information

Article

A Quantum Approach to News Verification from the Perspective of a News Aggregator

Theodore Andronikos [1,*,†] and Alla Sirokofskich [2,†]

[1] Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece
[2] Department of History and Philosophy of Sciences, National and Kapodistrian University of Athens, 15771 Athens, Greece; asirokof@math.uoa.gr
* Correspondence: andronikos@ionio.gr
† These authors contributed equally to this work.

Abstract: In the dynamic landscape of digital information, the rise of misinformation and fake news presents a pressing challenge. This paper takes a completely new approach to verifying news, inspired by how quantum actors can reach agreement even when they are spatially spread out. We propose a radically new—to the best of our knowledge—algorithm that uses quantum "entanglement" (think of it as a special connection) to help news aggregators "sniff out" bad actors, whether they are other news sources or even fact-checkers trying to spread misinformation. This algorithm does not rely on quantum signatures; it merely uses basic quantum technology which we already have, in particular, special pairs of particles called "EPR pairs" that are much easier to create than other options. More elaborate entangled states are like juggling too many balls—they are difficult to make and slow things down, especially when many players are involved. So, we adhere to Bell states, the simplest form of entanglement, which are easy to generate no matter how many players are involved. This means that our algorithm is faster to set up, works for any number of participants, and is more practical for real-world use. Additionally, as a "bonus point", it finishes in a fixed number of steps, regardless of how many players are involved, making it even more scalable. This new approach may lead to a powerful and efficient way to fight misinformation in the digital age, using the weird and wonderful world of quantum mechanics.

Keywords: fake news; quantum algorithms; quantum entanglement; Bell states; quantum games

Citation: Andronikos, T.; Sirokofskich, A. A Quantum Approach to News Verification from the Perspective of a News Aggregator. *Information* **2024**, *15*, 207. https://doi.org/10.3390/info15040207

Academic Editors: Wenbin Yu, Yadang Chen and Chengjun Zhang

Received: 27 February 2024
Revised: 31 March 2024
Accepted: 3 April 2024
Published: 6 April 2024

1. Introduction

In the contemporary digital era, the proliferation of fake news, defined as deliberately false information masquerading as legitimate news, has emerged as a pervasive challenge across online and social media platforms. The rapid dissemination of misinformation poses serious repercussions, eroding trust in institutions, inciting violence, and undermining democratic processes. The urgent need for robust fake news detection mechanisms is more pronounced than ever. Fake news flourishes in the online realm due to several contributing factors. The accessibility of content creation and sharing, coupled with anonymity and the absence of stringent oversight, empowers malicious actors to disseminate false narratives with impunity. Furthermore, social media algorithms, often designed to prioritize sensational and engaging content, inadvertently amplify the reach of fake news.

The prevalence of fake news underscores the necessity for the development and deployment of effective detection techniques. One strategy involves leveraging fact-checking organizations to manually verify the veracity of information. However, this approach is labor-intensive and unable to cope with the sheer volume of content produced daily. Alternatively, employing artificial intelligence (AI) and machine learning (ML) methodologies offers promise in automatically identifying fake news. These algorithms can scrutinize various factors, including language usage, writing style, and source reliability, to flag

potentially misleading content. Despite the potential of AI-driven detection methods, they encounter challenges. Fake news purveyors continuously adapt their strategies to evade detection, and AI models may exhibit biases or inaccuracies if trained on inadequate or skewed datasets.

Recent research [1,2] underscores the necessity for social media platforms to integrate diverse content verification techniques alongside existing algorithms and AI approaches to combat false news effectively. Additionally, taxonomy frameworks like the one proposed in [3,4], which categorizes false news into distinct types, can aid social media platforms in alerting users to potentially misleading content, contingent upon predefined standards for content analysis. The endeavor to automate the detection and prevention of false news presents formidable challenges, particularly concerning the assessment of content legitimacy [5,6]. Contemporary efforts predominantly rely on machine learning techniques to identify and mitigate fake news articles, as evidenced by numerous recent scholarly works [7–16]. The fusion of AI with blockchain technology emerges as a promising avenue for combating fake news [17]. This approach offers a decentralized and trustworthy platform for validating consent, authenticity, integrity, and perspectives on truth, thereby mitigating the spread of false narratives.

The quest for quantum computers that are powerful enough to dethrone their classical counterparts continues. While we have not reached the promised land yet, recent breakthroughs like IBM's 127-qubit Eagle [18], 433-qubit Osprey [19], and the colossal 1121-qubit Condor [20] indicate that progress is accelerating. Perhaps we are closer than we think to the quantum revolution. Simultaneously, impressive progress on nanomaterials suitable for quantum information processing and communications has been very recently achieved [21–24]. Given this broader context, it becomes clear that quantum technology has reached a level of maturity where it merits serious consideration for inclusion in a comprehensive framework aimed at combating misinformation.

As explained above, it seems doubtful that one single approach will be able to tackle the spread of fake news. A plethora of combined techniques and methodologies from different areas may prove more beneficial for that purpose. In our view, AI alone will not be sufficient, as it is plagued by an inherent antinomy. On one hand, AI possesses the capability to identify and mitigate false news, but, on the other hand, AI facilitates the proliferation of such deceptive online content. Having said that, we emphasize that AI can play an important role to this end. This role will be evident in the quantum era. Quantum machine learning seeks to merge the principles of quantum computing with those of machine learning. Considering the potential of quantum computers to enhance and far surpass the speed and efficiency of classical machine learning algorithms, it promises tangible advantages over classical ML, such as improved deepfake detection [25]. Researchers are actively pursuing the development of algorithmic methods that could effectively detect fake news and deepfakes by integrating quantum machine learning techniques [26]. Tian et al. [27] proposed a fake news detection system utilizing quantum K-Nearest Neighbors. Furthermore, Google has introduced an open-source library for quantum machine learning, suggesting the potential for quantum computing to address fake and deepfake challenges in the near term [28].

However, this paper explores a distinct quantum approach that can complement the use of quantum machine learning. It draws inspiration from successful quantum protocols that achieve distributed consensus and detectable Byzantine Agreement in distributed environments such as [29]. We acknowledge the prevalent practice in contemporary social media platforms, wherein independent third-party fact-checking organizations, certified by impartial authorities, are employed to identify, assess, and take action on content. This fact-checking methodology primarily targets viral misinformation, particularly blatant falsehoods lacking factual basis. Ideally, fact-checking entities prioritize verifying demonstrably false claims that are both timely and impactful. Naturally, fact-checkers themselves should be subject to scrutiny and ongoing evaluation. The algorithm proposed herein envi-

sions a decentralized setting where numerous news aggregators are overseen by multiple news verifiers responsible for content authentication.

Described as a quantum game, our algorithm involves familiar figures such as Alice and Bob, alongside their numerous counterparts. Employing games in our presentation aims to facilitate the comprehension of technical concepts. The year 1999 marked the beginning of quantum game theory with David Meyer's introduction of the PQ penny flip game [30]. This game mirrored the classic coin toss but with a quantum twist. Another key development came that same year from Eisert et al. [31]. They introduced the Eisert–Wilkens–Lewenstein protocol, a now widely used tool. This protocol allowed them to create a quantum version of the famous "Prisoner's Dilemma" where a quantum strategy could outperform any classical one [31]. This breakthrough sparked further research, with works like that of Rycerz et al.'s in 2020 building upon the Eisert–Wilkens–Lewenstein protocol [32]. For a recent sophisticated approach to the "Prisoner's Dilemma", we refer to [33] and references therein. While the quantum player often holds an advantage, it is not always a one-sided affair. Anand et al. in 2015 cleverly modified the PQ penny flip game rules to allow the classical player to win [34]. In [35], it was shown that the PQ penny flip game exhibits a fundamental connection to the dihedral groups. Another recent work explored general scenarios where both players choose moves from specific groups, leading to new insights [36]. Unsurprisingly, the concept of quantum coin flipping plays a vital role in secure communication protocols, where parties like Alice and Bob strive for agreement on a random bit. Bennett et al.'s seminal work in 2014 is a cornerstone in this area [37]. Notably, entanglement, a hallmark of quantum mechanics, plays a crucial role in many of these advancements. Moreover, even classical political institutions can undergo a quantization process, as demonstrated recently in [38].

Contribution. This paper introduces a novel perspective on the pressing issue of news verification by drawing inspiration from quantum protocols achieving distributed consensus, diverging from the more conventional quantum machine learning approach. We present the first entanglement-based algorithm, to the best of our knowledge, designed for news aggregators to identify potential malicious actors. These actors could include other news aggregators or, even more concerning, fact-checkers intentionally disseminating misinformation.

The key advantage of our algorithm, which does not rely on a quantum signature scheme, lies in its compatibility with current quantum technology, as it solely depends on EPR pairs. While more complex multi-particle entangled states are possible, they are challenging to produce with existing quantum systems, leading to extended preparation times and complexity, particularly in scenarios involving numerous participants. Contemporary quantum computers can easily generate $|GHZ_n\rangle$ and $|W_n\rangle$ states for small values of n. A methodology for constructing quantum circuits for such states is given in [39]. The resulting quantum circuits are efficient in the sense that they require $\lg n$ steps to generate the $|GHZ_n\rangle$ and $|W_n\rangle$ states. Unfortunately, the preparation and distribution of these states become increasingly difficult as n grows. Therefore, we exclusively employ Bell states, the simplest among maximally entangled states, in our algorithm.

Utilizing only EPR pairs—specifically $|\Phi^+\rangle$ pairs, regardless of the number of news aggregators and verifiers—results in reduced preparation time, improved scalability, and enhanced practicality. Additionally, our algorithm completes in a constant number of steps, irrespective of the number of participants, further enhancing its scalability and efficiency.

Organization

This article is organized as follows. The Introduction (Section 1) presents the subject matter, accompanied by bibliographic references to related works. A concise overview of the essential concepts is provided in Section 2, laying the foundation for understanding our protocol. A detailed explanation of the hypotheses underlying the QNVA is given in Section 3. The QNVA is formally presented in Section 4, where its inner workings are

explained in detail. The paper concludes with a summary and discussion of the finer points of the algorithm in Section 5.

2. Background and Notation

2.1. EPR Pairs

Quantum entanglement is a phenomenon where two or more particles become linked in such a way that they share the same fate, despite being separated by vast distances. This connection is so powerful that measuring the properties of one particle instantly determines the corresponding properties of its entangled partner, regardless of the separation between them. This instantaneous correlation defies our classical understanding of the universe and has profound implications for quantum mechanics and its potential applications. Mathematically, a single product state is not sufficient to describe entangled states of composite systems. Consequently, they must be described as a linear combination of two or more product states of their subsystems. The famous Bell states [40] are special quantum states involving two qubits, also called EPR pairs, that represent the simplest form of maximal entanglement. These states can be compactly described by the following formula, which was obtained from [41]:

$$\left|\beta_{x,y}\right\rangle = \frac{|0\rangle|y\rangle + (-1)^x|1\rangle|\overline{y}\rangle}{\sqrt{2}}\,, \tag{1}$$

where $|\overline{y}\rangle$ is the negation of $|y\rangle$.

There are four Bell states, and their specific mathematical expression is given below. The subscripts A and B are used to emphasize the subsystem to which the corresponding qubit belongs, that is, qubits $|\cdot\rangle_A$ belong to Alice and qubits $|\cdot\rangle_B$ belong to Bob.

$$\left|\Phi^+\right\rangle = |\beta_{00}\rangle = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B}{\sqrt{2}} \tag{2}$$

$$|\Phi^-\rangle = |\beta_{10}\rangle = \frac{|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B}{\sqrt{2}} \tag{3}$$

$$\left|\Psi^+\right\rangle = |\beta_{01}\rangle = \frac{|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B}{\sqrt{2}} \tag{4}$$

$$|\Psi^-\rangle = |\beta_{11}\rangle = \frac{|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B}{\sqrt{2}} \tag{5}$$

For existing quantum computers based on the circuit model, it is quite trivial to produce Bell states. The proposed algorithm relies on $|\Phi^+\rangle = \frac{|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B}{\sqrt{2}}$ pairs.

