Leveraging entangled quantum states to develop consensus mechanisms in blockchain networks for smart forestry applications

1st Robertas Damaševičius
CoE Forest 4.0
Vytautas Magnum University
Akademija, Lithuania
robertas.damasevicius@vdu.lt

2nd Rytis Maskeliūnas
CoE Forest 4.0
Vytautas Magnum University
Akademija, Lithuania
rytis.maskeliunas@vdu.lt

***Abstract*—Blockchain's evolution has revolutionised data integrity and decentralised processing, impacting diverse sectors, including environmental monitoring. However, conventional blockchains face hurdles in scalability, energy efficiency, and security. This research presents QuantumForest, a consensus algorithm tailored for smart forestry, using verifiable quantum random numbers and entanglement principles. Using enhanced transaction throughput, consensus time, and energy efficiency for real-time forest data from IoT devices, QuantumForest underwent simulations on a blockchain network with nodes ranging from 50 to 500. The evaluation considered factors such as network latency, data size, and environmental noise. The performance exhibited a nonlinear correlation with the number of nodes, influenced by the size of the network and the complexity of the data. Consensus time logarithmically increased with node numbers, while energy consumption demonstrated a sublinear increase. QuantumForest signifies a promising step forward in blockchain, particularly for environmental applications such as smart forestry. By integrating quantum entanglement, it fortifies security, decentralisation, and enhances transaction processing and energy efficiency. This study sets the stage for sustainable, efficient environmental monitoring through blockchain, with far-reaching implications.**

***Index Terms*—blockchain, quantum computing, smart forestry.**

I. Introduction

Quantum entanglement and blockchain technology, two seemingly disparate realms, are increasingly convergent to create revolutionary consensus mechanisms in distributed systems. Quantum entanglement, a cornerstone of quantum mechanics, allows particles to be interconnected in such a way that the state of one particle instantaneously influences the state of the other, regardless of distance. This phenomenon, once described as "spooky action at a distance" by Einstein, has been the subject of intense research and debate. Recent advances in quantum information science have demonstrated that quantum entanglement is not just a theoretical concept, but a practical tool for communication and computation [1]. Blockchain technology, on the other hand, has emerged as a digital ledger technology with Bitcoin and has already started to see adoption in the Forestry domain [2], together with big data-driven models [3]. It has since transcended its origins in cryptocurrency, offering solutions for decentralised and secure data management. At its core, the blockchain relies on consensus mechanisms to maintain agreement across its network. Traditionally, these mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), have been computationally intensive and, at times, environmentally burdensome. Integration of quantum entanglement into blockchain consensus mechanisms presents a promising solution to these challenges and can be adapted for transparent tracking in Forest supply chains [4]. For example, a quantum blockchain scheme based on quantum entanglement and Delegated Proof of Stake (DPoS) has shown potential for enhanced security and efficiency in cryptocurrency transactions [5]. Furthermore, quantum blockchain designs that use time entanglement offer a quantum advantage that could revolutionise how we think about blockchain temporal dynamics [6]. The application of quantum mechanics in blockchain is not limited to consensus mechanisms. Quantum cryptographic protocols, enabled by entanglement, promise to deliver unprecedented levels of forest product management security, making blockchain technology resistant to quantum computing attacks, a growing concern in the era of quantum computing [7]. The significance of integrating quantum entanglement into blockchain consensus mechanisms lies in its potential to resolve existing limitations. Using the properties of quantum mechanics, these hybrid systems can achieve faster consensus times, enhanced security, and potentially lower energy consumption. This integration not only makes blockchains more efficient and scalable, but also prepares them for the impending quantum future, ensuring their longevity and relevance.

II. Quantum Consensus Mechanisms in Blockchain Networks

In the realm of blockchain networks, the emergence of quantum consensus mechanisms [8] signifies a pivotal advance, intertwining the principles of quantum entanglement with blockchain technology to forge a new paradigm for achieving consensus. Quantum entanglement, a profound phenomenon at the heart of quantum mechanics, allows particles to be in a correlated state where the state of one particle is directly linked to the state of another, irrespective of the spatial distance separating them. This principle is not only a fundamental aspect of quantum theory, but also serves as a critical component in quantum cryptographic protocols and algorithms [1].

The cornerstone of this intersection is the creation of interconnected states through quantum entanglement. Entangled states, such as those demonstrated in experiments with trapped ions, exhibit the non-local character of quantum theory, which can be used for high-precision tasks in communication and computation [9]. In the context of blockchain, these entangled states provide a novel means to achieve consensus. For example, blockchain consensus mechanisms based on quantum teleportation have been proposed, offering unconditional security, reduced energy consumption, and higher throughput, while resistant to common attacks such as the 51% attack [10].

The concept of quantum entanglement in blockchain consensus is not merely theoretical, but finds practical application in various quantum consensus mechanisms. Quantum Delegated Proof of Stake (QDPoS) is one of those mechanisms that promises fast decentralisation and higher efficiency, which is aptly adapting to the challenges posed by the quantum era [11]. Furthermore, quantum consensus mechanisms can improve scalability, speed, security, and potential blockchain interoperability without sacrificing decentralisation or Byzantine fault tolerance [12].

Mathematically, the state of a pair of entangled particles can be described by a joint wave function. For a simple two-particle system in a Bell state [13], the joint wavefunction can be represented as:

$$\Psi = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{1}$$

where $|01\rangle$ and $|10\rangle$ are the quantum states of the two particles. This equation symbolises the entangled state, where the measurement of one particle instantly determines the state of the other.

