with other parties in the network [44], [45]. Therefore, the generation and distribution of private lists among network nodes are essential for achieving BFT [25]. A quantum protocol enables this list distribution to be unconditionally secure. Quantum solutions for the detectable BFT have been obtained by using entangled Aharonov states, singlet states, GHZ-like states, and quantum key distribution [20], [25]. More recently, it has been shown that the qudit-based solutions are more scalable than their entanglement-assisted counterparts [21], [42].

B. Qudit List Distribution

Before designing a counterfactual list distribution for the CQ-BFT protocol, we first briefly review the scalable quantum list distribution in [21]. The network consists of K nodes, as shown in Fig. 2. The party (e.g., Alice), which wants to broadcast her message to the $K-1$ participating nodes (Bobs), becomes the central node. We denote the ith participating node as Bob$_i$. In the protocol, Alice prepares a K-dimensional qudit

$$|\eta\rangle = \frac{1}{\sqrt{K}} \sum_{j=0}^{K-1} |j\rangle \,, \tag{1}$$

where $|j\rangle$ is the jth standard (computational) basis element. Let

$$\boldsymbol{V} = |0\rangle\langle 0| + \omega \sum_{k=1}^{K-1} |k\rangle\langle k| \tag{2}$$

$$\boldsymbol{U} = \sum_{\ell=0}^{K-1} \omega^{\ell} \, |\ell\rangle\langle \ell| \tag{3}$$

be unitary operations for basis and secret encoding where $\omega = e^{\jmath 2\pi/K}$ and $\jmath = \sqrt{-1}$. Alice applies the unitary operation $\boldsymbol{V}^{b_0}$ on the prepared qudit to encode her basis choice followed by $\boldsymbol{U}^{s_0}$ to encode her secret entry where $b_0 \in \mathbb{Q}_K = \{0, 1, \ldots, K-1\}$ is her choice of basis encoding and $s_0 \in \mathbb{Q}_K$ is her secret value for her private list.

Now, Alice sends her qudit to Bob$_1$ and he applies $\boldsymbol{U}^{s_1}\boldsymbol{V}^{b_1}$ on the received qudit where $b_1 \in \mathbb{Q}_K$ and $s_1 \in \mathbb{Q}_2$ are his basis and secret list choices, respectively. Bob$_1$ forwards the qudit to Bob$_2$ and the procedure is continued until the qudit reaches Bob$_{K-1}$. Finally, Bob$_{K-1}$ applies $\boldsymbol{U}^{s_{K-1}}\boldsymbol{V}^{b_{K-1}}$ according to his choice and performs a projective measurement with the projectors $\{|\eta\rangle\langle\eta|\, , \boldsymbol{I}_K - |\eta\rangle\langle\eta|\}$ where $\boldsymbol{I}_K$ denotes the K-dimensional identity operator. If the measurement outcome corresponds to $|\eta\rangle\langle\eta|$, all Bobs reveal their basis choices $b_1, b_2, \ldots, b_{K-1}$ in the reverse order of qudit transmissions. The list distribution of $s_0, s_1, \ldots, s_{K-1}$ is valid if

$$\sum_{i=0}^{K-1} b_i \mod K = 0. \tag{4}$$

The parties repeat this list distribution procedure to generate correlated private lists of length L. Let $\mathcal{L}_0$ be the list held by Alice and $\mathcal{L}_i$ be the lists held by Bob$_i$ for $i = 1, 2, \cdots, K-1$. Then, using the successful list distribution, the K parties achieve BFT with the help of pairwise classical communication as follows.

1) Alice sends $\boldsymbol{z}_{0,i} = (\mu_{0,i}, \mathcal{Y}_{0,i})$ to each Bob$_i$ where $\mu_{0,i} \in \mathbb{Q}_2$ is a message and $\mathcal{Y}_{0,i}$ is the list of indices of all the entries in $\mathcal{L}_0$ that contain the message $\mu_{0,i}$.
2) Bob$_i$ verifies if $\boldsymbol{z}_{0,i}$ corresponds to the entries in his own list and performs either of the following tasks.
   - If they match, i.e., $\boldsymbol{z}_{0,i} \equiv \mathcal{L}_i$, he sends $\boldsymbol{z}_{i,j}$ to each of the other Bob$_j$, $j \neq i$.[2]
   - If $\mathcal{Y}_{0,i}$ is inconsistent with the corresponding entries in $\mathcal{L}_i$, i.e., $\boldsymbol{z}_{0,i} \not\equiv \mathcal{L}_i$, Bob$_i$ sends the symbol $\perp$ to other parties without any accompanying sublist, meaning he has received the inconsistent data.
   - In case of any other transmission from Bob$_i$, other legitimate participants identify it as faulty through BFT.
3) A legitimate Bob$_i$ decides on $\mu_{0,i}$ as his final decision unless messages from other Bobs persuade him to decide that Alice is faulty [21].

[2] The equivalence $\equiv$ stands for consistency, i.e., $\boldsymbol{z}_{0,i} \equiv \mathcal{L}_i$ denotes that indices $\mathcal{Y}_{0,i}$ for the message $\mu_{0,i}$ is consistent with the corresponding entries in $\mathcal{L}_i$.

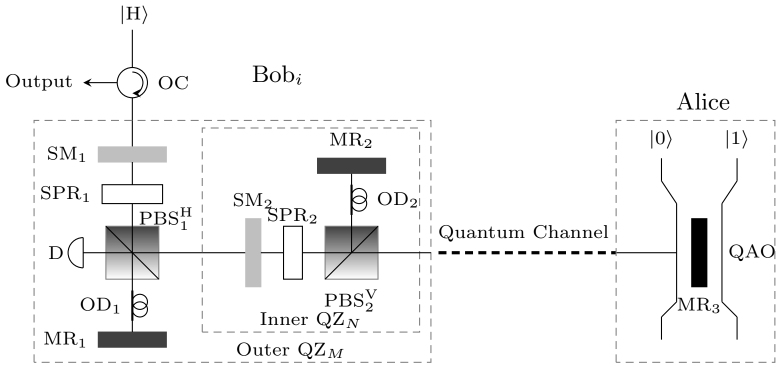


Fig. 3. A H-CQZ$_{M,N}$ gate where SM stands for a switchable mirror, SPR for a switchable polarization rotator, PBS for a polarizing beam splitter, OD for an optical delay, OC for an optical circulator, D for a detector, and H (V) for the horizontal (vertical) photon polarization. It is composed of two quantum Zeno (QZ) gates (see [34, Fig. 1], [35, Fig. 4])—inner QZ$_N$ gate with N cycles and outer QZ$_M$ gate with M cycles. The two optical paths SM$_{1(2)}$ → MR$_{1(2)}$ and SM$_{1(2)}$ → MR$_3$ correspond to the outer (inner) cycle of the H-CQZ$_{M,N}$ gate (see [34, Fig. 2], [35, Fig. 5]). When Bob$_i$ inputs his horizontal polarized photon$|\mathrm{H}\rangle$ into the H-CQZ$_{M,N}$ gate, the photon $|\mathrm{H}\rangle$ evolves through the gate, depending on the state of QAO at Alice, where $|0\rangle$ and $|1\rangle$ represent the absence and presence states of QAO, respectively. Unless the photon is absorbed, the H-CQZ$_{M,N}$ gate changes the polarization of the input photon in the presence state $|1\rangle$ of QAO and otherwise, keeps its polarization in a counterfactual manner for both cases (see [34, Table. I], [35, Fig. 5]) for the detailed operation of the CQZ gate).

C. Counterfactual List Distribution

We now devise a quantum protocol to securely distribute secret lists for CQ-BFT consensus using counterfactual quantum communication. We consider the same roles as in the qudit list distribution, where Alice acts as the central node and $K-1$ Bobs act as participating nodes. For simplicity, we assume $K=2^k$ for some positive integer k. In contrast to the qudit-based BFT, the proposed protocol allows Alice to utilize a k-qubit system for scalability. Alice starts the protocol by preparing a k-qubit initial state

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{K}}\sum_{x_1=0}^{1}\sum_{x_2=0}^{1}\cdots\sum_{x_k=0}^{1}|x_1x_2\cdots x_k\rangle \\ &= \frac{1}{\sqrt{K}}\sum_{\boldsymbol{x}\in\mathbb{Q}_2^k}|\boldsymbol{x}\rangle \end{aligned} \tag{5}$$

on k quantum absorptive objects (QAOs) for counterfactual communication with chained quantum Zeno (CQZ) gates (see Fig. 3). Alice then locally applies $\boldsymbol{A}=\boldsymbol{U}^{s_0}\boldsymbol{V}^{b_0}$ on $|\psi\rangle$.

Next, Bob$_i$ applies $\boldsymbol{B}_i=\boldsymbol{U}^{s_i}\boldsymbol{V}^{b_i}$ for $i=1,2,\cdots,K-1$. Bobs utilize H-CQZ$_{M,N}$ gates in Fig. 3 to ensure the counterfactuality of the list distribution protocol where H (V) stands for the horizontal (vertical) polarization of a photon. Alice and Bob$_i$ take the following steps to counterfactually apply—i.e., *telecompute*—$\boldsymbol{V}^{b_i}$ on the k-qubit system of Alice.

1) Bob$_i$ starts by throwing his horizontal polarized photon $|\mathrm{H}\rangle$ towards the counterfactual unitary telecomputation (CUT) for $\boldsymbol{V}^{b_i}$ as illustrated in Fig. 4(a). The composite state of Alice and Bob$_i$ at this input is given by

$$|\eta_{i,0}\rangle = |\psi_{i-1}\rangle\,|\mathrm{H}\rangle \tag{6}$$

where $|\psi_{i-1}\rangle$ is the state of Alice's QAOs after the list distribution of Bob$_{i-1}$, i.e.,

$$|\psi_{i-1}\rangle = \boldsymbol{B}_{i-1}\,|\psi_{i-2}\rangle \tag{7}$$

and $|\psi_0\rangle=\boldsymbol{A}\,|\psi\rangle$.