2.2. The State $|+\rangle$

Apart from $|\Phi^+\rangle$ pairs, our scheme makes use of another signature state, namely $|+\rangle$. For completeness, we recall the definition of $|+\rangle$ below:

$$|+\rangle = H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,. \tag{6}$$

State $|+\rangle$ can be readily produced by applying the Hadamard transform on $|0\rangle$. In the rest of this paper, the set of bit values $\{0, 1\}$ is denoted by $\mathbb{B}$. As a final note, let us clarify that measurements are always performed with respect to the computational basis $\{|0\rangle, |1\rangle\}$.

3. Hypotheses and Setting

Before we proceed with the comprehensive presentation of the proposed algorithm, it is useful to explicitly state the envisioned setting and the hypotheses that underlie the execution of our algorithm.

3.1. The Protagonists

As we have previously mentioned, we follow what can, almost, be considered a tradition and describe the proposed algorithm as a game. The players in this game are the spatially distributed news verifiers and news aggregators, collectively called Alice and Bob. First, we state the actors that appear in our settings and clarify the roles they are supposed to play:

($\mathbf{H}_1$) A trusted quantum source There exists a trusted quantum source that generates single qubits in the $|+\rangle$ state and EPR pairs in the $|\Phi^+\rangle$ state. The source also distributes these qubits to all other players through appropriate quantum channels, according to the entanglement distribution scheme outlined in the forthcoming Definition 1.

($\mathbf{H}_2$) News verifiers. There exist m special players that are called news verifiers. Their mission is to fact-check every piece of news and classify it as true or fake. In our game, this role is undertaken by Alice and her clones, who are denoted by $\text{Alice}_1, \ldots, \text{Alice}_m$. The news verifiers work independently of each other, and no communication, classical or quantum, takes place between any two of them.

($\mathbf{H}_3$) News aggregators. There are also n players that are called news aggregators, whose purpose is to gather and disseminate news that have been certified as true. This role is assumed by Bob and his clones that are denoted by $\text{Bob}_1, \ldots, \text{Bob}_n$, where, typically, $n > m$.

3.2. The Connections among the Players

Besides the players listed above, there is a network of quantum and classical channels that enables the exchange of information among the players. In particular, we assume the existence of the following communication channels:

($\mathbf{H}_4$) It is more realistic to consider that each Alice clone is not responsible for all news aggregators, but only for a specific group of news aggregators that are under her supervision. Henceforth, we shall assume that each Alice_i, $1 \leq i \leq m$, is connected via pairwise authenticated classical channels to a specific subset of news aggregators who constitute her active network, and Alice_i is their coordinator. These aggregators are Alice_i's receivers; their cardinality is denoted by n_i and they are designated by $\text{Bob}_1^i, \text{Bob}_2^i, \ldots, \text{Bob}_{n_i}^i$.

($\mathbf{H}_5$) Each Alice_i, $1 \leq i \leq m$, sends two things to every Bob_k^i, $1 \leq k \leq n_i$, in her active network:

- ◇ The result of the verification check, denoted by c_k^i.
- ◇ A proof sequence, denoted by $\mathbf{p}_k^i$, which is intended to convince Bob_k^i that she is honest.

The situation is visually depicted in Figure 1.

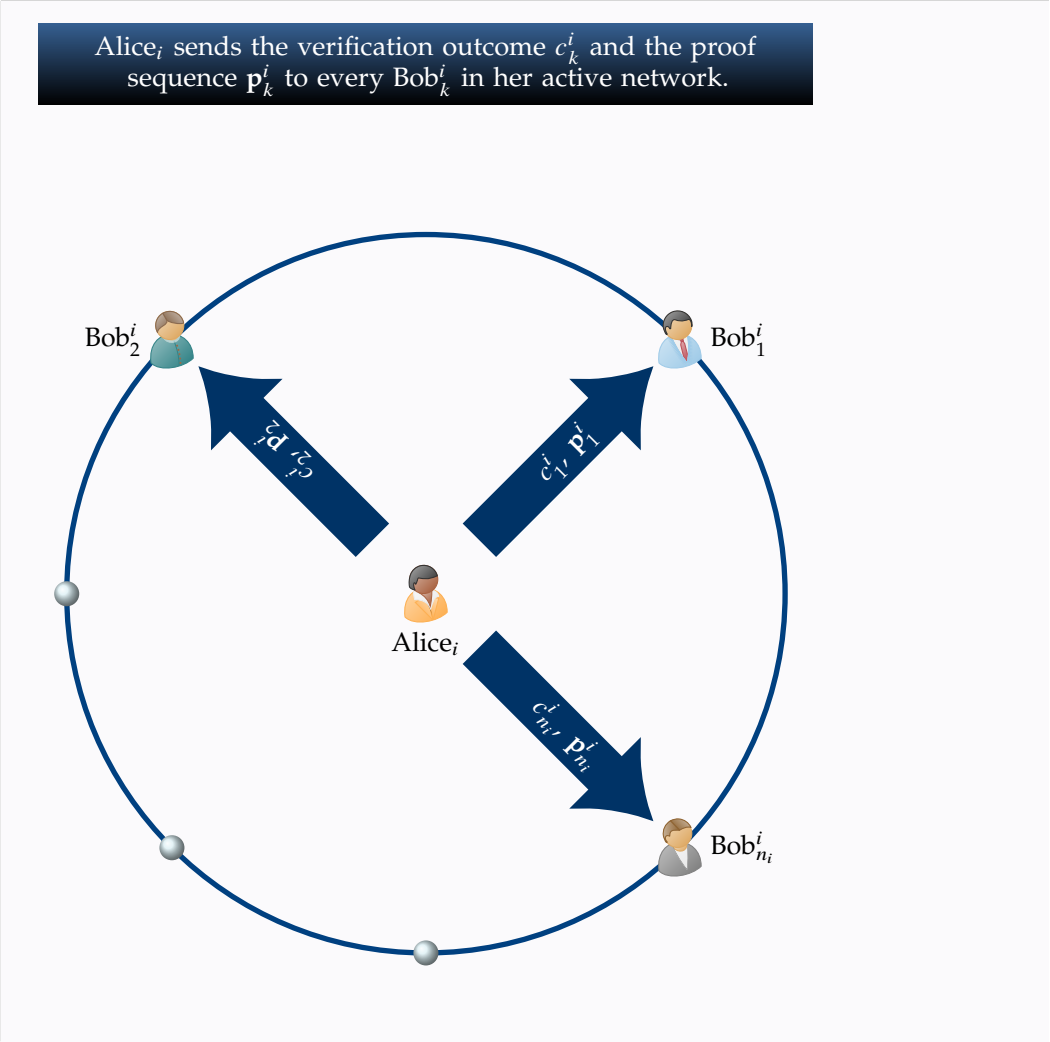

Figure 1. The above figure illustrates the fact that Alice$_i$, $1 \leq i \leq m$, sends the verification outcome c_k^i and the proof sequence $\mathbf{p}_k^i$ to every Bob$_k^i$, $1 \leq k \leq n_i$, in her active network.

(**H**$_6$) All news aggregators that belong to the same active network are connected via pairwise authenticated classical channels. This enables them to exchange, whenever they deem necessary, the verification outcomes and the proof sequences they received from their coordinator. This action can be considered as an extra layer of verification and an indirect way in which aggregators can assess the honesty of other aggregators, as well as the honesty of their coordinator. This topology is shown in Figure 2. We clarify that aggregators that have no coordinator in common, do not communicate in any way.

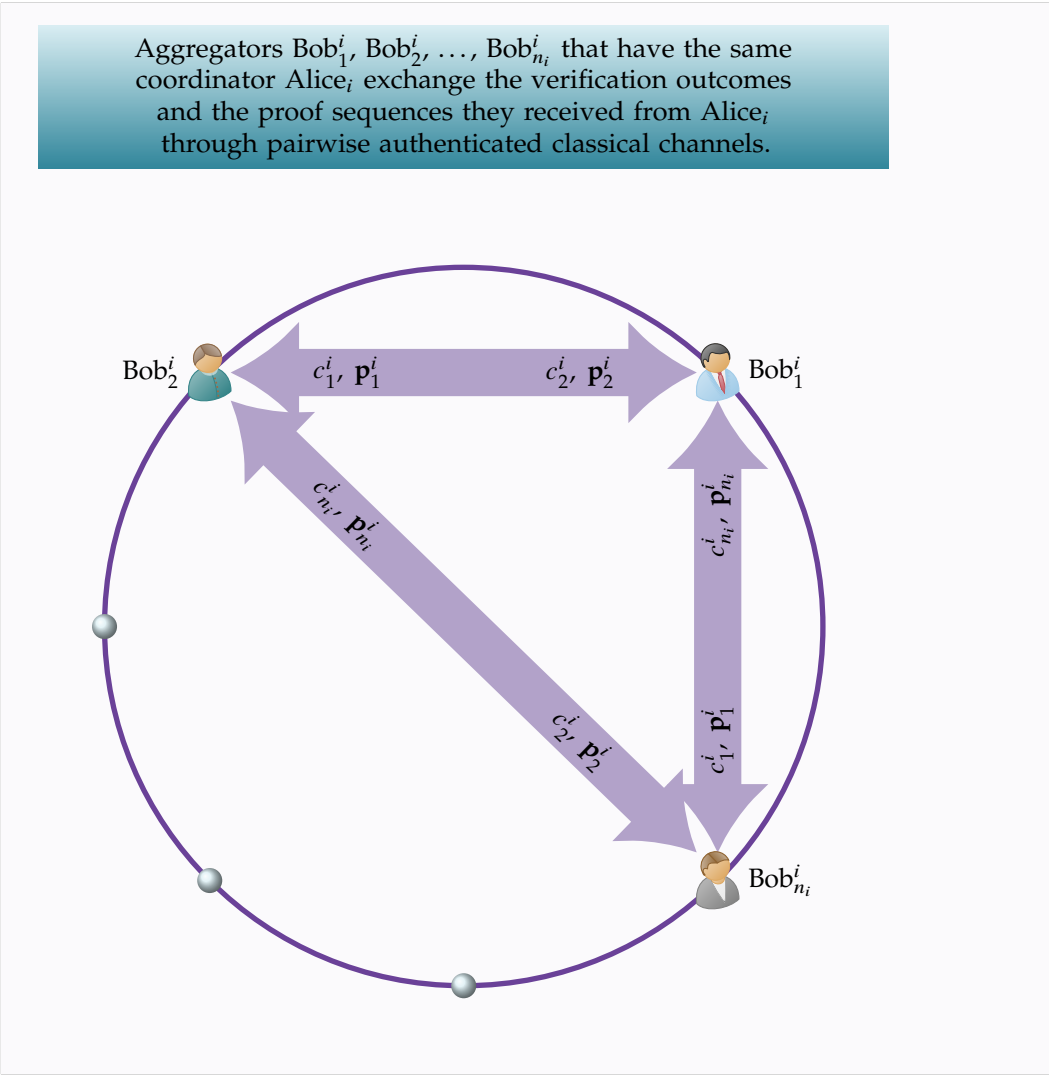

Figure 2. The above figure illustrates the fact that all news aggregators with the same coordinator Alice_i, i.e., $\text{Bob}_1^i, \text{Bob}_2^i, \ldots, \text{Bob}_{n_i}^i$, can exchange the verification outcomes and the proof sequences they received from Alice_i through pairwise authenticated classical channels.

($\mathbf{H}_7$) Every news aggregator is responsible for maintaining the reputation system outlined below, independently, and in parallel with every other news aggregator:

- ◇ A news ranking system that characterizes news as either true or fake.
- ◇ A reputation catalog that reflects the personal assessment of the aggregator regarding every other player (both verifier and aggregator) involved in information exchange.