2) Alice and Bob$_i$ apply the H-CQZ$_{M,N}$ gate for the $(k+1)$-qubit controlled unitary operation

$$\boldsymbol{Q} = |\boldsymbol{0}\rangle\langle\boldsymbol{0}|\otimes\boldsymbol{I}_2+\sum_{\substack{\boldsymbol{x}\in\mathbb{Q}_2^k\\ \boldsymbol{x}\neq\boldsymbol{0}}}|\boldsymbol{x}\rangle\langle\boldsymbol{x}|\otimes\boldsymbol{X}\boldsymbol{Z} \tag{8}$$

on the composite state $|\eta_{i,0}\rangle$ where $\boldsymbol{X}$ and $\boldsymbol{Z}$ denote the Pauli-X and Pauli-Z operators, respectively. For the counterfactual controlled unitary $\boldsymbol{Q}$, QAOs act as the control qubits and the photon is the target qubit. Unless the photon is absorbed, it transforms the composite state $|\eta_{i,0}\rangle$ to the entangled state

$$|\eta_{i,1}\rangle = \frac{1}{\sqrt{K}}\Big(|\boldsymbol{0}\rangle\,|\mathrm{H}\rangle+\sum_{\substack{\boldsymbol{x}\in\mathbb{Q}_2^k\\ \boldsymbol{x}\neq\boldsymbol{0}}}\alpha_i\left(\boldsymbol{x}\right)|\boldsymbol{x}\rangle\,|\mathrm{V}\rangle\Big) \tag{9}$$

with probability [34], [35]

$$\begin{aligned}\lambda_K &= \left(1-\frac{1}{K}\sin^2\theta_M\right)^M \\ &\prod_{m=1}^{M}\left[1-\frac{K-1}{K}\sin^2\left(m\theta_M\right)\sin^2\theta_N\right]^N,\end{aligned} \tag{10}$$

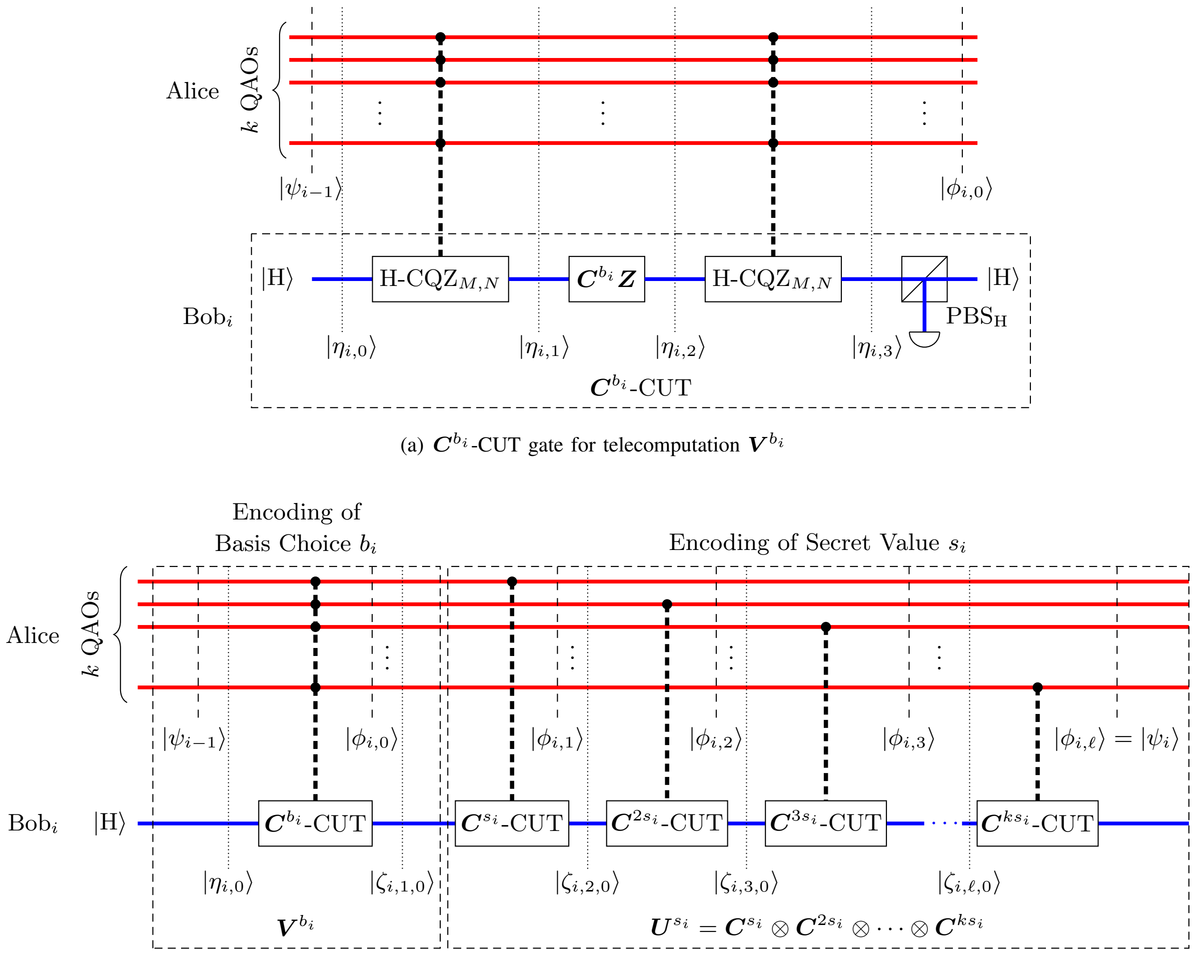
where $\theta_M=\pi/\left(2M\right)$, $\alpha_i\left(\boldsymbol{x}\right)=\omega^{ds_{i-1}+b_{i-1}}\alpha_{i-1}\left(\boldsymbol{x}\right)$, $\alpha_0\left(\boldsymbol{x}\right)=1$, d is the decimal representation of the binary vector $\boldsymbol{x}$, and $|\mathrm{V}\rangle$ is the vertical polarized photon.

3) Bob$_i$ now locally applies a single-qubit unitary operation $\boldsymbol{C}^{b_i}\boldsymbol{Z}$ on his photon where

$$\boldsymbol{C}=\begin{bmatrix}1 & 0\\ 0 & \omega\end{bmatrix}. \tag{11}$$

It transforms the composite state $|\eta_{i,1}\rangle$ to

$$|\eta_{i,2}\rangle = \frac{1}{\sqrt{K}}\Big(|\boldsymbol{0}\rangle\,|\mathrm{H}\rangle-\sum_{\substack{\boldsymbol{x}\in\mathbb{Q}_2^k\\ \boldsymbol{x}\neq\boldsymbol{0}}}\omega^{b_i}\alpha_i\left(\boldsymbol{x}\right)|\boldsymbol{x}\rangle\,|\mathrm{V}\rangle\Big). \tag{12}$$



(a) $\boldsymbol{C}^{b_i}$-CUT gate for telecomputation $\boldsymbol{V}^{b_i}$

(b) Complete CUT operations for telecomputation $\boldsymbol{B}_i = \boldsymbol{U}^{s_i}\boldsymbol{V}^{b_i}$

Fig. 4. Counterfactual encoding of basis choice b_i and secret value s_i for Bob$_i$, $i = 1, 2, \ldots K-1$: (a) the $\boldsymbol{C}^{b_i}$-CUT gate for telecomputation $\boldsymbol{V}^{b_i}$ (counterfactual encoding of basis choice b_i) and (b) the complete CUT operations for telecomputation $\boldsymbol{B}_i = \boldsymbol{U}^{s_i}\boldsymbol{V}^{b_i}$. The $\boldsymbol{C}^{b_i}$-CUT gate has three sequential operations: the first H-CQZ$_{M,N}$ operation, a local single-qubit unitary operation $\boldsymbol{C}^{b_i}$, and the second H-CQZ$_{M,N}$ operation. Here, Alice holds k QAOs in the state $|\psi_{i-1}\rangle$ and Bob$_i$ inputs his horizontal polarized photon $|\mathrm{H}\rangle$ into the CUT gate. The first H-CQZ$_{M,N}$ gate entangles Alice and Bob$_i$. Then, Bob$_i$ encodes his basis choice b_i using the local operation $\boldsymbol{C}^{b_i}$. Finally, the second H-CQZ$_{M,N}$ gate disentangles Alice and Bob$_i$. In this way, Bob$_i$ encodes his basis choice b_i counterfactually by telecomputing $\boldsymbol{V}^{b_i}$ on Alice's QAOs. Next, to counterfactually encode his secret value s_i, Bob$_i$ telecomputes the k-qubit separable unitary $\boldsymbol{U}^{s_i} = \boldsymbol{C}^{s_i} \otimes \boldsymbol{C}^{2s_i} \otimes \cdots \otimes \boldsymbol{C}^{ks_i}$ on Alice's QAOs in the state $|\phi_{i,0}\rangle$ by successively using k $\boldsymbol{C}^{\ell s_i}$-CUT gates, $\ell = 1, 2, \ldots, k$, where each $\boldsymbol{C}^{\ell s_i}$-CUT gate telecomputes the single-qubit unitary $\boldsymbol{C}^{\ell s_i}$ on the ℓth QAO of Alice and transforms the QAOs in the state $|\phi_{i,\ell}\rangle$. Unless the photon is absorbed, the complete CUT operations of Bob$_i$ telecompute the unitary $\boldsymbol{B}_i$ on the k-qubit QAO system of Alice to counterfactually encode his basis choice b_i and secret value s_i, which transform the state of Alice's QAOs to $|\phi_{i,k}\rangle = \boldsymbol{B}_i |\psi_{i-1}\rangle = |\psi_i\rangle$.