News deemed as fake must be appropriately flagged as such, so that the public is made aware of this. The reputation catalog takes the form of two lists containing the unreliable verifiers and aggregators.

The intuition behind the latter hypothesis is quite straightforward. It is expedient to record and consider unreliable those players that have exhibited contradictory and/or malicious behavior, and distinguish them from those players that have demonstrated consistent adherence to the rules and have a history of accurate and truthful reporting. By maintaining these records, each aggregator plays an important role in ensuring the integrity and efficiency of the news network. By identifying and isolating unreliable entities, he helps to protect the network from malicious actors and maintain the trust among participants.

4. The Quantum News Verification Algorithm

In this section, we present the quantum news verification algorithm, or QNVA for short. Every Alice is tasked with verifying important news and sending the result of her verification check to all her agents:

- ◇ If the news in question passed the verification check, then Alice sends via the classical channel the bit 1 to every Bob in her active network to signify its credibility. Additionally, she sends a personalized proof, which is a sequence of bits, to each of her agents. The important thing here is that for each Bob, the proof is different because it is constructed specifically for him.
- ◇ Symmetrically, if the news failed to pass the check, Alice sends via the classical channel the bit 0 to every agent in her active network to indicate that it is fake, together with a personalized proof.

The QNVA is presented from the point of view of the individual Bob, where, of course, we assume that all Bobs implement the same algorithm consistently. The algorithm itself can be conceptually organized into three distinct phases.

4.1. The Entanglement Distribution Phase

The first is the entanglement distribution phase, which refers to the generation and distribution of entangled $|\Phi^+\rangle$ pairs and qubits in the $|+\rangle$ state. As we have explained in hypothesis 1 ($\mathbf{H}_1$), we assume the existence of a trusted quantum source that undertakes this task. In view of the capabilities of modern quantum apparatus, the trusted quantum source should have no difficulty in accomplishing this task. In terms of notation, we use the small Latin letters q and r, with appropriate subscripts and superscripts, to designate the first and the second qubits, respectively, of the same $|\Phi^+\rangle$ pair.

Definition 1 (Entanglement Distribution Scheme)**.** *The trusted source creates two types of sequences, one that is intended for verifiers and one that is intended for aggregators. Both are distributed through quantum channels to their intended recipients. Specifically, for each piece of news that must be checked, and for each Alice$_i$, $1 \leq i \leq m$, the source creates*

- ◇ *one* verification *sequence* $\mathbf{q}^i$ *that is sent to Alice$_i$ and has the form*

$$\mathbf{q}^i = \underbrace{q^i_{n_i,d} \ldots q^i_{k,d} \ldots q^i_{1,d}}_{\text{tuple } d} \cdots \underbrace{q^i_{n_i,2} \ldots q^i_{k,2} \ldots q^i_{1,2}}_{\text{tuple } 2} \underbrace{q^i_{n_i,1} \ldots q^i_{k,1} \ldots q^i_{1,1}}_{\text{tuple } 1}, \text{ and} \quad (7)$$

- ◇ n_i verification *sequences* $\mathbf{r}^i_1, \mathbf{r}^i_2, \ldots, \mathbf{r}^i_{n_i}$ *sent to* $Bob^i_1, Bob^i_2, \ldots, Bob^i_{n_i}$, *respectively, that have the form*

$$\mathbf{r}^i_k = \underbrace{|+\rangle \ldots r^i_{k,d} \ldots |+\rangle}_{\text{tuple } d} \cdots \underbrace{|+\rangle \ldots r^i_{k,2} \ldots |+\rangle}_{\text{tuple } 2} \underbrace{|+\rangle \ldots r^i_{k,1} \ldots |+\rangle}_{\text{tuple } 1}, \; 1 \leq k \leq n_i \,. \quad (8)$$

In the $\mathbf{q}^i$ *and* $\mathbf{r}^i_1, \mathbf{r}^i_2, \ldots, \mathbf{r}^i_{n_i}$ *sequences, the subscript d is a positive integer called the* degree of accuracy *of the verification. Furthermore, according to our convention, $q^i_{k,l}$ and $r^i_{k,l}$ denote the first and second qubits of the same $|\Phi^+\rangle$ pair that is used in the formation of the l^{th} tuple. Obviously, $|+\rangle$ designates qubits that are in the $|+\rangle$ state.*

The situation regarding the sequences of qubits distributed to Alice$_i$ and the Bobs in her active network are visualized in Figure 3.

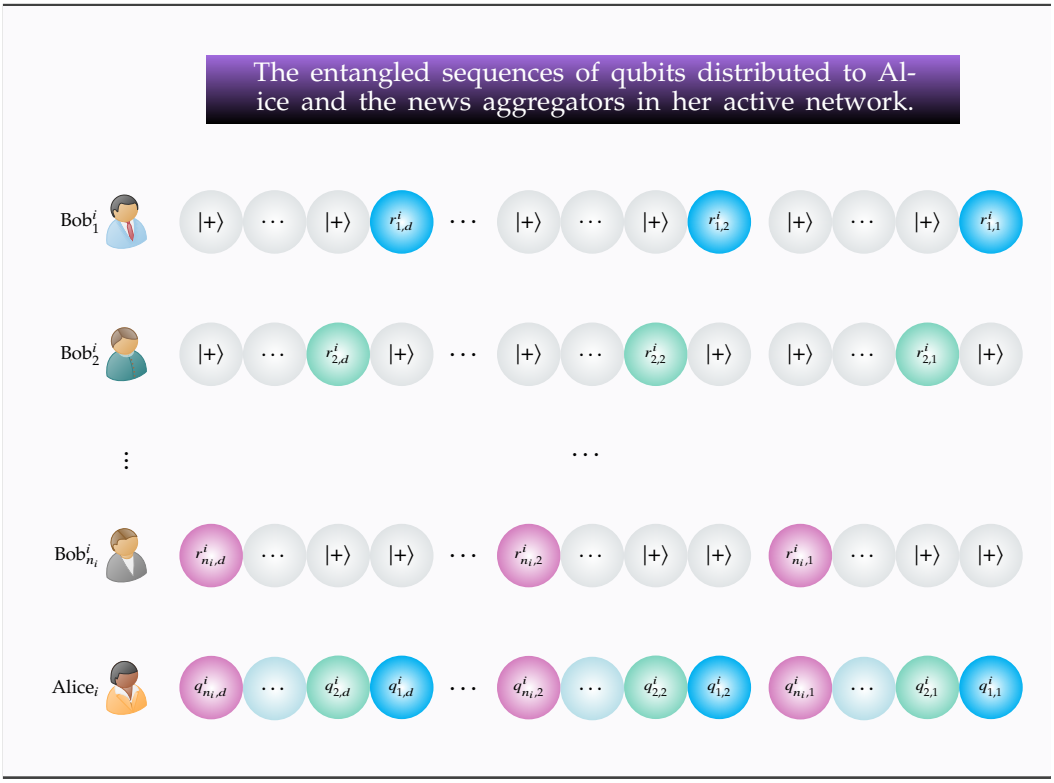

Figure 3. This figure visualizes the entangled sequences of qubits that are distributed to Alice and the news aggregators in her active network. The convention behind this depiction is to draw qubits that belong to the same $|\Phi^+\rangle$ pair using the same color. For instance, the EPR pairs shared between Alice$_i$ and Bob$_1^i$, which occupy position 1 in each n_i-tuple of the $\mathbf{q}^i$ and $\mathbf{r}_1^i$ sequences, are drawn in blue. The $|\Phi^+\rangle$ pairs shared between Alice$_i$ and Bob$_2^i$, occupying position 2 in each n_i-tuple of the $\mathbf{q}^i$ and $\mathbf{r}_2^i$ sequences, are drawn in green. Following this pattern, the EPR pairs linking Alice$_i$ and Bob$_{n_i}^i$ are shown in red. All other positions of the sequences $\mathbf{r}_1^i, \mathbf{r}_2^i, \ldots, \mathbf{r}_{n_i}^i$ contain qubits in the $|+\rangle$ state, which are drawn in silver.

In Figure 3, the adopted visual convention is to draw qubits that belong to the same $|\Phi^+\rangle$ pair with the same color. To this end, the EPR pairs shared between Alice$_i$ and Bob$_1^i$, which occupy position 1 in each n_i-tuple of the $\mathbf{q}^i$ and $\mathbf{r}_1^i$ sequences, are drawn in blue. Similarly, the $|\Phi^+\rangle$ pairs shared between Alice$_i$ and Bob$_2^i$, located in the second position of each n_i-tuple of the $\mathbf{q}^i$ and $\mathbf{r}_2^i$ sequences, are shown in green. In the same manner, red signifies the EPR pairs linking Alice$_i$ and Bob$_{n_i}^i$ occupying the last position of every n_i-tuple of the $\mathbf{q}^i$ and $\mathbf{r}_{n_i}^i$ sequences. The silver qubits designate qubits in the $|+\rangle$ state that fill the remaining positions of the sequences $\mathbf{r}_1^i, \mathbf{r}_2^i, \ldots, \mathbf{r}_{n_i}^i$. The intuition behind the construction of the above quantum sequences is outlined below:

- **($\mathbf{I}_1$)** Alice$_i$, $1 \leq i \leq m$, is linked to each one of her agents Bob$_1^i$, Bob$_2^i$, …, Bob$_{n_i}^i$ because her verification sequence $\mathbf{q}^i$ is entangled with their verification sequences $\mathbf{r}_1^i, \mathbf{r}_2^i, \ldots, \mathbf{r}_{n_i}^i$.
- **($\mathbf{I}_2$)** All these quantum sequences are made up of d in total n_i-tuples of qubits.
- **($\mathbf{I}_3$)** Sequence $\mathbf{q}^i$ is made up exclusively from entangled qubits.
- **($\mathbf{I}_4$)** In $\mathbf{q}^i$, the qubits in position 1, namely $q_{1,1}^i, q_{1,2}^i, \ldots, q_{1,d}^i$, are entangled with the corresponding qubits $r_{1,1}^i, r_{1,2}^i, \ldots, r_{1,d}^i$ of the sequence $\mathbf{r}_1^i$ that belongs to Bob$_1^i$. This is because $q_{1,l}^i$ and $r_{1,l}^i$, $1 \leq l \leq d$, belong to the same $|\Phi^+\rangle$ pair by construction.
- **($\mathbf{I}_5$)** For precisely the same reason, the qubits in position k, $k = 2, \ldots, n_i$, i.e., $q_{k,1}^i$, $q_{k,2}^i, \ldots, q_{k,d}^i$, are entangled with the corresponding qubits $r_{k,1}^i, r_{k,2}^i, \ldots, r_{k,d}^i$ of the sequence $\mathbf{r}_k^i$ owned by Bob$_k^i$.

($\mathbf{I}_6$) In every sequence $\mathbf{r}_k^i$, $k = 1, \ldots, n_i$, the qubits $r_{k,l}^i$, $l = 1, \ldots, d$, that occupy the k^{th} position in each n_i-tuple, are entangled with the corresponding qubits $q_{k,l}^i$ of $\mathbf{q}^i$. All other qubits are in the $|+\rangle$ state.

In Section 5, where we discuss the effect of the degree of accuracy of the QNVA, we shall suggest appropriate values for d.

In view of the structural form of the sequences defined by Formulae (7) and (8), we also refer to them as (d, n_i) quantum sequences because they are constructed by d repetitions of structurally similar tuples of the same length, namely n_i. These d tuples are enumerated as shown in (7) and (8), that is, tuple 1 is the rightmost tuple and tuple d is the leftmost tuple.

4.2. Entanglement Validation Phase

Undoubtedly, this is a most crucial phase, as the entire algorithm hinges upon the existence of entanglement. Without guaranteed entanglement, the algorithm's functionality is compromised. The validation procedure can result into two distinct outcomes. If entanglement is successfully ascertained, the QNVA can proceed to confidently verify the information at hand. Failure to validate entanglement indicates the absence of the necessary entanglement. This could stem from either noisy quantum channels or malicious interference from an adversary. Regardless of the cause, the only viable solution is to halt the ongoing algorithm execution and commence the entire procedure anew, after implementing corrective measures.

Given its utmost significance, this phase has undergone thorough scrutiny in the existing literature. Our algorithm adheres to the sophisticated methodologies outlined in prior works, including [42–47]. Hence, to preclude redundant exposition, we direct the reader to the previously mentioned bibliography for all the details essential for the successful implementation of this phase.

4.3. The News Verification Phase

Our algorithm classifies news as true or fake during the third and last phase, aptly named news verification phase. To initiate this phase, Alice$_i$ and the agents in her active network, Bob$_1^i$, Bob$_2^i$, …, Bob$_{n_i}^i$, measure their quantum sequences to obtain the classical bit sequences denoted by the lowercase bold letters $\mathbf{a}^i$ and $\mathbf{b}_1^i$, $\mathbf{b}_2^i$, …, $\mathbf{b}_{n_i}^i$, respectively. Taking into account the entanglement distribution scheme of Definition 1, we see that the measurement reveals some important correlations among these sequences. These correlations are depicted in Figure 4 below.

Definition 2 (Classical Bit Sequences)**.** *Upon measuring their qubit sequences, news verifier Alice$_i$ and news aggregators Bob$_1^i$, Bob$_2^i$, …, Bob$_{n_i}^i$, obtain the classical bit sequences $\mathbf{a}^i$ and $\mathbf{b}_1^i$, $\mathbf{b}_2^i$, …, $\mathbf{b}_{n_i}^i$, respectively, that can be written explicitly as follows:*

$$\mathbf{a}^i = \underbrace{a_{n_i,d}^i \ldots a_{k,d}^i \ldots a_{1,d}^i}_{\text{tuple } d} \cdots \underbrace{a_{n_i,2}^i \ldots a_{k,2}^i \ldots a_{1,2}^i}_{\text{tuple } 2} \underbrace{a_{n_i,1}^i \ldots a_{k,1}^i \ldots a_{1,1}^i}_{\text{tuple } 1}, \text{ and} \tag{9}$$

$$\mathbf{b}_k^i = \underbrace{b_{n_i,d}^i \ldots b_{k,d}^i \ldots b_{1,d}^i}_{\text{tuple } d} \cdots \underbrace{b_{n_i,2}^i \ldots b_{k,2}^i \ldots b_{1,2}^i}_{\text{tuple } 2} \underbrace{b_{n_i,1}^i \ldots b_{k,1}^i \ldots b_{1,1}^i}_{\text{tuple } 1}, \tag{10}$$

where $k = 1, \ldots, n_i$.

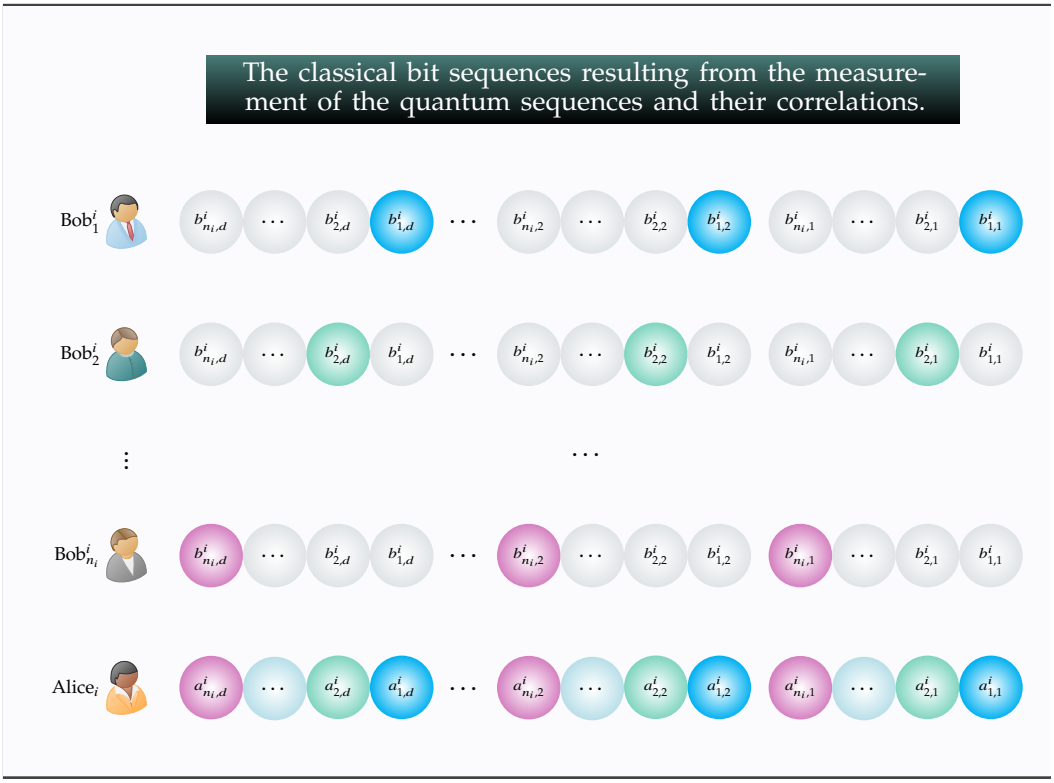

Figure 4. This figure shows the classical bit sequences that result after Alice and the news aggregators measure their quantum sequences. The correlations among pairs of bits in these sequences are visualized by drawing correlated pairs with the same color.

Although the sequences defined by Formulae (9) and (10) consist of classical bits, their structural form is identical to that of the original qubit sequences. So, we will also refer to them as (d, n_i) classical sequences because they are constructed by repeating d times structurally similar tuples of length n_i. Following this line of thought, we may consider an arbitrary (d, n_i) sequence $\mathbf{s}$ made of symbols from some fixed alphabet, and express it in an alternative but equivalent way, emphasizing its composition in terms of n_i-tuples, as follows.

$$\mathbf{s} = \underbrace{s_{n_i,d} \ldots s_{2,d} s_{1,d}}_{\text{tuple } d} \cdots \underbrace{s_{n_i,2} \ldots s_{2,2} s_{1,2}}_{\text{tuple 2}} \underbrace{s_{n_i,1} \ldots s_{2,1} s_{1,1}}_{\text{tuple 1}}$$
$$\mathbf{s} = \mathbf{s}_d \cdots \mathbf{s}_2 \mathbf{s}_1 . \tag{11}$$

Let us also clarify that by writing $\mathbf{s} = \mathbf{s}_d \cdots \mathbf{s}_2 \mathbf{s}_1$, where $\mathbf{s}_l = s_{n_i,l} \ldots s_{2,l} s_{1,l}$ and $1 \leq l \leq d$, we have effectively enumerated the d tuples of $\mathbf{s}$ in a way that 1 is the rightmost and d is the leftmost tuple. In the rest of our exposition, we will also need a special n_i-tuple that is constructed by using a new symbol $*$, different from 0 and 1. This is denoted by $\mathbf{s}_*$ and is referred to as the cryptic tuple.

$$\mathbf{s}_* = \underbrace{* \ldots * *}_{n_i \text{ occurrences}} . \tag{12}$$

With the above convention, we may write Alice$_i$'s bit sequence $\mathbf{a}^i$ in the next form, emphasizing the fact that it is composed of d tuples.

$$\mathbf{a}^i = \mathbf{a}_d \cdots \mathbf{a}_2 \mathbf{a}_1 \tag{13}$$

Definition 3 (Proof Sequences). *News verifier Alice$_i$, $1 \le i \le m$, sends two things to all the news aggregators in her active network Bob$^i_1$, Bob$^i_2$, ..., Bob$^i_{n_i}$:*

◇ *The result of the verification check, denoted by $c^i_k \in \mathbb{B}$, which is just a single bit. If the news is true, then c^i_k is just the bit 1, whereas if the news is fake, c^i_k is the bit 0.*

◇ *A* proof sequence, *denoted by $\mathbf{p}^i_k$, which is intended to convince Bob^i_k that she is honest. Each proof sequence $\mathbf{p}^i_k$ is a (d, n_i) sequence of symbols from $\mathbb{B} \cup \{*\}$, i.e., $\mathbf{p}^i_k = \mathbf{p}_d \ \ldots \ \mathbf{p}_2 \ \mathbf{p}_1$. It is critical that these proof sequences be personalized, which effectively means they must be different for every news aggregator. Their construction is described below.*

– *If $c^i_k = 1$, the proof $\mathbf{p}^i_k$ sequence sent to news aggregator Bob^i_k, $1 \le k \le n_i$, also designated by $\mathbb{1}^i_k$ for emphasis, has the explicit form shown below:*

$$\mathbb{1}^i_k = \mathbf{p}_d \ \ldots \ \mathbf{p}_2 \ \mathbf{p}_1 \ , \ \text{where} \ \ \mathbf{p}_l = \begin{cases} \mathbf{a}_l & \text{if } a^i_{k,l} = 1 \\ \mathbf{s}_* & \text{if } a^i_{k,l} = 0 \end{cases} , \ 1 \le l \le d \ . \tag{14}$$

– *Symmetrically, if $c^i_k = 0$, the proof sequence sent to Bob^i_k, $1 \le k \le n_i$, denoted by $\mathbb{0}^i_k$ for emphasis, has the following explicit form:*

$$\mathbb{0}^i_k = \mathbf{p}_d \ \ldots \ \mathbf{p}_2 \ \mathbf{p}_1 \ , \ \text{where} \ \ \mathbf{p}_l = \begin{cases} \mathbf{a}_l & \text{if } a^i_{k,l} = 0 \\ \mathbf{s}_* & \text{if } a^i_{k,l} = 1 \end{cases} , \ 1 \le l \le d \ . \tag{15}$$

A proof sequence for a verification check c^i_k that is faithfully constructed according to Definition 3 is said to be *consistent* with c^i_k. The previous Definition 3 guarantees that, no matter what the verification outcome is, Bob^i_k receives a different proof sequence from every other Bob$^i_{k'}$ when $k' \ne k$. The other crucial property that characterizes the proof sequences is that, besides the fact that tuples entirely comprise 0 and 1 bits, they also contain a statistically equal number of cryptic tuples consisting of the special symbol $*$. Probabilistic analysis allows Bob^i_k to assess whether or not Alice$_i$ and the other Bobs act honestly and consistently. To this end, it is necessary to examine the positions of the n_i-tuples that contain specific combinations of bits.

Definition 4. *Let* $\mathbf{s} = \underbrace{s_{n_i,d} \ldots s_{2,d} s_{1,d}}_{\text{tuple } d} \cdots \underbrace{s_{n_i,2} \ldots s_{2,2} s_{1,2}}_{\text{tuple } 2} \underbrace{s_{n_i,1} \ldots s_{2,1} s_{1,1}}_{\text{tuple } 1}$ *be a (d, n_i) sequence. If k and k', $1 \le k \ne k' \le n_i$, are two given indices, and $x, y \in \mathbb{B}$, we define the following sets:*

$$P_x(\mathbf{s}, k) = \{l \mid s_{k,l} = x\} \ , \tag{16}$$

$$P_{x,y}(\mathbf{s}, k, k') = \{l \mid s_{k,l} = x \wedge s_{k',l} = y\} \ , \ \text{and} \tag{17}$$

$$P_*(\mathbf{s}) = \{l \mid \mathbf{s}_l = \mathbf{s}_*\} \ . \tag{18}$$

The previous definition completes the necessary machinery and notation for the presentation of the QNVA. We shall now proceed to explain the QNVA in detail and, at the same time, prove its correctness. In the rest of this section, we present the algorithm from the point of view of the typical news aggregator Bob^i_k, $1 \le k \le n_i$. In what follows, we use the notation $|S|$ to designate the number of elements of a given set S.