4) Finally, Alice and Bob$_i$ apply the controlled unitary $\boldsymbol{Q}$ again by using the H-CQZ$_{M,N}$ gate to complete the basis encoding telecomputation $\boldsymbol{V}^{b_i}$ on Alice's QAOs. Unless the photon is absorbed, it transforms the composite state $|\eta_{i,2}\rangle$ to the disentangled state

$$\begin{aligned} |\eta_{i,3}\rangle &= \left(\boldsymbol{V}^{b_i} \otimes \boldsymbol{I}_2\right) |\eta_{i,0}\rangle \\ &= |\phi_{i,0}\rangle\, |\mathrm{H}\rangle \end{aligned} \tag{13}$$

with probability λ_K, where

$$|\phi_{i,0}\rangle = \boldsymbol{V}^{b_i} |\psi_{i-1}\rangle \tag{14}$$

is the state of Alice's QAOs after encoding the basis choice b_i of Bob$_i$ (see Algorithm 1).

Note that the k-qubit system (Alice's QAOs) $|\phi_{i,0}\rangle$ in (14) can be written as

$$|\phi_{i,0}\rangle = \frac{1}{\sqrt{K}} \sum_{\boldsymbol{x} \in \mathbb{Q}_2^k} \beta_i(\boldsymbol{x})\, |\boldsymbol{x}\rangle \tag{15}$$

where

$$\beta_i(\boldsymbol{x}) = \begin{cases} 1, & \text{if } \boldsymbol{x} = \boldsymbol{0}, \\ \omega^{b_i}\alpha_i(\boldsymbol{x}), & \text{otherwise.} \end{cases} \tag{16}$$

The secret encoding unitary $\boldsymbol{U}^{s_i}$ can be decomposed into k single-qubit unitary operators $\boldsymbol{C}^{\ell s_i}$, with each being counterfactually applied on the ℓth QAO (qubit) of Alice, $\ell = 1, 2, \ldots, k$, as follows:

$$\boldsymbol{U}^{s_i} = \bigotimes_{\ell=1}^{k} \boldsymbol{C}^{\ell s_i}. \tag{17}$$

Algorithm 1: Telecomputation $\boldsymbol{V}^{b_i}$ of Bob$_i$ on Alice's QAOs in the state $|\psi_{i-1}\rangle$.

```
Input:  k QAOs in the state $|\psi_{i-1}\rangle$ at Alice,
        Photon in the state $|\mathrm{H}\rangle$ at Bob$_i$,
        Basis choice $b_i \in \mathbb{Q}_K$ of Bob$_i$
Output: k QAOs in the state $|\phi_{i,0}\rangle = \boldsymbol{V}^{b_i} |\psi_{i-1}\rangle$
$|\eta_{i,0}\rangle \leftarrow |\psi_{i-1}\rangle |\mathrm{H}\rangle$,
$|\eta_{i,1}\rangle \leftarrow \boldsymbol{Q} |\eta_{i,0}\rangle$,
$|\eta_{i,2}\rangle \leftarrow \left(\boldsymbol{I}_K \otimes \boldsymbol{C}^{b_i} \boldsymbol{Z}\right) |\eta_{i,1}\rangle$,
$|\eta_{i,3}\rangle \leftarrow \boldsymbol{Q} |\eta_{i,2}\rangle$,
$|\phi_{i,0}\rangle |\mathrm{H}\rangle \leftarrow |\eta_{i,3}\rangle$,
return $|\phi_{i,0}\rangle$
```

To telecompute $\boldsymbol{U}^{s_i}$ on the state $|\phi_{i,0}\rangle$ of Alice's QAOs for encoding the secret value s_i, Alice and Bob$_i$ take the following steps.

1) Bob$_i$ throws his horizontal polarized photon $|\mathrm{H}\rangle$ (output of the first CUT gate for $\boldsymbol{V}^{b_i}$) towards k CUT gates successively for $\boldsymbol{U}^{s_i}$ as illustrated in Fig. 4(b). The ℓth CUT gate telecomputes (i.e., counterfactually applies) $\boldsymbol{C}^{\ell s_i}$ on the ℓth QAO of Alice to encode the secret value s_i of Bob$_i$. The composite state of Alice and Bob$_i$ at the ℓth CUT input is given by

$$|\zeta_{i,\ell,0}\rangle = |\phi_{i,\ell-1}\rangle |\mathrm{H}\rangle \tag{18}$$

where $|\phi_{i,\ell-1}\rangle$ is the state of Alice's QAOs at the output of the $(\ell-1)$th CUT gate for the secret-value encoding (telecomputation) $\boldsymbol{C}^{(\ell-1)s_i}$ of Bob$_i$, i.e.,

$$|\phi_{i,\ell-1}\rangle = \left(\boldsymbol{I}_{2^{\ell-2}} \otimes \boldsymbol{C}^{(\ell-1)s_i} \otimes \boldsymbol{I}_{2^{k-\ell+1}}\right) |\phi_{i,\ell-2}\rangle . \tag{19}$$

2) Alice and Bob$_i$ apply the H-CQZ$_{M,N}$ gate for the 2-qubit controlled unitary operation

$$\boldsymbol{R}_\ell = \sum_{\boldsymbol{x} \in \mathbb{Q}_2^k} |\boldsymbol{x}\rangle\langle\boldsymbol{x}| \otimes (\boldsymbol{X}\boldsymbol{Z})^{x_\ell} \tag{20}$$

on the composite state $|\zeta_{i,\ell,0}\rangle$. For the counterfactual controlled unitary $\boldsymbol{R}_\ell$, the ℓth QAO of Alice acts as the control qubit, and the photon of Bob$_i$ is the target qubit. Unless the photon is discarded in the H-CQZ$_{M,N}$ gate, it transforms the composite state $|\zeta_{i,\ell,0}\rangle$ to

$$\begin{aligned} |\zeta_{i,\ell,1}\rangle = \frac{1}{\sqrt{K}} & \sum_{\substack{\boldsymbol{x} \setminus x_\ell \in \mathbb{Q}_2^{k-1} \\ x_\ell = 0}} \beta_{i,\ell}(\boldsymbol{x}) |\boldsymbol{x}\rangle |\mathrm{H}\rangle \\ & + \frac{1}{\sqrt{K}} \sum_{\substack{\boldsymbol{x} \setminus x_\ell \in \mathbb{Q}_2^{k-1} \\ x_\ell = 1}} \beta_{i,\ell}(\boldsymbol{x}) |\boldsymbol{x}\rangle |\mathrm{V}\rangle \end{aligned} \tag{21}$$

with probability λ_2, where $\beta_{i,\ell}(\boldsymbol{x}) = \omega^{(\ell-1)s_i} \beta_{i,\ell-1}(\boldsymbol{x})$ and $\beta_{i,0}(\boldsymbol{x}) = \beta_i(\boldsymbol{x})$ in (16).

Algorithm 2: Telecomputation $\boldsymbol{U}^{s_i}$ of Bob$_i$ on Alice's QAOs in the state $|\phi_{i,0}\rangle$.

```
Input:  k QAOs in the state $|\phi_{i,0}\rangle$ at Alice,
        Photon in the state $|\mathrm{H}\rangle$ at Bob$_i$,
        Secret value $s_i \in \mathbb{Q}_2$ of Bob$_i$
Output: k QAOs in the state
        $|\psi_i\rangle = \boldsymbol{U}^{s_i} |\phi_{i,0}\rangle = \left(\bigotimes_{\ell=1}^{k} \boldsymbol{C}^{\ell s_i}\right) |\phi_{i,0}\rangle$
for $\ell \in 1 \to k$ do
    $|\zeta_{i,\ell,0}\rangle \leftarrow |\phi_{i,\ell-1}\rangle |\mathrm{H}\rangle$,
    $|\zeta_{i,\ell,1}\rangle \leftarrow \boldsymbol{R}_\ell |\zeta_{i,\ell,0}\rangle$,
    $|\zeta_{i,\ell,2}\rangle \leftarrow \left(\boldsymbol{I}_K \otimes \boldsymbol{C}^{\ell s_i} \boldsymbol{Z}\right) |\zeta_{i,\ell,1}\rangle$,
    $|\zeta_{i,\ell,3}\rangle \leftarrow \boldsymbol{R}_\ell |\zeta_{i,\ell,2}\rangle$,
    $|\phi_{i,\ell}\rangle |\mathrm{H}\rangle \leftarrow |\zeta_{i,\ell,3}\rangle$,
return $|\psi_i\rangle = |\phi_{i,k}\rangle$
```

3) Bob$_i$ now locally applies a single-qubit unitary operation $\boldsymbol{C}^{\ell s_i}\boldsymbol{Z}$ on his photon, which transforms $|\zeta_{i,\ell,1}\rangle$ to

$$\begin{aligned} |\zeta_{i,\ell,2}\rangle = \frac{1}{\sqrt{K}} & \sum_{\substack{\boldsymbol{x} \setminus x_\ell \in \mathbb{Q}_2^{k-1} \\ x_\ell = 0}} \beta_{i,\ell}(\boldsymbol{x}) |\boldsymbol{x}\rangle |\mathrm{H}\rangle \\ & - \frac{1}{\sqrt{K}} \sum_{\substack{\boldsymbol{x} \setminus x_\ell \in \mathbb{Q}_2^{k-1} \\ x_\ell = 1}} \omega^{\ell s_i} \beta_{i,\ell}(\boldsymbol{x}) |\boldsymbol{x}\rangle |\mathrm{V}\rangle . \end{aligned} \tag{22}$$

4) Finally, Alice and Bob$_i$ apply the controlled unitary $\boldsymbol{R}_\ell$ again by using the H-CQZ$_{M,N}$ gate to disentangle the photon from the QAOs. Unless the photon is absorbed, it transforms the composite state $|\zeta_{i,\ell,2}\rangle$ to

$$\begin{aligned} |\zeta_{i,\ell,3}\rangle &= \left(\boldsymbol{I}_{2^{\ell-1}} \otimes \boldsymbol{C}^{\ell s_i} \otimes \boldsymbol{I}_{2^{k-\ell}} \otimes \boldsymbol{I}_2\right) |\zeta_{i,\ell,0}\rangle \\ &= |\phi_{i,\ell}\rangle |\mathrm{H}\rangle \end{aligned} \tag{23}$$

with probability λ_2.