In today's complex news environment, malicious intent can manifest in many subtle ways. One may easily envision the next most critical scenarios:

($\mathbf{S}_1$) An unreliable and dishonest Alice$_i$ sends to Bob^i_k the verification outcome c^i_k, but the latter is accompanied with the wrong proof sequence $\mathbf{p}^i_k$.

($\mathbf{S}_2$) A malicious news aggregator, say Bob$^i_{k'}$, ($k' \ne k$), falsely claims that he received from Alice$_i$ the opposite verification outcome accompanied by a consistent proof sequence.

($\mathbf{S}_3$) An insidious Alice$_i$ deliberately spreads disinformation and confusion by sending opposite verification outcomes c_k^i and $\overline{c_k^i}$ to Bob$_k^i$ and Bob$_{k'}^i$ ($k' \neq k$), using consistent proof sequences $\mathbf{p}_k^i$ and $\mathbf{p}_{k'}^i$ in each case.

The first scenario ($\mathbf{S}_1$) can be easily detected and countered by the QNVA. The second scenario ($\mathbf{S}_2$) can be addressed with some additional effort. Our algorithm can also deal with the third scenario ($\mathbf{S}_3$), which reveals the existence of a truly malicious Alice, with some additional inference on the part of Bob. QNVA owes its ability to cope with each one of the above scenarios to the structural properties of the proof sequences. These properties are a direct result of the entanglement distribution scheme explained in Definition 1. The next Proposition 1 lays the groundwork for the subsequent analysis of our verification procedures.

Proposition 1 (Dishonest news verifier detection)**.** *Let us assume that news aggregator Bob$_k^i$, $1 \leq k \leq n_i$, has received from his coordinator Alice$_i$, $1 \leq i \leq m$, the verification outcome $c_k^i \in \mathbb{B}$, and the proof sequence $\mathbf{p}_k^i$. If the proof sequence $\mathbf{p}_k^i$ is consistent with c_k^i, then it must satisfy the following properties:*

$$\mathbb{E}\Big[\ |\ P_{c_k^i}(\mathbf{p}_k^i, k)\ |\ \Big] = \mathbb{E}\Big[\ |\ P_*(\mathbf{p}_k^i)\ |\ \Big] = \frac{d}{2}\ ,\ \textit{and} \tag{19}$$

$$\mathbb{E}\Big[\ |\ P_{c_k^i, c_k^i}(\mathbf{p}_k^i, k, k')\ |\ \Big] = \mathbb{E}\Big[\ |\ P_{c_k^i, \overline{c_k^i}}(\mathbf{p}_k^i, k, k')\ |\ \Big] = \frac{d}{4}\ ,\ \forall k'\ ,\ 1 \leq k' \neq k \leq n_i\ . \tag{20}$$

Proof. The proof is quite straightforward because it is based on the entanglement distribution scheme of Definition 1. The entanglement distribution scheme stipulates that each n_i-tuple in the original qubit sequence of Alice$_i$ shares one $|\Phi^+\rangle = \frac{|0\rangle_A|0\rangle_k + |1\rangle_A|1\rangle_k}{\sqrt{2}}$ pair with every Bob$_k^i$, $k = 1, \ldots, n_i$. Therefore, there are d in total bits $a_{k,l}^i$ that occupy the k^{th} position in every tuple l of $\mathbf{a}^i$, $1 \leq l \leq d$, which are equal to the corresponding bits $b_{k,l}^i$ of $\mathbf{b}_k^i$. This is captured by the next formula:

$$a_{k,l}^i = b_{k,l}^i\ ,\ 1 \leq l \leq d\ . \tag{21}$$

The remaining bits of $\mathbf{b}_k^i$ result from measuring qubits in the $|+\rangle$ state. Hence, we expect half of them to end up as 0, and the remaining half to end up as 1. More importantly though, these bits are not correlated with the corresponding bits of $\mathbf{a}^i$. Consequently, we can easily draw the following conclusions:

- Measuring a pair of qubits in the $|\Phi^+\rangle$ state will result in both qubits collapsing in state $|0\rangle$ with probability 0.5, or in state $|1\rangle$ with probability 0.5. This implies that the expected number of the $a_{k,l}^i$ and $b_{k,l}^i$ bits with value 1(0) is $\frac{d}{2}$. Consequently, the expected number of tuples in $\mathbf{a}^i$ (and in $\mathbf{b}_k^i$) in which the bit in the k^{th} position has value 1(0) is $\frac{d}{2}$. Thus, irrespective of whether the verification outcome c_k^i is 1 or 0, the expected number of tuples in $\mathbf{p}_k^i$ in which the bit in the k^{th} position has value c_k^i is $\frac{d}{2}$, which proves property (19). This also means that the expected number of the remaining tuples in $\mathbf{p}_k^i$, which are cryptic tuples according to Definition 3, is also $\frac{d}{2}$.
- Measuring two pairs of qubits, both in the $|\Phi^+\rangle$ state, will result in both qubits of the first pair collapsing in state $|0\rangle$ with probability 0.5, or in state $|1\rangle$ with probability 0.5, and, independently, both qubits of the second pair collapsing in state $|0\rangle$ with probability 0.5, or in state $|1\rangle$ with probability 0.5. This means that the expected number of the $a_{k,l}^i$ and $a_{k',l}^i$ bits with values "00", "01", "10", and "11" is $\frac{d}{4}$. Consequently, the expected number of tuples in $\mathbf{a}^i$ in which the bits in positions k and k' contain any one of the aforementioned combinations is $\frac{d}{4}$. Thus, irrespective of whether the verification outcome c_k^i is 1 or 0, the expected number of tuples in $\mathbf{p}_k^i$ in which the bits in positions k and k' are $c_k^i c_k^i$ or $c_k^i \overline{c_k^i}$ is $\frac{d}{4}$, which proves property (20).

This completes the proof of this proposition. □

The properties outlined in Proposition 1 are instrumental in the design of the verification tests that are used as subroutines for the QNVA. These tests, which are performed by every news aggregator Bob_k^i, $1 \le k \le n_i$, in order to assess whether or not the coordinator Alice_i and the other news aggregators are honest, are based on the verification outcome c_k^i and the proof sequence $\mathbf{p}_k^i$ that Bob_k^i has received from Alice_i.

As we have emphasized, our algorithm can handle all three scenarios mentioned above. For the first scenario ($\mathbf{S}_1$), the verification test IsAlice'sProofConsistent contained in Figure 5 can decide whether or not $\mathbf{p}_k^i$ is consistent with c_k^i by checking if it satisfies Proposition 1. It relies on the auxiliary test IsProofBalanced, also shown below in Figure 6. It is essential to point out that in a real implementation of these tests one must take into account the possible imperfections of the quantum channel, and the probabilistic outcome of the measurements. That means that the stringent equality requirement of the expected values as expressed in the propositions should be relaxed and one should instead check for approximate equality $\approx$ or approximate inequality $\not\approx$. In the presentation of the pseudocode, we adopt the following conventions:

- i, $1 \le i \le m$, is the index of Alice_i;
- k, $1 \le k \le n_i$, is the index of Bob_k^i;
- c_k^i is the verification outcome that Alice_i sends to Bob_k^i;
- $\mathbf{p}_k^i$ is the proof sequence that Alice_i sends to Bob_k^i;
- $\mathbf{b}_k^i$ is the classical bit sequence of Bob_k^i.

Verification Test 1: IsAlice'sProofConsistent$(i, k, c_k^i, \mathbf{p}_k^i, \mathbf{b}_k^i)$

```
N = | P_{c_k^i}(p_k^i, k) |
if N ≠ d/2 then
    return FALSE
foreach l ∈ P_{c_k^i}(p_k^i, k) do
    if (p_{k,l}^i ≠ b_{k,l}^i) then
        return FALSE
return IsProofBalanced(i, k, c_k^i, p_k^i)
```

Figure 5. Bob_k^i uses the above algorithm to check if the proof sequence $\mathbf{p}_k^i$ is consistent with the verification outcome c_k^i.

Auxiliary Test: IsProofBalanced$(i, k, c_k^i, \mathbf{p}_k^i)$

```
for r(≠ k) = 1 to n_i do
    N_1 = | P_{c_k^i, c_k^i}(p_k^i, k, r) |
    N_2 = | P_{c_k^i, ¬c_k^i}(p_k^i, k, r) |
    if (N_1 ≠ d/4 OR N_2 ≠ d/4) then
        return FALSE
return TRUE
```

Figure 6. This auxiliary algorithm is invoked by Bob_k^i to ascertain whether property (20) of Proposition 1 holds.

To cope with the second scenario ($\mathbf{S}_2$), the verification test IsBob'sProofConsistent contained in Figure 7 can decide whether or not $\mathbf{p}_k^i$ is consistent with c_k^i by virtue of the results proven in the next proposition.

Verification Test 3: IsBob'sProofConsistent$(i, k, k', c^i_k, \mathbf{p}^i_k, \overline{c^i_k}, \mathbf{p}^i_{k'})$

$N = |\, P_{\overline{c^i_k}}(\mathbf{p}^i_{k'}, k') \,|$
if $N \neq \frac{d}{2}$ **then**
  return FALSE
if $P_{c^i_k, \overline{c^i_k}}(\mathbf{p}^i_k, k, k') \neq P_{c^i_k, \overline{c^i_k}}(\mathbf{p}^i_{k'}, k, k')$ **then**
  return FALSE
return IsProofBalanced$(i, k', \overline{c^i_k}, \mathbf{p}^i_{k'})$

Figure 7. Bob^i_k uses the above algorithm to check if $\mathbf{p}^i_{k'}$ is consistent with $\overline{c^i_k}$ that $\text{Bob}^i_{k'}$ claims to have received from Alice_i.

Proposition 2. *Suppose that* Bob^i_k, $1 \leq k \leq n_i$, *has received from* $Alice_i$, $1 \leq i \leq m$, *the verification outcome* $c^i_k = 1$ ($c^i_k = 0$), *and the consistent proof sequence* $\mathbb{1}^i_k$ ($\mathbb{0}^i_k$).

Let us further assume that Bob^i_k *has also received from* $Bob^i_{k'}$, $(k' \neq k)$ *the opposite verification outcome* $c^i_{k'} = 0$ ($c^i_{k'} = 1$) *and the sequence* $\mathbb{0}^i_{k'}$, ($\mathbb{1}^i_{k'}$) *as proof. If* $\mathbb{0}^i_{k'}$, ($\mathbb{1}^i_{k'}$) *is consistent with* 0 (1), *then, in addition to the properties listed in Proposition 1, it must also satisfy the following relation:*

$$\left\{ \begin{array}{l} P_{1,0}(\mathbb{1}^i_k, k, k') = P_{1,0}(\mathbb{0}^i_{k'}, k, k') \\ \\ P_{0,1}(\mathbb{0}^i_k, k, k') = P_{0,1}(\mathbb{1}^i_{k'}, k, k') \end{array} \right\} \tag{22}$$

Proof. Without loss of generality we imagine a situation that has evolved as follows:

- Initially, Bob^i_k received from Alice_i the verification outcome $c^i_k = 1$ and the consistent proof sequence $\mathbb{1}^i_k$;
- Subsequently, Bob^i_k received from $\text{Bob}^i_{k'}$ the opposite verification outcome $c^i_{k'} = 0$ and the sequence $\mathbb{0}^i_{k'}$ as proof.

We shall prove that if $\mathbb{0}^i_{k'}$ is consistent with the outcome 0, then, in addition to the properties listed in Proposition 1, relation (22) must also hold.

The proof is an immediate consequence of the manner in which proof sequences are constructed. If we recall Definition 3, we see that the proof sequence $\mathbb{1}^i_k$ ($\mathbb{0}^i_k$), which is consistent with the verification outcome $c^i_k = 1$ ($c^i_k = 0$), contains all the n_i-tuples of Alice_i's bit sequence $\mathbf{a}^i$ in which the bit in the k^{th} position has value 1 (0), including all those in which the bit in position k' has the value 1, and all those in which the bit in position k' has the value 0.

$$\mathbf{a}^i = \underbrace{a^i_{n_i,d} \ldots a^i_{k,d} \ldots a^i_{1,d}}_{\text{tuple } d} \cdots \underbrace{a^i_{n_i,2} \ldots a^i_{k,2} \ldots a^i_{1,2}}_{\text{tuple 2}} \underbrace{a^i_{n_i,1} \ldots a^i_{k,1} \ldots a^i_{1,1}}_{\text{tuple 1}}, \text{ and} \tag{23}$$

$$\mathbf{b}^i_k = \underbrace{b^i_{n_i,d} \ldots b^i_{k,d} \ldots b^i_{1,d}}_{\text{tuple } d} \cdots \underbrace{b^i_{n_i,2} \ldots b^i_{k,2} \ldots b^i_{1,2}}_{\text{tuple 2}} \underbrace{b^i_{n_i,1} \ldots b^i_{k,1} \ldots b^i_{1,1}}_{\text{tuple 1}}, \tag{24}$$

Symmetrically, if the proof sequence $\mathbb{0}^i_{k'}$, ($\mathbb{1}^i_{k'}$) is consistent with the opposite verification outcome $c^i_{k'} = 0$ ($c^i_{k'} = 1$), then it must contain all the n_i-tuples of $\mathbf{a}^i$ in which the bit in position k' has value 0 (1), including all those in which the bit in position k has the value 0, and all those in which the bit in position k has the opposite value 1.

Therefore, if both proof sequences $\mathbb{1}^i_k$ and $\mathbb{0}^i_{k'}$ ($\mathbb{0}^i_k$ and $\mathbb{1}^i_{k'}$) are consistent with the verification checks $c^i_k = 1$ and $c^i_{k'} = 0$ ($c^i_k = 0$ and $c^i_{k'} = 1$), respectively, then they must

contain all the n_i-tuples of $\mathbf{a}^i$ in which the bit in the k^{th} position has the value 1 (0) and the bit in position k' has the opposite value 0 (1). Formally, we can express this fact as

$$\left\{ \begin{array}{l} P_{1,0}(\mathbb{1}^i_k, k, k') = P_{1,0}(\mathbb{0}^i_{k'}, k, k') \\ \\ P_{0,1}(\mathbb{0}^i_k, k, k') = P_{0,1}(\mathbb{1}^i_{k'}, k, k') \end{array} \right\}, \tag{25}$$

which concludes this proof. The opposite case is completely symmetrical and is omitted. □

The previous proposition can be cast into its most general form as the following Corollary.

Corollary 1. *Let us assume that* Bob^i_k, $1 \leq k \leq n_i$, *has received the following:*

- ◇ *From* $Alice_i$, $1 \leq i \leq m$, *the verification outcome* c^i_k *and the sequence* $\mathbf{p}^i_k$ *as proof;*
- ◇ *From* $Bob^i_{k'}$, $(k' \neq k)$ *the opposite verification outcome* $c^i_{k'} = \overline{c^i_k}$ *and the sequence* $\mathbf{p}^i_{k'}$ *as proof.*

Then, if both $\mathbf{p}^i_{k'}$ *and* $\mathbf{p}^i_{k'}$ *are consistent with* c^i_k *and* $\overline{c^i_k}$, *respectively, they must also satisfy the following property:*

$$P_{c^i_k, \overline{c^i_k}}(\mathbf{p}^i_k, k, k') = P_{c^i_k, \overline{c^i_k}}(\mathbf{p}^i_{k'}, k, k') \tag{26}$$

Proof. If we recall Definition 3 again, we see that if the proof sequence $\mathbf{p}^i_k$ is consistent with c^i_k, then it contains all the n_i-tuples of $Alice_i$'s bit sequence $\mathbf{a}^i$ in which the bit in the k^{th} position has value c^i_k, including all those in which the bit in position k' has the same value c^i_k, and all those in which the bit in position k' has the opposite value $\overline{c^i_k}$. Symmetrically, if the proof sequence $\mathbf{p}^i_{k'}$ is consistent with $\overline{c^i_k}$, then it contains all the n_i-tuples of $\mathbf{a}^i$ in which the bit in position k' has value $\overline{c^i_k}$, including all those in which the bit in position k has the same value $\overline{c^i_k}$, and all those in which the bit in position k has the opposite value c^i_k. Therefore, if they are both consistent, proof sequences $\mathbf{p}^i_k$ and $\mathbf{p}^i_{k'}$ contain all the n_i-tuples of $\mathbf{a}^i$ in which the bit in the k^{th} position has value c^i_k and the bit in position k' has the opposite value $\overline{c^i_k}$. This is simply written as

$$P_{c^i_k, \overline{c^i_k}}(\mathbf{p}^i_k, k, k') = P_{c^i_k, \overline{c^i_k}}(\mathbf{p}^i_{k'}, k, k') \ , \tag{27}$$

which completes the proof of this corollary. □

To sum up, the property expressed by relation (26) asserts that if two proof sequences $\mathbf{p}^i_k$ and $\mathbf{p}^i_{k'}$ corresponding to opposite outcomes c^i_k and $\overline{c^i_k}$ are both consistent, then they must contain precisely the same tuples of $\mathbf{a}^i$ in which the bit in the k^{th} position is c^i_k and the bit in position k' is $\overline{c^i_k}$. This property can be employed by Bob^i_k to detect if $Bob^i_{k'}$ deliberately spreads misinformation, as formalized by the next Theorem 1.

Theorem 1 (Malicious news aggregator detection)**.** *Suppose that* Bob^i_k, $1 \leq k \leq n_i$, *has received from* $Alice_i$, $1 \leq i \leq m$, *the verification outcome* c^i_k, *and the consistent proof sequence* $\mathbf{p}^i_k$.

Any attempt by another news aggregator $Bob^i_{k'}$, $(k' \neq k)$ *to falsely claim that he received* $\overline{c^i_k}$ *from* $Alice_i$, *despite the fact that in reality he received* c^i_k, *and forge a proof sequence* $\mathbf{p}^i_{k'}$, *consistent with* $\overline{c^i_k}$ *will be detected by* Bob^i_k.

Proof. The present situation concerns how a malicious $Bob^i_{k'}$ may try to deceive Bob^i_k $(k' \neq k)$. $Bob^i_{k'}$ has received from $Alice_i$ the verification outcome c^i_k together with a proof sequence $\mathbf{p}^i_{k'}$, consistent with c^i_k. Nevertheless, $Bob^i_{k'}$ intends to falsely claim that he has received $\overline{c^i_k}$. The question is, can $Bob^i_{k'}$ construct a convincing proof sequence $\mathbf{p}^i_{k'}$, consistent with $\overline{c^i_k}$? We proceed to show that this is probabilistically impossible.

Having received and validated $\mathbf{p}^i_k$, Bob^i_k knows the set $P_{c^i_k,\overline{c^i_k}}(\mathbf{p}^i_k, k, k')$ of the positions of all the n_i-tuples of $\mathbf{a}^i$ that contain c^i_k and $\overline{c^i_k}$ in positions k and k', respectively.

On the other hand, $\text{Bob}^i_{k'}$ has received the proof sequence $\mathbf{p}^i_{k'}$ that is also consistent with c^i_k. Accordingly, $\text{Bob}^i_{k'}$ knows the following two facts:

(**Fact**$_1$) The indices of the n_i-tuples of $\mathbf{a}^i$ that contain c^i_k in position k', which includes those that also contain c^i_k in position k, and those that also contain $\overline{c^i_k}$ in position k, i.e., the set

$$P_{c^i_k}(\mathbf{p}^i_{k'}, k') = P_{c^i_k,c^i_k}(\mathbf{p}^i_{k'}, k', k) \cup P_{c^i_k,\overline{c^i_k}}(\mathbf{p}^i_{k'}, k', k)\ . \tag{28}$$

(**Fact**$_2$) The indices of the cryptic tuples $\mathbf{s}_*$ of $\mathbf{a}^i$, i.e., the set $P_*(\mathbf{p}^i_{k'})$.

By knowing the indices of the cryptic tuples, $\text{Bob}^i_{k'}$ is able to infer with certainty, i.e., probability 1, that these indices correspond to n_i-tuples of $\mathbf{a}^i$ that contain $\overline{c^i_k}$ in position k'. In his effort to forge a proof sequence consistent with $\overline{c^i_k}$, $\text{Bob}^i_{k'}$ will correctly place all the tuples of $\mathbf{a}^i$ that contain $\overline{c^i_k}$ in position k'. According to Proposition 1, their expected number is $\frac{d}{2}$, so in reality they would be $\approx \frac{d}{2}$. So, $\text{Bob}^i_{k'}$ will avoid trivial mistakes, such as either of the following:

- Including a tuple where the bit in the k' position has the wrong value;
- Using fewer than expected tuples with $\overline{c^i_k}$ in position k'.

$\text{Bob}^i_{k'}$'s real weakness stems from the fact that the tuples he must include in his forged proof sequence may contain either c^i_k with probability 0.5, or $\overline{c^i_k}$ with equal probability 0.5 in the k^{th} position because $\text{Bob}^i_{k'}$ does not know with certainty, even for a single tuple, if it contains c^i_k or $\overline{c^i_k}$ in position k. Therefore, when forging a proof sequence consistent with $\overline{c^i_{k'}}$, $\text{Bob}^i_{k'}$ has to guess for every tuple whether to place c^i_k or $\overline{c^i_k}$ in position k. Thus, he is prone to make two types of mistakes:

(**M**$_1$) Place c^i_k in the k^{th} position of a wrong n_i-tuple not contained in $P_{c^i_k,\overline{c^i_k}}(\mathbf{p}^i_k, k, k')$.

(**M**$_2$) Place $\overline{c^i_k}$ in the k^{th} position of a wrong n_i-tuple that does appear in $P_{c^i_k,\overline{c^i_k}}(\mathbf{p}^i_k, k, k')$.

In other words, the question now becomes the following: how probable is it for $\text{Bob}^i_{k'}$ to construct a proof sequence $\mathbf{p}^i_{k'}$ so that the set $P_{c^i_k,\overline{c^i_k}}(\mathbf{p}^i_{k'}, k, k')$ is equal to the set $P_{c^i_k,\overline{c^i_k}}(\mathbf{p}^i_k, k, k')$?

The probability that $\text{Bob}^i_{k'}$ succeeds in doing so equals the probability of picking the one correct configuration out of many. The total number of configurations is equal to the number of ways to place $\approx \frac{d}{4}$ identical objects into $\approx \frac{d}{2}$ distinguishable boxes. Hence, the probability that $\text{Bob}^i_{k'}$ places *all* the $\approx \frac{d}{4}$ values c^i_k correctly in the $\approx \frac{d}{2}$ cryptic n_i-tuples is

$$P\big(\text{Bob}^i_{k'} \text{ places all } c^i_k \text{ correctly}\big) \approx \frac{1}{\binom{d/2}{d/4}}\ , \tag{29}$$

which is practically zero for appropriately chosen values of d. Thus, the end result will violate property (26) of Corollary 1.