5) Alice and Bob$_i$ repeat Step 1)–4) for $\ell = 1, 2, \cdots, k$ to complete the secret encoding telecomputation $\boldsymbol{U}^{s_i}$ on Alice's QAOs. Note that

$$\begin{aligned} |\phi_{i,k}\rangle &= \left(\bigotimes_{\ell=1}^{k} \boldsymbol{C}^{\ell s_i}\right) |\phi_{i,0}\rangle \\ &= \boldsymbol{B}_i |\psi_{i-1}\rangle \\ &= |\psi_i\rangle \end{aligned} \tag{24}$$

is the state of Alice's QAOs after the list distribution of Bob$_i$ (see Algorithm 2).

Once all Bobs complete their telecomputations for the counterfactual list distribution, Alice (central node) measures the state of her QAOs in the Fourier basis $\{|\psi\rangle, |\psi^\perp\rangle\}$ [42]. If the measurement result is $|\psi\rangle$, all nodes reveal their choices of basis $b_0, b_1, \ldots, b_{K-1}$. Then, if these basis choices satisfy the condition (4), the list distribution of values $s_0, s_1, \ldots, s_{K-1}$ is treated as valid. In contrast to the qudit-based BFT, these bases are revealed in random order. The counterfactual basis encoding and random revealing are to prevent any party (especially the central node) from cheating in a way that leads to an invalid list distribution being treated as valid. This list distribution procedure is repeated to generate private correlated lists of length L.

D. Byzantine Agreement

With the successful list distribution, the parties achieve BFT by exchanging classical messages as mentioned in Section III-B. Assuming the central node (Alice) is legitimate for the CQ-BFT setup, legitimate Bob$_i$ reaches agreement on the message $\mu_{0,i}$ and decides that Bob$_j$ is legitimate if $\boldsymbol{z}_{j,i} \equiv \mathcal{L}_i$, $j \in \mathbb{Q}_K \setminus \{0, i\}$. Note that the CQ-BFT protocol does not require any shared phase reference between the network nodes due to its counterfactual operations [46], [47]. Hence, the CQ-BFT removes the requirement of *a priori* quantum handshake among the network nodes to share a phase reference. However, as a tradeoff, there is a nonzero probability, known as the *abortion rate*, that the photon is traveled over the quantum channel and the protocol is discarded to ensure the counterfactuality [34], [35]. This abortion rate goes to zero as the cycle numbers M and N of the CQZ gate tend to infinity. Fig. 5 shows the abortion rate

$$q\left(\boldsymbol{B}_i\right) = 1 - \lambda_K^2 \lambda_2^{2\log_2 K} \tag{25}$$

for telecomputation $\boldsymbol{B}_i$ to encode the basis choice b_i and secret value s_i of Bob$_i$ as a function of M and N when $K = 4$.

The CQ-BFT first distributes a private correlated list among communicating nodes to achieve a detectable broadcast. The upper bound on the number of dishonest nodes in the network for the fault tolerance is half the total number of nodes K in the network [22]. Here, fault tolerance indicates the minimum number of honest nodes to achieve Byzantine agreement. The probabilistic bounds for the failure of the protocol approach to zero as the length of the private list increases [22].

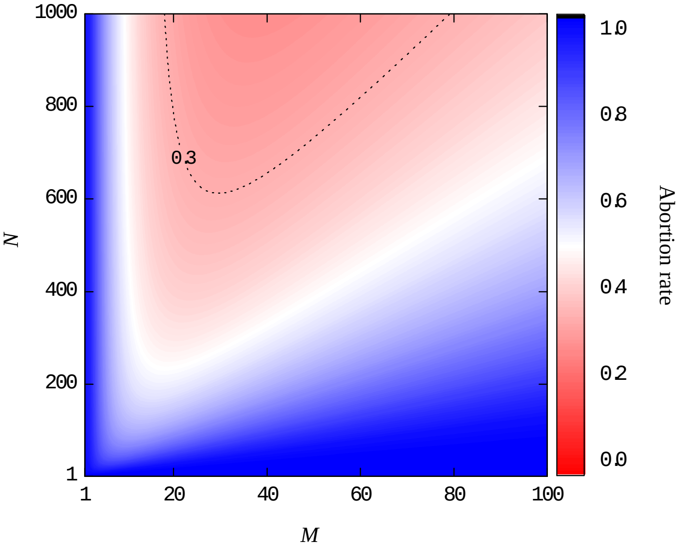


Fig. 5. Abortion rate $q\left(\boldsymbol{B}_i\right)$ as a function of M and N for telecomputation $\boldsymbol{B}_i$ of Bob$_i$ when $K = 4$.

IV. Security of CQ-BFT

Security is an important aspect in human-centric Metaverse to build trust among users, protect user data from unauthorized access, and resolve identity management issues. It is important to realize that any security vulnerabilities can have serious implications for Metaverse users and other stakeholders, such as cybercrime, discrimination, and legal issues. To provide a secure and trustworthy environment for users to interact, it is essential to ensure physical layer security, as it is the most important factor in securing the network infrastructure of the Metaverse. Since the CQ-BFT is implemented at the physical layer of Metaverse network infrastructure, it is necessary to ensure that the protocol can effectively prevent physical attacks and disruptions to the network. In the presence of pairwise classical authenticated channels, the security of Byzantine agreement boils down to the security of the distributed lists [25]. The security of the distributed lists includes secrecy and correctness, as well as protection against denial-of-service attacks during the list distribution protocol. A malicious agent sabotages the list distribution with the aim to steal more information about the list being shared. This sabotage results in the distribution of incorrect list entries, which causes some form of denial-of-service attacks. In the following, we consider different possible attacks in the list distribution protocol and discuss the security of the CQ-BFT protocol against these attacks.

A. Intercept-and-Resend Attacks

In intercept-and-resend attacks, Eve intercepts the transmitted quantum state, measures the state on the basis based on prior knowledge, and retransmits the quantum state to the receiver depending on the measurement outcome. Similarly, in Metaverse, Eve can intercept the communication between the nodes and modifies the transaction data before resending it to the network. Alternatively, she can store the intercepted qubit in her quantum memory and send a new qubit to the receiver. Using these attacks, she can cause users to lose their assets in Metaverse, such as increasing the transaction fee or changing the destination address. In counterfactual quantum communication, no information-carrying particle is transmitted over the channel. In case any information-carrying particle is transmitted over the channel, the protocol round is discarded to keep the counterfactuality, which makes the CQ-BFT protocol secure against intercept-and-resend attacks. This counterfactual nature eliminates the possibility of intercepting any information-carrying qubit. In the CQ-BFT protocol, only the $|\mathrm{H}\rangle$ component of the photon enters the channel in each cycle under the probabilistic model, and the entropy over the channel becomes zero. Therefore, Eve's interception of $|\mathrm{H}\rangle$ does not give her any new information.

Alternatively, Eve can randomly block or reflect the photon wave function in the quantum channel to sabotage the list distribution. To counter this denial-of-service attack, Bob$_i$ uses the decoy photons to detect the presence of Eve in the channel. When Bob$_i$ sends the decoy photon, the list distribution procedure is paused until the round for the decoy photon is completed. The probability that Bob$_i$ uses a decoy photon is a function of M, N, and the success probability required to detect an eavesdropper in the channel. Note that if the photon

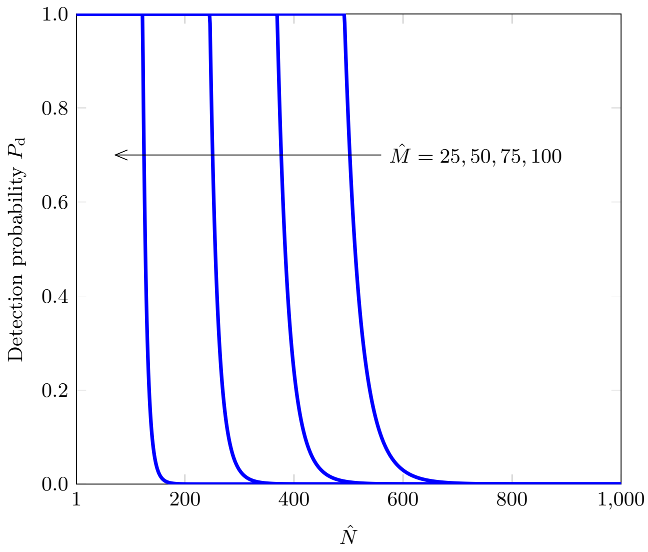


Fig. 6. Probability P_d that an eavesdropper (Eve) is detected for her unauthorized access as a function of $\hat{N}$ when $\hat{M} = 25, 50, 75, 100$. For each single H-CQZ$_{\hat{M},\hat{N}}$ operation, Eve must complete her attack within the access time window t_w of Alice. In addition, the time interval that she can guess b_i or s_i is between t_1 and t_2 where t_1 is the time after Bob$_i$ has performed his local operation $\boldsymbol{C}^{b_i}$ and t_2 is the time before Bob$_i$ completes his second H-CQZ$_{M,N}$ operation.

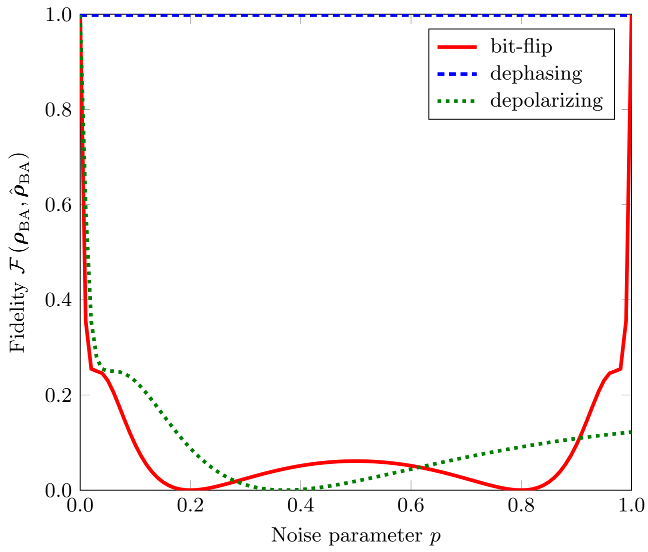


Fig. 7. Fidelity for the CQ-BFT protocol as a function of the noise parameter p of the polarization DoF (bit-flip, dephasing, and depolarizing) noise when $K = 4$, $M = 50$, and $N = 1000$.

is found in the channel and interacts with Alice's QAO, it is absorbed by the QAO and jumps to a higher energy level. In the absence of QAO, the photon is reflected to Bob and is discarded at the detector D$_1$ in the CQZ gate (see Fig. 3). For the $\boldsymbol{V}^{b_i}$ gate, the probability that at least one QAO is in the presence state is equal to $(K-1)/K$ whereas there is $1/2$ probability that the corresponding QAO is in the presence state to implement $\boldsymbol{C}^{\ell s_i}$. Therefore, for given values of M and N, the presence of Eve can be detected if the detection probability is different from Alice's detection probability. In this way, the CQ-BFT protocol can mitigate the security threat of intercept-and-resend attacks and compromise the security and integrity of the blockchain-based Metaverse.

B. Man-in-the-Middle Attacks

In the blockchain-empowered Metaverse, multiple nodes participate in the consensus mechanism to validate transactions and ensure the integrity of the blockchain. In man-in-the-middle attacks, a malicious actor (Eve) intercepts and manipulates the communication between the nodes and causes them to accept fraudulent transactions or reject valid transactions. Eve can introduce a man-in-the-middle attack in the CQ-BFT protocol by acting either as Alice or Bob$_i$ in the network.

1) Eve as Alice: Eve can impersonate Alice by using her QAOs. Similar to the intercept-and-resend attack, Bob uses decoy photons and particles to detect the presence of Eve in the channel.

2) Eve as Bob$_i$: Eve can impersonate Bob by applying $\boldsymbol{U}$ and $\boldsymbol{V}$ on her own auxiliary photons. If Eve uses a non-counterfactual setup, there is a high probability that her photon is absorbed by one of the QAOs possessed by Alice. Due to abnormal detection probability, Alice can detect the presence of an eavesdropper in the channel. In case Eve utilizes a counterfactual setup such as the H-CQZ gate to apply $\boldsymbol{U}$ and $\boldsymbol{V}$, the probabilistic model to find the photon in the channel enables to detect the presence of Eve. Consider that Alice uses near-perfect detectors with the detection range $\{f_\mathrm{min}, f_\mathrm{min}+\Delta f, f_\mathrm{min}+2\Delta f, \cdots, f_\mathrm{min}+(\delta-1)\Delta f\}$. In each round of communication, Bob randomly chooses a frequency within this range to prepare his photon in the initial state $|\mathrm{H}\rangle$. If the photon is absorbed by QAO, Bob$_i$ publicly announces the photon's frequency. The probability that the randomly chosen frequency of Bob's photon is different from the randomly chosen frequency of Eve's auxiliary photon is $1-1/\delta$, which enables Alice and Bob to detect the presence of Eve in the channel. Note that the random frequency introduces a frequency signature for Bob$_i$. This frequency signature for quantum information transfer (without quantum authenticated channels) makes the CQ-BFT protocol comparable with classical BFT schemes based on classical authenticated channels. Furthermore, in the existing schemes, a quantum bit error rate (QBER) is one of the widely used metrics to detect the presence of an eavesdropper in the quantum channel, which requires revealing a part of the distributed list. If the QBER is beyond a certain threshold, the communicating parties detect Eve and hold the communication [25], [42].

C. Trojan Horse Attacks

In Trojan horse attacks, Eve uses an auxiliary photon to gain access to secret information by analyzing this reflected photon [36]. Similar to the man-in-the-middle attack, Eve can either target Alice's or Bob's end to launch a Trojan horse attack, which can compromise the security and privacy of user information in the Metaverse.

1) Targeting Bob's End: On Bob's end, a fixed H-CQZ unit is attached to the channel. Eve cannot gain any information

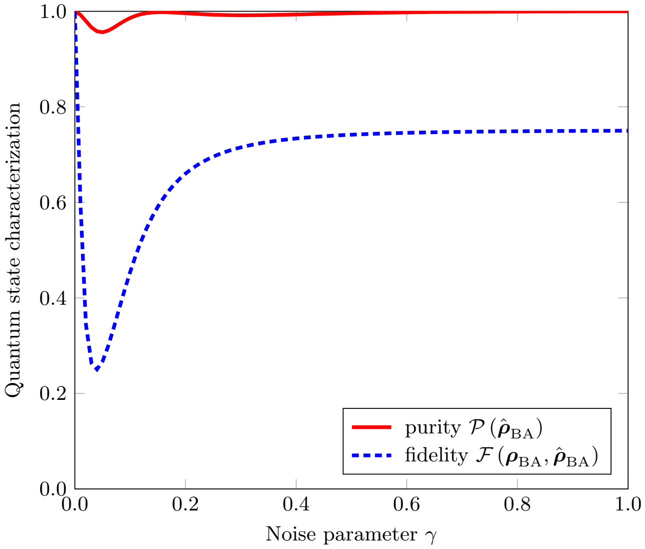


Fig. 8. Fidelity and purity for the CQ-BFT protocol as a function of the noise parameter γ of the path DoF (amplitude damping) noise when $K = 4$, $M = 50$, and $N = 1000$.

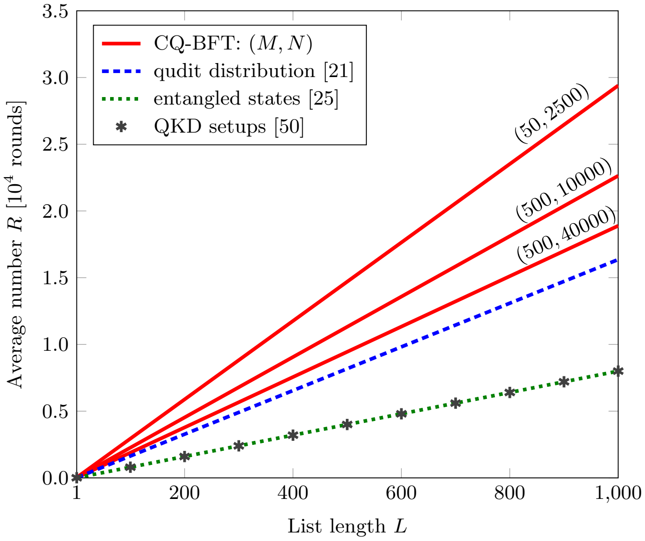


Fig. 9. Average rounds R as a function of the list length L for the CQ-BFT protocol and Byzantine agreement protocols using the qudit distribution [21], multipartite entangled states [25], and QKD setups [50] when $K = 4$. For the CQ-BFT protocol, we choose $(M, N) = (50, 2500)$, $(500, 10000)$, and $(500, 40000)$.

using her probing photon since the setup is publicly known and fixed. The changing components belong to the local computation unit operating $\boldsymbol{C}^{b_i}$ or $\boldsymbol{C}^{\ell s_i}$. However, the local computational elements are inaccessible to Eve's photon.

2) Targeting Alice's End: On Alice's end, the state of the QAO system is evolving under the action of $\boldsymbol{U}$ and $\boldsymbol{V}$ from each party. Alice's QAOs are individually accessible to Eve during the $\boldsymbol{U}$ operation by Bob. Conventionally, Eve can use a photon of either a different wavelength or in a different time window and send it to Alice directly. However, with near-perfect detectors, this attack fails because Alice's absorption of Eve's photon can be communicated between legitimate parties to establish the presence of Eve [36].

3) Counterfactual Trojan Horse Attacks: Alternatively, Eve can launch a counterfactual Trojan horse attack, wherein she sends a polarized photonic component into the channel between Alice and Bob. However, due to the counterfactual nature, the photon may enter the channel resulting in Eve's detection. In case the photon is not absorbed by the QAOs due to weak interaction between the QAOs and photon, Eve does not have enough information to distinguish between possible states of the QAOs [27], [48]. In what follows, we demonstrate numerical examples of this counterfactual Trojan horse attack.

The counterfactual attacking power or hashrate of an eavesdropper is directly proportional to the number of $\hat{M}$ outer and $\hat{N}$ inner cycles that Eve uses to devise her attack configuration. However, she must complete the attack within the access time window of Alice. Let t_{w} and t_{in} denote the access time window of Alice and t_{in} denote the time that Eve needs to complete one inner cycle. Eve is undetectable only if $\hat{M}\hat{N}t_{\mathrm{in}} \leq t_{\mathrm{w}}$, that is, if the whole cycle duration of Eve is less than Alice's access time window. Otherwise, Eve is surely detectable by Alice as her photon will appear in the channel. Under t_{w}, the probability that Eve is detected for a single H-CQZ$_{\hat{M},\hat{N}}$ gate is give by [36]

$$P_1 = \sum_{m=1}^{M_{\mathrm{e}}} \sin\left(m\theta_{\hat{M}}\right)\left[1 - \cos^{2\hat{N}}\left(2\theta_{\hat{N}}\right)\right]. \tag{26}$$

Since $(2k+2)^{K-1}$ H-CQZ$_{\hat{M},\hat{N}}$ gates are required for the complete CQ-BFT operation, the total detection probability is equal to

$$P_{\mathrm{d}} = P_1^{(2k+2)^{K-1}}. \tag{27}$$

Since Bob$_i$ locally encodes b_i and s_i for each CTU operation, the only time window that Eve can manipulate b_i and s_i is the time required to implement the second H-CQZ$_{\hat{M},\hat{N}}$ gate (see Fig. 4). Under these constraints, Fig. 6 shows the probability that Eve is detected for unauthorized access with her attacking power $\hat{M}$ and $\hat{N}$. As $\hat{M}$ and $\hat{N}$ increase, the probability of detecting the presence of Eve in the channel decreases.