Ergo, when Bob^i_k checks the consistency of the proof sequence sent by $\text{Bob}^i_{k'}$, he will easily detect inconsistencies and infer that $\text{Bob}^i_{k'}$ deliberately spreads disinformation. □

So, to cope with the second scenario ($\mathbf{S}_2$), one may rely on the verification test Is-Bob'sProofConsistent (shown in Figure 7), which can decide whether or not $\mathbf{p}^i_{k'}$ is consistent with $\overline{c^i_k}$ by checking if it satisfies property (26) of Corollary 1. We again note that in a real implementation of the next test we must take into account the possible imperfections of the quantum channel, and the probabilistic outcome of the measurements,

which implies that the strict inequality requirement should be relaxed and we should test for approximate inequality $\not\approx$. In the pseudocode, we use the following conventions:

- $i, 1 \leq i \leq m$, is the index of Alice$_i$;
- $k, 1 \leq k \leq n_i$, is the index of Bob^i_k;
- $k', 1 \leq k' \neq k \leq n_i$, is the index of Bob$^i_{k'}$;
- c^i_k is the verification outcome that Alice$_i$ has sent to Bob^i_k;
- $\mathbf{p}^i_k$ is the proof sequence that Alice$_i$ has sent to Bob^i_k;
- $\overline{c^i_k}$ is the verification outcome that Bob$^i_{k'}$ claims he received from Alice$_i$;
- $\mathbf{p}^i_{k'}$ is the proof sequence that Bob$^i_{k'}$ claims he received from Alice$_i$.

By combining both verification checks, it is possible to detect an insidious Alice$_i$ who deliberately spreads disinformation and confusion by sending opposite verification outcomes c^i_k and $\overline{c^i_k}$ to Bob^i_k and Bob$^i_{k'}$, $(k' \neq k)$, using the correct proof sequences $\mathbf{p}^i_k$ and $\mathbf{p}^i_{k'}$ in each case. This is analyzed in the following Theorem 2.

Theorem 2 (Malicious news verifier detection)**.** *Suppose that Bob^i_k, $1 \leq k \leq n_i$, has received from Alice$_i$, $1 \leq i \leq m$, the verification outcome c^i_k and the consistent proof sequence $\mathbf{p}^i_k$.*

Bob^i_k infers that Alice$_i$ is a malicious actor that deliberately spreads disinformation if he also receives a proof sequence $\mathbf{p}^i_{k'}$, consistent with the opposite outcome $\overline{c^i_k}$ from another news aggregator Bob$^i_{k'}$, $(k' \neq k)$.

Proof. The present situation examines how a news aggregator can uncover an insidious news verifier Alice$_i$ who deliberately spreads disinformation and confusion by sending the verification outcome c^i_k to Bob^i_k and, at the same time, sending the opposite verification outcome $\overline{c^i_k}$ to Bob$^i_{k'}$, $(k' \neq k)$, using consistent proof sequences $\mathbf{p}^i_k$ and $\mathbf{p}^i_{k'}$ in each case.

According to Theorem 1, the probability that another news aggregator Bob$^i_{k'}$, $(k' \neq k)$ will manage to construct on his own a proof sequence $\mathbf{p}^i_{k'}$, consistently is negligible. Hence, if the verification test IsBob'sProofConsistent shown in Figure 7 returns TRUE, the logical conclusion is that Alice$_i$ herself must have sent the consistent proof sequence $\mathbf{p}^i_{k'}$ to Bob$^i_{k'}$.

Thus, Alice$_i$ deliberately sends contradictory verification outcomes to create confusion and spread disinformation. □

At this point, summarizing the previous analysis, we present the proposed quantum news verification algorithm QNVA(k), listed below as Algorithm 1. For every piece of news that must be checked, the QNVA is employed by each news aggregator Bob^i_k, $1 \leq k \leq n_i$, independently and in parallel with every other news aggregator. In the presentation, we use the following notation:

- $i, 1 \leq i \leq m$, is the index of Alice$_i$.
- $k, 1 \leq k \leq n_i$, is the index of Bob^i_k.
- QNVA(k) is the instance of QVNA executed by Bob^i_k.
- M_A and M_V denote the lists of malicious news aggregators and news verifiers, respectively, as surmised by Bob^i_k. The purpose of the reputation lists is to identify insidious agents and ignore any further communication originating from them.
- $k', 1 \leq k' \neq k \leq n_i$, is the index of Bob$^i_{k'}$.
- c^i_k is the verification outcome that Alice$_i$ has sent to Bob^i_k.
- $\mathbf{p}^i_k$ is the proof sequence that Alice$_i$ has sent to Bob^i_k.
- $c^i_{k'}$ is the verification outcome that Bob$^i_{k'}$ claims he received from Alice$_i$.
- $\mathbf{p}^i_{k'}$ is the proof sequence that Bob$^i_{k'}$ claims he received from Alice$_i$.

Algorithm 1: QNVA(k)

(**Step**$_0$) **Initialize** ▹ $M_A = M_V = \emptyset$

(**Step**$_1$) **Receive** ▹ Bob$_k^i$ receives Alice$_i$'s verification outcome c_k^i and proof $\mathbf{p}_k^i$.

(**Step**$_2$) **Test** ▹ Bob$_k^i$ calls the verification test IsAlice'sProofConsistent (Figure 5) to check whether $\mathbf{p}_k^i$ is consistent with c_k^i.

- ⋆ If the test returns TRUE, then Bob$_k^i$ accepts Alice$_i$'s assessment.
- ⋆ If the test returns FALSE, then Bob$_k^i$ rejects the news in question as fake, adds Alice$_i$ to his M_V list, and terminates the algorithm.

(**Step**$_3$) **Send** ▹ Upon the successful completion of the previous verification check, Bob$_k^i$ sends to every other Bob$_{k'}^i$, $(1 \leq k' \neq k \leq n_i)$ not contained in his M_A list, the verification outcome c_k^i and the accompanying proof $\mathbf{p}_k^i$ received from Alice$_i$.

(**Step**$_4$) **Receive** ▹ Bob$_k^i$ receives from every other Bob$_{k'}^i$, $(1 \leq k' \neq k \leq n_i)$ not contained in his M_A list, the verification outcome $c_{k'}^i$ and proof $\mathbf{p}_{k'}^i$, Bob$_{k'}^i$ claims he received from Alice$_i$.

(**Step**$_5$) **Compare** ▹ Bob$_k^i$ compares his c_k^i to all other $c_{k'}^i$.

- ⋆ If all $c_{k'}^i$ coincide with c_k^i, then Bob$_k^i$ sticks to his preliminary decision, and terminates the algorithm.
- ⋆ If there is *at least one* $c_{k'}^i$ such that $c_{k'}^i = \overline{c_k^i}$, Bob$_k^i$ calls the verification test IsBob'sProofConsistent (Figure 7) to check whether $\mathbf{p}_{k'}^i$ is consistent with $\overline{c_k^i}$.
  - □ If the test returns FALSE, then Bob$_k^i$ adds Bob$_{k'}^i$ to his M_A list, and repeats the same procedure for the next opposite verification outcome, if any.
  - □ If the test returns TRUE, then Bob$_k^i$ rejects the news in question as fake, adds Alice$_i$ to his M_V list, and terminates the algorithm.

In real life, the existence of opposite conflicting verification outcomes increases the odds of confusion and spread of misinformation. The quantum news verification algorithm, by taking advantage of the phenomenon of entanglement and its unique ramifications, can eliminate the risks in certain critical situations, as those outlined in the preceding scenarios ($\mathbf{S}_1$)–($\mathbf{S}_3$).

5. Discussion and Conclusions

In the era of social media, the proliferation of fake news has emerged as a pressing issue. Particularly in economically developed countries, users tend to encounter more false information than accurate content. The impact of fake news on major social media platforms extends beyond the digital realm, influencing people's opinions and actions in the real world. Researchers have been driven to seek practical solutions to address this undesirable situation.

This research paper introduces a fresh perspective on the critical topic of news verification. Departing from the conventional quantum machine learning approach, our approach explores an alternative quantum avenue. Drawing inspiration from successful quantum protocols that achieve detectable Byzantine Agreement in massively distributed environments, we propose the entanglement-based quantum algorithm QNVA.

The QNVA offers several advantages:

- Generality: It can handle any number of news aggregators and verifiers.
- Efficiency: The algorithm completes in a constant number of steps, regardless of the participant count.
- Simplicity: It relies solely on EPR (specifically $|\Phi^+\rangle$) pairs. EPR pairs are the easiest maximally entangled states to produce, unlike more complex states such as $|GHZ_n\rangle$ and $|W_n\rangle$, which do not scale so easily as the number of players increases.

The aforementioned attributes underscore its scalability and practical applicability. To reinforce this assertion, we examine in Table 1 how the chosen value of the accuracy degree d influences the likelihood of a malicious aggregator successfully fabricating a consistent proof sequence. Notably, the accuracy degree d remains independent of the number of participants, further enhancing the algorithm's scalability. Naturally, selecting an appropriate value for d is crucial to ensure that the probability of a malicious actor successfully forging a consistent proof sequence is negligible. The rationale behind d not scaling with the number of aggregators and verifiers lies in the protocol's consistent utilization of EPR pairs, signifying bipartite entanglement. As per protocol guidelines, each consistency check involves a comparison between two bit vectors. Consequently, irrespective of the participant count, each comparison entails only two bit strings. Furthermore, even in the most general scenario, this comparison involves just two bits, denoted as i and j, in each tuple. Thus, probabilistically, the situation remains consistent. In essence, the probability of a malicious aggregator deceiving an honest aggregator hinges on the likelihood of selecting the correct configuration from many possibilities. The total number of configurations equals the ways to distribute approximately $\frac{d}{4}$ identical objects (either 0 or 1) into approximately $\frac{d}{2}$ distinguishable boxes (representing the uncertain tuples). The probability of a cheater correctly placing *all* the approximately $\frac{d}{4}$ bits within the approximately $\frac{d}{2}$ cryptic tuples is

$$P(\text{ malicious aggregator cheats }) \approx \frac{1}{\binom{d/2}{d/4}}, \tag{30}$$

which tends to zero as d increases.

Table 1. This table shows how the chosen value of the degree of accuracy d affects the probability that a malicious aggregator succeeds in forging a consistent proof sequence.

How the Degree of Accuracy d Affects the Probability P			
d	**d/2**	**d/4**	**P(malicious aggregator cheats)**
4	2	1	5.000E−1
8	4	2	1.667E−1
16	8	4	1.429E−2
32	16	10	7.770E−5
64	21	16	1.664E−9