D. Entangle-and-Measure Attacks

Eve can entangle her photons with Alice and measure them to project Alice's QAOs into some state for both $\boldsymbol{U}$ and $\boldsymbol{V}$ operations. However, this entangle-and-measure attack leads the final state to a non-Fourier basis state [42]. If Eve is suspected of launching this attack, the protocol may be run multiple times with the same configuration (choice commitment from all parties) [42]. Measuring multiple copies with the same configuration should result in the same measurement outcome in the absence of Eve. Hence, Eve's presence is detectable by different measurement outcomes for multiple runs. This differs from previous protocols [42], where Eve had full access to the qudit and could use Fourier basis measurements herself.

V. Noise Robustness, Scalability, and Decentralization of CQ-BFT

A. Noise Robustness

Noise robustness is extremely important for the blockchain-based Metaverse to scale effectively. Channel noise causes decoherence of quantum states, leading to data corruption, delayed processing, and higher computational requirements. Since the CQ-BFT utilizes counterfactual communication, its noise robustness is closely tied to the counterfactual behavior of the system. In the H-CQZ gate, the $|\mathrm{H}\rangle$ component of the photon wave function passes through the channel under the probabilistic model to interact with the QAOs at Alice's side. However, this photon component carries no information and is discarded to maintain the counterfactuality of the protocol [26], [34]. In counterfactual communication, quantum channel noise in a polarization or path degree of freedom (DoF) of the photon is a significant type of noise.

1) Polarization DoF Noise: We now consider bit-flip, dephasing, and depolarizing noise in the polarization DoF of the photon. These noisy quantum states are described by completely positive trace-preserving (CPTP) maps $\mathcal{N}$ as in (28) where $\boldsymbol{\rho}$ is an arbitrary input state (density matrix), $p \in [0, 1]$ is a noise parameter, and $\boldsymbol{Y}$ denotes the Pauli-Y operator. Let $\boldsymbol{\rho}_{\mathrm{BA}} = |\psi\rangle_{\mathrm{BA}}\langle\psi|$ and $\hat{\boldsymbol{\rho}}_{\mathrm{BA}} = |\hat{\psi}\rangle_{\mathrm{BA}}\langle\hat{\psi}|$ where $|\psi\rangle_{\mathrm{BA}}$ and $|\hat{\psi}\rangle_{\mathrm{BA}}$ denote the output quantum states of the CQ-BFT protocol in noiseless and noisy quantum channels, respectively. Then, the fidelity between the density matrices $\boldsymbol{\rho}_{\mathrm{BA}}$ and $\hat{\boldsymbol{\rho}}_{\mathrm{BA}}$ is given by

$$\mathcal{F}\left(\boldsymbol{\rho}_{\mathrm{BA}}, \hat{\boldsymbol{\rho}}_{\mathrm{BA}}\right) = \mathrm{tr}\left(\sqrt{\sqrt{\boldsymbol{\rho}_{\mathrm{BA}}}\hat{\boldsymbol{\rho}}_{\mathrm{BA}}\sqrt{\boldsymbol{\rho}_{\mathrm{BA}}}}\right)^2 \tag{29}$$

where $\mathrm{tr}\left(\cdot\right)$ denotes the trace operator.

Fig. 7 shows the fidelity $\mathcal{F}\left(\boldsymbol{\rho}_{\mathrm{BA}}, \hat{\boldsymbol{\rho}}_{\mathrm{BA}}\right)$ of the counterfactual list distribution for four parties ($K = 4$) in the presence of the polarization DoF noise when $M = 50$ and $N = 1000$ for each H-CQZ gate utilized in $\boldsymbol{U}$ and $\boldsymbol{V}$ operations. We see the counterfactual list distribution allows perfect robustness against dephasing noise. In contrast, there is a sudden fidelity drop under bit-flip and depolarizing noise. As M and N increase, the large number of cycles increases the sensitivity of the communication system towards bit-flip and dephasing noise. A modified version of CQZ gates has been recently proposed to enhance the noise robustness of counterfactual quantum teleportation [49]. This modification and quantum error correction can be considered to recover the quantum state in the CQ-BFT protocol for noisy quantum channels.

2) Path DoF Noise: To preserve the quantum interference pattern and correctly extract the information, the path length of the photon component in the counterfactual communication channel must be carefully balanced with the reference path length. However, the effective path length can be affected by several reasons, including the photonic loss in the channel. In counterfactual communication, the photon component that enters the transmission channel can be lost due to absorption, scattering, mode mismatch, bend loss, or other factors. This photonic loss causes the disruption of the photon interference pattern in the interferometer, which can be additionally misinterpreted as the absorption of QAO. Hence, this makes it more challenging for the receiver to distinguish the actual information from background noise. The photonic loss can be modeled as amplitude damping noise with a photon decay probability γ [49]. The CPTP map $\mathcal{N}$ for amplitude damping noise can be written as

TABLE I

Scalability efficiency χ_{s} for $K = 4$

Protocol		Efficiency χ_{s}
CQ-BFT: (M, N)	(50, 2500)	0.136
	(200, 10000)	0.176
	(200, 40000)	0.212
Qudit distribution [21]		0.250
Entangled states [25]		0.500
QKD setups [50]		0.500

$$\mathcal{N}\left(\boldsymbol{\rho}\right) = \boldsymbol{E}_0\boldsymbol{\rho}\boldsymbol{E}_0^{\dagger} + \boldsymbol{E}_1\boldsymbol{\rho}\boldsymbol{E}_1^{\dagger} \tag{30}$$

where the superscript † denotes the transpose conjugate and

$$\boldsymbol{E}_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \tag{31}$$

$$\boldsymbol{E}_1 = \begin{bmatrix} 0 & \sqrt{\gamma} \\ 0 & 0 \end{bmatrix} \tag{32}$$

are the Kraus operators acting only on the paths of the inner interferometer of the CQZ gate.

Fig. 8 shows quantum state characterization for the counterfactual list distribution under amplitude damping noise due to the photonic loss when $K = 4$, $M = 50$, and $N = 1000$. Although the fidelity $\mathcal{F}\left(\boldsymbol{\rho}_{\mathrm{BA}}, \hat{\boldsymbol{\rho}}_{\mathrm{BA}}\right)$ of the protocol is not close to one, its noisy purity

$$\mathcal{P}\left(\hat{\boldsymbol{\rho}}_{\mathrm{BA}}\right) = \mathrm{tr}\left(\hat{\boldsymbol{\rho}}_{\mathrm{BA}}^2\right) \tag{33}$$

is almost one, which is a desirable property in many quantum information processing tasks.

B. Scalability

A blockchain network is *scalable* if it can process a large volume of transactions without any delay or difficulties. The blockchain-based Metaverse involves many users generating a high volume of transactions, such as virtual assets and virtual currency transactions. Hence, blockchain scalability is crucial in the Metaverse to ensure the quality of service. The CQ-BFT

$$\mathcal{N}\left(\boldsymbol{\rho}\right) = \begin{cases} \left(1-p\right)\boldsymbol{\rho} + p\boldsymbol{X}\boldsymbol{\rho}\boldsymbol{X}, & \text{bit-flip} \\ \left(1-p\right)\boldsymbol{\rho} + p\boldsymbol{Z}\boldsymbol{\rho}\boldsymbol{Z}, & \text{dephasing} \\ \left(1-\frac{3}{4}p\right)\boldsymbol{\rho} + \frac{1}{4}p\left(\boldsymbol{X}\boldsymbol{\rho}\boldsymbol{X} + \boldsymbol{Y}\boldsymbol{\rho}\boldsymbol{Y} + \boldsymbol{Z}\boldsymbol{\rho}\boldsymbol{Z}\right), & \text{depolarizing} \end{cases} \tag{28}$$

TABLE II
SECURITY, SCALABILITY, AND DECENTRALIZATION FOR Q-BFT PROTOCOLS

Consensus mechanism		CQ-BFT	QDPoS [18]	Q-BFT [20]	Q-BFT [21]
Security	Fault tolerance	$K/2$	$K/2$	$K/2$	$K/2$
	Internal attacks	List inconsistency	Sudden change in voting patterns	List inconsistency	List inconsistency
	External attacks	Resistant against intercept-and-resend attacks man-in-the-middle attacks Trojan horse attacks entangle-and-measure attacks	Resistant against hashrate attacks	N/A	N/A
Scalability	Quantum resources	$k + 2^k - 1$ qubits	k qubits	k qutrits	Single qudit
	Noise robustness	Robust against dephasing noise	N/A	N/A	N/A
	Effieicency	Probabilistic (M, N)	N/A	Probabilistic	Probabilistic
Decentralization		Moderate	High	Low	Moderate

protocol focuses on the consensus layer of the blockchain, where all the parties have an identical view of their agreement, and the multiple operations performed by the parties add more complexity and operational overhead to the network. In addition, due to the distributed nature of blockchain, the Metaverse requires a lot of bandwidth, computing, and storage to ensure the integrity of the ledger. These requirements ultimately reduce the scalability of Metaverse at the expense of enhanced security and noise robustness.

We consider the scalability efficiency as a metric to measure the scalability of the BFT protocol. For the consensus mechanism, the private list distribution between participating nodes is the most crucial stage in the network. For scalability simulations, we measure the average number R of rounds required to produce the list of length L in the CQ-BFT protocol and compare the scalability efficiency χ_{s}—defined by $\chi_{\mathrm{s}} = 2^K L/R$—with the qudit list distribution algorithm [21]. As both protocols are random in nature, the success probability depends on system parameters such as the type of quantum states, basis encoding methods, and the number of nodes. To measure the scalability efficiency, we utilize the discrete event quantum network simulator, which is a tool to simulate a network of quantum processors connected by pairwise classical and quantum channels. The simulation parameters for the CQ-BFT protocol include the node number K, list length L, and the numbers of inner and outer cycles (M and N). These parameters also determine the success probability of the gate operations at each node. If any of the gate operations are unsuccessful, the corresponding node broadcasts a failure message, and the protocol will be restarted.