Author Contributions: Conceptualization, T.A. and A.S.; methodology, T.A.; validation, A.S.; formal analysis, A.S.; investigation, T.A.; writing original draft preparation, T.A. and A.S.; writing review and editing, T.A. and A.S.; visualization, A.S.; supervision, T.A.; project administration, T.A. and A.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable; the study does not report any data.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Campan, A.; Cuzzocrea, A.; Truta, T.M. Fighting fake news spread in online social networks: Actual trends and future research directions. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; IEEE: Piscataway, NJ, USA, 2017. https://doi.org/10.1109/bigdata.2017.8258484.
2. Zhou, X.; Zafarani, R.; Shu, K.; Liu, H. Fake News: Fundamental Theories, Detection Strategies and Challenges. In Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining, WSDM '19, Melbourne, VIC, Australia, 11–15 February 2019; ACM: New York, NY, USA, 2019. https://doi.org/10.1145/3289600.3291382.
3. Vorhies, W. Using Algorithms to Detect Fake News—The State of the Art—DataScienceCentral.com—datasciencecentral.com. 2017. Available online: https://www.datasciencecentral.com/using-algorithms-to-detect-fake-news-the-state-of-the-art/ (accessed on 14 January 2024).
4. Shu, K.; Sliva, A.; Wang, S.; Tang, J.; Liu, H. Fake News Detection on Social Media: A Data Mining Perspective. *ACM SIGKDD Explor. Newsl.* **2017**, *19*, 22–36. https://doi.org/10.1145/3137597.3137600.
5. Rashkin, H.; Choi, E.; Jang, J.Y.; Volkova, S.; Choi, Y. Truth of Varying Shades: Analyzing Language in Fake News and Political Fact-Checking. In Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing, Copenhagen, Denmark, 7–11 September 2017; Association for Computational Linguistics: Cambridge, MA, USA, 2017. https://doi.org/10.18653/v1/d17-1317.
6. Mustafaraj, E.; Metaxas, P.T. The Fake News Spreading Plague: Was it Preventable? *arXiv* **2017**. https://doi.org/10.48550/ARXIV.1703.06988.
7. Gilda, S. Notice of Violation of IEEE Publication Principles: Evaluating machine learning algorithms for fake news detection. In Proceedings of the 2017 IEEE 15th Student Conference on Research and Development (SCOReD), Wilayah Persekutuan Putrajaya, Malaysia, 13–14 December 2017; IEEE: Piscataway, NJ, USA, 2017. https://doi.org/10.1109/scored.2017.8305411.
8. Farajtabar, M.; Yang, J.; Ye, X.; Xu, H.; Trivedi, R.; Khalil, E.; Li, S.; Song, L.; Zha, H. Fake News Mitigation via Point Process Based Intervention. In Proceedings of the 34th International Conference on Machine Learning, Sydney, Australia, 6–11 August 2017; Precup, D.; Teh, Y.W., Eds.; PMLR 2017; Volume 70, Proceedings of Machine Learning Research, pp. 1097–1106.
9. Agudelo, G.E.R.; Parra, O.J.S.; Velandia, J.B., Raising a Model for Fake News Detection Using Machine Learning in Python. In *Challenges and Opportunities in the Digital Era*; Springer International Publishing: Cham, Switzerland 2018; pp. 596–604. https://doi.org/10.1007/978-3-030-02131-3_52.
10. Kesarwani, A.; Chauhan, S.S.; Nair, A.R.; Verma, G., Supervised Machine Learning Algorithms for Fake News Detection. In *Advances in Communication and Computational Technology*; Springer Nature: Singapore, 2020; pp. 767–778. https://doi.org/10.1007/978-981-15-5341-7_58.
11. Kesarwani, A.; Chauhan, S.S.; Nair, A.R. Fake News Detection on Social Media using K-Nearest Neighbor Classifier. In Proceedings of the 2020 International Conference on Advances in Computing and Communication Engineering (ICACCE), Las Vegas, NV, USA, 22–24 June 2020; IEEE: Piscataway, NJ, USA, 2020. https://doi.org/10.1109/icacce49060.2020.9154997.
12. Ozbay, F.A.; Alatas, B. Fake news detection within online social media using supervised artificial intelligence algorithms. *Phys. A: Stat. Mech. Its Appl.* **2020**, *540*, 123174. https://doi.org/10.1016/j.physa.2019.123174.
13. Vijayaraghavan, S.; Wang, Y.; Guo, Z.; Voong, J.; Xu, W.; Nasseri, A.; Cai, J.; Li, L.; Vuong, K.; Wadhwa, E. Fake News Detection with Different Models. *arXiv* **2003** https://doi.org/10.48550/ARXIV.2003.04978.
14. Choudhary, P.; Pandey, S.; Tripathi, S.; Chaurasiya, S., Fake News Detection Based on Machine Learning. In *Lecture Notes in Electrical Engineering*; Springer: Singapore, 2021; pp. 67–75. https://doi.org/10.1007/978-981-15-9938-5_8.
15. Nagashri, K.; Sangeetha, J., Fake News Detection Using Passive-Aggressive Classifier and Other Machine Learning Algorithms. In *Advances in Computing and Network Communications*; Springer: Singapore, 2021; pp. 221–233. https://doi.org/10.1007/978-981-33-6987-0_19.
16. Pandey, S.; Prabhakaran, S.; Subba Reddy, N.V.; Acharya, D. Fake News Detection from Online media using Machine learning Classifiers. *J. Physics: Conf. Ser.* **2022**, *2161*, 012027. https://doi.org/10.1088/1742-6596/2161/1/012027.
17. Tee, W.J.; Murugesan, R.K. Trust Network, Blockchain and Evolution in Social Media to Build Trust and Prevent Fake News. In Proceedings of the 2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA), Subang Jaya, Malaysia, 26–28 October 2018; IEEE: Piscataway, NJ, USA, 2018. https://doi.org/10.1109/icaccaf.2018.8776822.
18. Chow, J.; Dial, O.; Gambetta, J. IBM Quantum Breaks the 100-Qubit Processor Barrier. 2021. Available online: https://www.ibm.com/quantum/blog/127-qubit-quantum-processor-eagle (accessed on 2 March 2024).
19. Newsroom, I. IBM Unveils 400 Qubit-Plus Quantum Processor. 2022. Available online: https://newsroom.ibm.com/2022-11-09-IBM-Unveils-400-Qubit-Plus-Quantum-Processor-and-Next-Generation-IBM-Quantum-System-Two (accessed on 2 March 2024).
20. Gambetta, J. The Hardware and Software for the Era of Quantum Utility Is Here. 2023. Available online: https://www.ibm.com/quantum/blog/quantum-roadmap-2033 (accessed on 2 March 2024).
21. Alfieri, A.; Anantharaman, S.B.; Zhang, H.; Jariwala, D. Nanomaterials for Quantum Information Science and Engineering. *Adv. Mater.* **2023**, *35*, 2109621. https://doi.org/10.1002/adma.202109621.
22. Kagan, C.R.; Bassett, L.C.; Murray, C.B.; Thompson, S.M. Colloidal Quantum Dots as Platforms for Quantum Information Science. *Chem. Rev.* **2021**, *121*, 3186–3233. https://doi.org/10.1021/acs.chemrev.0c00831.

23. Rozenman, G.G.; Kundu, N.K.; Liu, R.; Zhang, L.; Maslennikov, A.; Reches, Y.; Youm, H.Y. The quantum internet: A synergy of quantum information technologies and 6G networks. *IET Quantum Commun.* **2023**, *4*, 147–166. https://doi.org/10.1049/qtc2.12069.
24. Feinberg, A.J.; Verma, D.; O'Connell-Lopez, S.M.; Erukala, S.; Tanyag, R.M.P.; Pang, W.; Saladrigas, C.A.; Toulson, B.W.; Borgwardt, M.; Shivaram, N.; et al. Aggregation of solutes in bosonic versus fermionic quantum fluids. *Sci. Adv.* **2021**, *7*, eabk2247. https://doi.org/10.1126/sciadv.abk2247.
25. EPFL.; Quantum Integrity. Quantum Integrity and EPFL develop Deep Fake Detector. 2019. Available online: https://www.startupticker.ch/en/news/september-2019/quantum-integrity-and-epfl-develop-deep-fake-detector (accessed on 14 January 2024).
26. Kamal, S.; Chahar, V.; Sharma, S. Quantum Machine Learning-based Detection of Fake News and Deep Fake Videos. *IEEE Technol. Policy Ethics* **2022**. Available online: https://cmte.ieee.org/futuredirections/tech-policy-ethics/july-2022/quantum-machine-learning-based-detection-of-fake-news-and-deep-fake-videos (accessed on 2 March 2024).
27. Tian, Z.; Baskiyar, S. Fake News Detection: An Application of Quantum K-Nearest Neighbors. In Proceedings of the 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 5–7 December 2021; IEEE: Piscataway, NJ, USA, 2021. https://doi.org/10.1109/ssci50451.2021.9659944.
28. Google. Announcing TensorFlow Quantum: An Open Source Library for Quantum Machine Learning—blog.research.google. 2020. Available online: https://blog.research.google/2020/03/announcing-tensorflow-quantum-open.html (accessed on 14 January 2024).
29. Andronikos, T.; Sirokofskich, A. A Quantum Detectable Byzantine Agreement Protocol Using Only EPR Pairs. *Appl. Sci.* **2023**, *13*, 8405. https://doi.org/10.3390/app13148405.
30. Meyer, D.A. Quantum strategies. *Phys. Rev. Lett.* **1999**, *82*, 1052. https://doi.org/10.1103/physrevlett.82.1052.
31. Eisert, J.; Wilkens, M.; Lewenstein, M. Quantum games and quantum strategies. *Phys. Rev. Lett.* **1999**, *83*, 3077. https://doi.org/10.1103/physrevlett.83.3077.
32. Rycerz, K.; Frackiewicz, P. A quantum approach to twice-repeated 2 x 2 game. *Quantum Inf. Process.* **2020**, *19*, 269. https://doi.org/10.1007/s11128-020-02743-0.
33. Altintas, A.A.; Ozaydin, F.; Bayindir, C.; Bayrakci, V. Prisoners' Dilemma in a Spatially Separated System Based on Spin–Photon Interactions. *Photonics* **2022**, *9*, 617. https://doi.org/10.3390/photonics9090617.
34. Anand, N.; Benjamin, C. Do quantum strategies always win? *Quantum Inf. Process.* **2015**, *14*, 4027–4038. https://doi.org/10.1007/s11128-015-1105-y.
35. Andronikos, T.; Sirokofskich, A. The Connection between the PQ Penny Flip Game and the Dihedral Groups. *Mathematics* **2021**, *9*, 1115. https://doi.org/10.3390/math9101115.
36. Andronikos, T. Conditions that enable a player to surely win in sequential quantum games. *Quantum Inf. Process.* **2022**, *21*, 268. https://doi.org/10.1007/s11128-022-03604-8.
37. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
38. Andronikos, T.; Stefanidakis, M. A Two-Party Quantum Parliament. *Algorithms* **2022**, *15*, 62. https://doi.org/10.3390/a15020062.
39. Cruz, D.; Fournier, R.; Gremion, F.; Jeannerot, A.; Komagata, K.; Tosic, T.; Thiesbrummel, J.; Chan, C.L.; Macris, N.; Dupertuis, M.A.; et al. Efficient Quantum Algorithms for GHZ and W States, and Implementation on the IBM Quantum Computer. *Adv. Quantum Technol.* **2019**, *2*, 1900015. https://doi.org/10.1002/qute.201900015.
40. Bell, J.S. On the Einstein Podolsky Rosen paradox. *Phys. Phys. Fiz.* **1964**, *1*, 195–200. https://doi.org/10.1103/physicsphysiquefizika.1.195.
41. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2010.
42. Neigovzen, R.; Rodó, C.; Adesso, G.; Sanpera, A. Multipartite continuous-variable solution for the Byzantine agreement problem. *Phys. Rev. A* **2008**, *77*, 062307. https://doi.org/10.1103/physreva.77.062307.
43. Feng, Y.; Shi, R.; Zhou, J.; Liao, Q.; Guo, Y. Quantum Byzantine Agreement with Tripartite Entangled States. *Int. J. Theor. Phys.* **2019**, *58*, 1482–1498. https://doi.org/10.1007/s10773-019-04035-5.
44. Wang, W.; Yu, Y.; Du, L. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm. *Sci. Rep.* **2022**, *12*, 8606. https://doi.org/10.1038/s41598-022-12412-0.
45. Yang, Z.; Salman, T.; Jain, R.; Pietro, R.D. Decentralization Using Quantum Blockchain: A Theoretical Analysis. *IEEE Trans. Quantum Eng.* **2022**, *3*, 4100716. https://doi.org/10.1109/tqe.2022.3207111.
46. Qu, Z.; Zhang, Z.; Liu, B.; Tiwari, P.; Ning, X.; Muhammad, K. Quantum detectable Byzantine agreement for distributed data trust management in blockchain. *Inf. Sci.* **2023**, *637*, 118909. https://doi.org/10.1016/j.ins.2023.03.134.
47. Ikeda, K.; Lowe, A. Quantum protocol for decision making and verifying truthfulness among N-quantum parties: Solution and extension of the quantum coin flipping game. *IET Quantum Commun.* **2023**, *4*, 218–227. https://doi.org/10.1049/qtc2.12066.