Fig. 9 shows the average number R of rounds as a function of the list length L for the CQ-BFT and the qudit protocol in [21] when $K = 4$ and $(M, N) = (50, 2500)$, $(500, 10000)$, and $(500, 40000)$. For comparison, we also plot the simulation results for two other Byzantine agreement protocols using the multipartite entangled states [25] and quantum key distribution (QKD) setups [50] to distribute the private correlated list. Note that the scalability efficiency χ_{s} of the qudit distribution protocol [21] serves as an upper bound for the CQ-BFT protocol's scalability efficiency, approaching as M and N go to infinity (see Table I). However, large M and N also increase the time required to complete the list distribution task, which highlights the tradeoff of the CQ-BFT protocol between security and scalability. Both protocols proposed in [25] and [50] have higher scalability efficiency than the qudit or CQ-BFT protocols. However, since these protocols require multiple measurement devices on each node, their scalability deteriorates exponentially with detector imperfections [21]. In contrast, the CQ-BFT protocol requires only a single measurement regardless of the number of nodes, which provides more robustness toward detector imperfections.

C. Decentralization

Decentralization in the human-centric Metaverse provides individuals authority over their assets, data, and identities. This property enables users to contribute to developing the virtual platform and engage in decision-making processes. Generally, decentralization is determined by the level of dependency between nodes. Here, we describe this dependency as the number of operations each node performs during the protocol. In the qudit distribution protocol [21], each node performs three fundamental tasks. All nodes can communicate quantum states and perform quantum operations. The initial node has the additional task of generating quantum states and starting the protocol, while the last node can measure the quantum states and broadcast its results to all other nodes. In a general setup, each node can be the initial or last node. This increases the degree of decentralization as the node need not rely on a trusted external source as in [20]. In the CQ-BFT protocol, the role of each node remains unchanged, as in the qudit protocol, which reveals the same decentralization degree. It has been claimed that the quantum delegated proof of stake (QDPoS) protocol has full decentralization due to the fact that it requires no trusted certificate authority [18]. The CQ-BFT protocol still requires a trusted state distribution. However, this can be easily verified by partitioning the protocol into verification steps before performing the list distribution [25].

The security, scalability, and decentralization are compared in Table II for four quantum consensus protocols applicable to the blockchain and the human-centric Metaverse: CQ-BFT, quantum delegated proof of stake (QDPoS) [18], entangled qutrit [20], and qudit distribution [21] protocols. While it is challenging to satisfy all stringent requirements of the blockchain simultaneously in counterfactual setups, resource optimization [51] and error correction techniques can be further considered to enhance the scalability of the CQ-BFT protocol.

VI. Conclusion

We have devised counterfactual unitary telecomputation to securely distribute correlated private lists for the BFT consensus. Our counterfactual BFT protocol has been demonstrated to be resistant to attacks from external adversaries and malicious parties who conspire to compromise the system security. In addition, the protocol withstands dephasing noise and operates efficiently even without a shared phase reference. Moreover, the CQ-BFT protocol inherits the same fault tolerance bound as the known Q-BFT protocol and is highly decentralized. These advantages make it a suitable candidate for blockchain-based human-centric Metaverse applications. The use of this counterfactual BFT design in quantum blockchain promises the next phase of blockchain, leading to the secure human-centric Metaverse.

References

[1] H. Ning, H. Wang, Y. Lin, W. Wang, S. Dhelim, F. Farha, J. Ding, and M. Daneshmand, "A survey on Metaverse: The state-of-the-art, technologies, applications, and challenges," *arXiv:2111.09673*, 2021.

[2] L. Cao, "Decentralized AI: Edge intelligence and smart blockchain, Metaverse, Web3, and DeSci," *IEEE Intell. Syst.*, vol. 37, no. 3, pp. 6–19, Jul. 2022.

[3] Y. Fu, C. Li, F. R. Yu, T. H. Luan, P. Zhao, and S. Liu, "A survey of blockchain and intelligent networking for the Metaverse," *IEEE Internet Things J.*, vol. 10, no. 4, Nov. 2022.

[4] M. A. I. Mozumder, M. M. Sheeraz, A. Athar, S. Aich, and H.-C. Kim, "Overview: Technology roadmap of the future trend of Metaverse based on IoT, blockchain, AI technique, and medical domain Metaverse activity," in *Proc. International Conference on Advanced Communication Technology (ICACT)*, PyeongChang, Korea, Feb. 2022, pp. 256–261.

[5] H. Lin, S. Wan, W. Gan, J. Chen, and H.-C. Chao, "Metaverse in education: Vision, opportunities, and challenges," *arXiv:2211.14951*, 2022.

[6] M. Wang, H. Yu, Z. Bell, and X. Chu, "Constructing an edu-Metaverse ecosystem: A new and innovative framework," *IEEE Trans. Learn. Technol.*, vol. 15, no. 6, pp. 685–696, Sep. 2022.

[7] G. W. et al., "Development of Metaverse for intelligent healthcare," *Nat. Mach. Intell.*, vol. 4, no. 11, pp. 922–929, Sep. 2022.

[8] F. M. F. Saboune, "Virtual reality in social media marketing will be the new model of advertising and monetization," in *Proc. International Conference on Social Networks Analysis, Management and Security (SNAMS)*, Milan, Italy, Nov. 2022, pp. 1–7.

[9] P. Bhattacharya, M. S. Obaidat, D. Savaliya, S. Sanghavi, S. Tanwar, and B. Sadaun, "Metaverse assisted telesurgery in healthcare 5.0: An interplay of blockchain and explainable AI," in *Proc. of International Conference on Computer, Information and Telecommunication Systems (CITS)*, Piraeus, Greece, Jul. 2022, pp. 1–5.

[10] A. Singhal, N. Singhal, K. Sharma *et al.*, "Metaverse: Cryptocurrency price analysis using Monte Carlo simulation," in *Proc. International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, India, Jan. 2023, pp. 1–8.

[11] Z. Chen, J. Wu, W. Gan, and Z. Qi, "Metaverse security and privacy: An overview," *arXiv:2211.14948*, 2022.

[12] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "Metachain: A novel blockchain-based framework for Metaverse applications," *arXiv:2201.00759*, 2021.

[13] Y. Cai, J. Llorca, A. M. Tulino, and A. F. Molisch, "Compute-and data-intensive networks: The key to the Metaverse," in *Proc. International Conference on 6G Networking (6GNet)*, Paris, France, Jul. 2022, pp. 1–8.

[14] F. Tang, X. Chen, M. Zhao, and N. Kato, "The roadmap of communication and networking in 6G for the Metaverse," *IEEE Wirel. Commun.*, pp. 1–15, June 2022 (Early Access), doi:10.1109/MWC.019.2100721.

[15] F. Zaman, A. Farooq, M. A. Ullah, H. Jung, H. Shin, and M. Z. Win, "Quantum machine intelligence for 6G URLLC," *IEEE Wireless Commun.*, vol. 30, no. 2, pp. 22–30, Apr. 2023.

[16] V. Bhatia and K. Ramkumar, "An efficient quantum computing technique for cracking RSA using Shor's algorithm," in *Proc. International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, Oct. 2020, pp. 89–94.

[17] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.

[18] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism QDPoS," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, pp. 3264–3276, Aug. 2022.

[19] M. Dianati and R. Alléaume, "Architecture of the secoqc quantum key distribution network," in *Proc. International Conference on Quantum, Nano, and Micro Technologies (ICQNM)*, Guadeloupe, French Caribbean, Jan. 2007.

[20] M. Fitzi, N. Gisin, and U. Maurer, "Quantum solution to the Byzantine agreement problem," *Phys. Rev. Lett.*, vol. 87, no. 21, p. 217901, Nov. 2001.

[21] A. Tavakoli, A. Cabello, M. Żukowski, and M. Bourennane, "Quantum clock synchronization with a single qudit," *Sci. Rep.*, vol. 5, no. 1, p. 7982, Jan. 2015.

[22] M. Fitzi, N. Gisin, U. Maurer, and O. von Rotz, "Unconditional Byzantine agreement and multi-party computation secure against dishonest minorities from scratch," in *Proc. International Conference on the Theory and Applications of Cryptographic Techniques*, Amsterdam, Netherlands, Apr. 2002, pp. 482–501.

[23] Z. Quan and T. Chaojing, "Simple proof of the unconditional security of the Bennett 1992 quantum key distribution protocol," *Phys. Rev. A*, vol. 65, no. 6, p. 062301, May 2002.

[24] A. Cabello, "Solving the liar detection problem using the four-qubit singlet state," *Phys. Rev. A*, vol. 68, no. 1, p. 012304, Jul. 2003.

[25] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter, "Experimental demonstration of a quantum protocol for Byzantine agreement and liar detection," *Phys. Rev. Lett.*, vol. 100, no. 7, p. 070504, Feb. 2008.

[26] H. Salih, Z. H. Li, M. Al-Amri, and M. S. Zubairy, "Protocol for direct counterfactual quantum communication," *Phys. Rev. Lett.*, vol. 110, no. 17, pp. 1–5, Apr. 2013.

[27] T.-G. Noh, "Counterfactual quantum cryptography," *Phys. Rev. Lett.*, vol. 103, no. 23, p. 230501, Dec. 2009.

[28] R. H. Dicke, "Interaction-free quantum measurements: A paradox," *Am. J. Phys.*, vol. 49, no. 10, pp. 925–930, Oct. 1981.

[29] P. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. A. Kasevich, "Interaction-free measurement," *Phys. Rev. Lett.*, vol. 74, no. 24, p. 4763, Nov. 1995.

[30] W. M. Itano, D. J. Heinzen, J. J. Bollinger, and D. Wineland, "Quantum Zeno effect," *Phys. Rev. A*, vol. 41, no. 5, p. 2295, Mar. 1990.

[31] Z.-H. Li, M. Al-Amri, and M. S. Zubairy, "Direct counterfactual transmission of a quantum state," *Phys. Rev. A*, vol. 92, no. 5, p. 052315, Nov 2015.

[32] Z.-H. Li, M. Al-Amri, X.-H. Yang, and M. S. Zubairy, "Counterfactual exchange of unknown quantum states," *Phys. Rev. A*, vol. 100, no. 2, p. 022110, Aug. 2019.

[33] H. A. Shenoy, R. Srikanth, and T. Srinivas, "Counterfactual quantum certificate authorization," *Phys. Rev. A*, vol. 89, no. 5, p. 052307, May 2014.

[34] F. Zaman, U. Khalid, T. Q. Duong, H. Shin, and M. Z. Win, "Quantum full-duplex communication," *IEEE J. Sel. Areas Commun.*, June 2023 (Early Access), doi:10.1109/JSAC.2023.3287611.

[35] F. Zaman, S. N. Paing, A. Farooq, H. Shin, and M. Z. Win, "Concealed quantum telecomputation for anonymous 6G URLLC networks," *IEEE J. Sel. Areas Commun.*, vol. 41, no. 7, pp. 2278–2296, Jul. 2023.

[36] Z.-H. Li, L. Wang, J. Xu, Y. Yang, M. Al-Amri, and M. S. Zubairy, "Counterfactual trojan horse attack," *Phys. Rev. A*, vol. 101, no. 2, p. 022336, Feb. 2020.

[37] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS attacks from flash crowds using flow correlation coefficient," *IEEE Trans. Parallel. Distrib. Syst.*, vol. 23, no. 6, pp. 1073–1080, Jun. 2012.

[38] D. Wu and N. Ansari, "A cooperative computing strategy for blockchain-secured fog computing," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6603–6609, Jul. 2020.

[39] ——, "A trust-evaluation-enhanced blockchain-secured industrial IoT system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5510–5517, Oct. 2020.

[40] I. Homoliak, S. Venugopalan, D. Reijsbergen, Q. Hum, R. Schumi, and P. Szalachowski, "The security reference architecture for blockchains: Toward a standardized model for studying vulnerabilities, threats, and defenses," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 1, pp. 341–390, Oct. 2021.

[41] M.-Y. Kao, *Encyclopedia of algorithms*. Springer Science & Business Media, 2016.

[42] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, "Experimental quantum multiparty communication protocols," *npj Quantum Inf.*, vol. 2, no. 1, p. 16010, Jun. 2016.

[43] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Commun. Surv. Tutor.*, vol. 22, no. 2, pp. 1432–1465, May 2020.

[44] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *J. ACM*, vol. 27, no. 2, p. 228–234, Apr. 1980.

[45] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, p. 382–401, Jul. 1982.

[46] E. O. Ilo-Okeke, L. Tessler, J. P. Dowling, and T. Byrnes, "Remote quantum clock synchronization without synchronized clocks," *npj Quantum Inf.*, vol. 4, no. 1, p. 40, Aug. 2018.

[47] S. D. Bartlett, T. Rudolph, and R. W. Spekkens, "Reference frames, superselection rules, and quantum information," *Rev. Mod. Phys.*, vol. 79, no. 2, pp. 555–609, Apr. 2007.

[48] X. Yang, K. Wei, H. Ma, S. Sun, Y. Du, and L. Wu, "Trojan horse attacks on counterfactual quantum key distribution," *Phys. Lett. A*, vol. 380, no. 18, pp. 1589–1592, Apr. 2016.

[49] M. A. Ullah, S. N. Paing, and H. Shin, "Noise-robust quantum teleportation with counterfactual communication," *IEEE Access*, vol. 10, pp. 61 484–61 493, Mar. 2022.

[50] S. Iblisdir and N. Gisin, "Byzantine agreement with two quantum-key-distribution setups," *Phys. Rev. A*, vol. 70, no. 3, p. 034306, Sep. 2004.

[51] F. Zaman, K. Lee, and H. Shin, "Information carrier and resource optimization of counterfactual quantum communication," *Quantum Inf. Process.*, vol. 20, no. 5, p. 168, May 2021.

Saw Nang Paing received the B.E. degree in computer engineering and information technology from Mandalay Technology University (MTU), Myanmar, in 2019. She is working towards the Ph.D. degree in quantum information science with the Department of Electronics and Information Convergence Engineering, Kyung Hee University (KHU), South Korea. Her research interests include distributed quantum networks, quantum communication, and quantum security.

Jason William Setiawan received the B.S. degree in electrical engineering from Bandung Institute of Technology, Indonesia, in 2020. He is currently pursuing the Ph.D. degree in quantum information science with the Department of Electronics and Information Convergence Engineering, Kyung Hee University (KHU), South Korea. His research interests include quantum information science, quantum communication, and quantum networks.

Muhammad Asad Ullah received his Ph.D. from the Department of Electronics and Information Convergence Engineering, Kyung Hee University, in 2022. Before that, he received his B.E. degree in electrical engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2014. His research interests include quantum computing, quantum communications, and quantum algorithms.

Fakhar Zaman (Member, IEEE) received the B.E. degree in electrical engineering from the National University of Sciences and Technology (NUST), Pakistan, in 2015 and Ph.D. degree in Electronics and Information Convergence Engineering from the Kyung Hee University (KHU), S. Korea, in 2023. During his Ph.D., he spent one year at the Massachusetts Institute of Technology (MIT) as an exchange visiting student. At MIT, he was with the Laboratory for Information and Decision Systems from September 2022 to August 2023.

Currently, he is a CSIRO Early Research Career (CERC) Fellow at the Commonwealth Scientific and Industrial Research Organisation (CSIRO), Australia. His research interests include quantum-enhanced reinforcement learning, quantum machine learning, quantum error mitigation, and robotics.

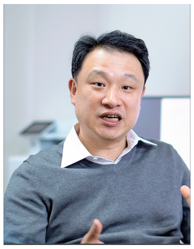
Dr. Zaman received the Best Paper award at KICS-Fall Conference on Communications in 2019. He served as a reviewer for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS and several international conferences.

Trung Q. Duong (Fellow, IEEE) received his Ph.D. degree in telecommunications systems from Blekinge Institute of Technology, Sweden in 2012. In 2013, he joint Queen's University Belfast, UK, as an academic staff, where he is now a Chair Professor in Telecommunications. He is a Research Chair of the Royal Academy of Engineering. He was a Distinguished Advisory Professor at Inje University, South Korea (2017-2019). He is an Adjunct Professor and the Director of Institute for AI and Big Data at Duy Tan University, Vietnam (2012-present), a Distinguished Professor at Thuyloi University, Vietnam (2023-2028) and a Visiting Professor (under Eminent Scholar program) at Kyung Hee University, South Korea (2023-2024). His current research interests include quantum communications, wireless communications, signal processing, machine learning, and realtime optimisation.

Dr. Duong has served as an Editor/Guest Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON COMMUNICATIONS, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS LETTERS, IEEE WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS MAGAZINES, and IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS. He received the Best Paper Award at the IEEE VTC-Spring 2013, IEEE ICC 2014, IEEE GLOBECOM 2016, 2019, 2022, IEEE DSP 2017, and IWCMC 2019, 2023. He is the recipient of prestigious Royal Academy of Engineering Research Fellowship (2015-2020) and has won a prestigious Newton Prize 2017. He is a Fellow of Asia-Pacific Artificial Intelligence Association (AAIA).

Octavia A. Dobre (Fellow, IEEE) received the Dipl. Ing. and Ph.D. degrees from the Polytechnic Institute of Bucharest, Romania, in 1991 and 2000, respectively. Between 2002 and 2005, she was with the New Jersey Institute of Technology, USA. In 2005, she joined Memorial University, Canada, where she is currently a Professor and Canada Research Chair Tier 1. She was a Visiting Professor with Massachusetts Institute of Technology, USA and Université de Bretagne Occidentale, France. Her research interests encompass wireless communication and networking technologies, as well as optical and underwater communications. She has (co-)authored over 450 refereed papers in these areas.

Dr. Dobre serves as the Director of Journals of the Communications Society. She was the inaugural Editor-in-Chief (EiC) of the IEEE OPEN JOURNAL OF THE COMMUNICATIONS SOCIETY and the EiC of the IEEE COMMUNICATIONS LETTERS. Dr. Dobre was a Fulbright Scholar, Royal Society Scholar, and Distinguished Lecturer of the IEEE Communications Society. She obtained Best Paper Awards at various conferences, including IEEE ICC, IEEE Globecom, IEEE WCNC, and IEEE PIMRC. Dr. Dobre is an elected member of the European Academy of Sciences and Arts, a Fellow of the Engineering Institute of Canada, and a Fellow of the Canadian Academy of Engineering.



Hyundong Shin (Fellow, IEEE) received the B.S. degree in Electronics Engineering from Kyung Hee University (KHU), Yongin-si, Korea, in 1999, and the M.S. and Ph.D. degrees in Electrical Engineering from Seoul National University, Seoul, Korea, in 2001 and 2004, respectively. During his postdoctoral research at the Massachusetts Institute of Technology (MIT) from 2004 to 2006, he was with the Laboratory for Information Decision Systems (LIDS). In 2006, he joined the KHU, where he is currently a Professor in the Department of Electronic Engineering. His research interests include quantum information science, wireless communication, and machine intelligence. Dr. Shin received the IEEE Communications Society's Guglielmo Marconi Prize Paper Award and William R. Bennett Prize Paper Award. He served as the Publicity Co-Chair for the IEEE PIMRC and the Technical Program Co-Chair for the IEEE WCNC and the IEEE GLOBECOM. He was an Editor of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS and IEEE COMMUNICATIONS LETTERS.