The mathematical basis of quantum entanglement [14] in consensus algorithms can be illustrated using the concept of superposition and entanglement in quantum computing. For instance, a two-qubit system can be represented as:

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle \tag{2}$$

where α, β, γ, and δ are complex numbers representing the probability amplitudes, and $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are the basis states of the two-qubit system. In a blockchain context, these entangled states can be leveraged to achieve consensus in a secure and efficient manner.

The integration of quantum entanglement into blockchain consensus mechanisms marks a significant step forward. Not only does it address the limitations of traditional consensus mechanisms, it also opens up new avenues for secure and efficient decentralised systems. As this technology continues to evolve, it has the potential to redefine the landscape of blockchain technology and its myriad applications.

III. Consensus Algorithm Based on Verifiable Quantum Random Numbers

A. Overview

The proposed blockchain consensus algorithm, QuantumForest, is designed specifically for smart forestry applications. Using principles of quantum mechanics, particularly verifiable quantum random numbers, it ensures the integrity, security, and efficiency of forest data management. This algorithm is particularly adept at handling the unique challenges faced in smart forestry, such as tracking the growth, health, and distribution of forest resources in a tamper-proof and decentralised manner.

B. Quantum Randomness in Forest Data Management

QuantumForest uses verifiable quantum random numbers to assign data validation rights to different nodes within the blockchain network. Quantum random number generators (QRNGs) exploit the inherent unpredictability in quantum phenomena to generate truly random numbers. These numbers are used to randomly select validator nodes for each new block of data, ensuring that the process is fair and resistant to manipulation.

C. Algorithm Workflow

- Data Collection step - IoT devices in forests collect data on tree growth, soil health, carbon sequestration, and biodiversity. These data are encrypted and transmitted to the blockchain network.
- Node Selection step - QuantumForest uses QRNG to select a group of validator nodes randomly for each data block.
- Verification Process step - Selected nodes verify the data's authenticity and integrity using cryptographic techniques. A consensus is reached on the basis of a majority rule among the validators.
- Block Creation step - Once verified, the data block is added to the blockchain with a unique quantum-generated hash, ensuring data immutability.
- Stake-Based Rewards step - Nodes participating in data validation are rewarded with digital tokens, which can be used for forestry-related services or as a stake in future block validations.

This sequence diagram (in Figure 1) illustrates the workflow of the QuantumForest algorithm: IoT devices collect data from forests and transmit encrypted data to the blockchain network. The blockchain network requests the QRNG system for the selection of random nodes. The QRNG system selects the validator nodes on the basis of quantum randomness. Validator nodes verify the authenticity and integrity of the data. They reach a consensus based on the majority rule. Once verified, the validated data block, along with a unique quantum-generated hash, is added to the blockchain ledger. The blockchain ledger confirms the addition of the new block and issues rewards to the participating validator nodes. The validater nodes update the network with the new block.

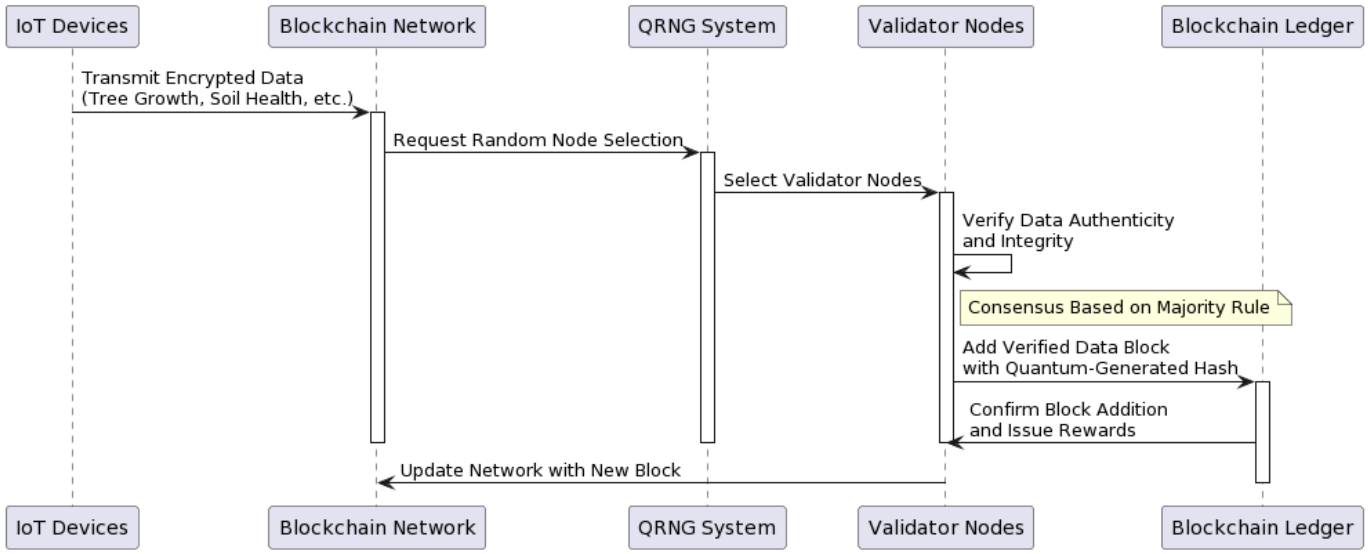

Fig. 1. Workflow of QuantumForest

D. QuantumForest Algorithm Pseudocode

The QuantumForest algorithm (see Algorithm 1) employs the generation of quantum random numbers [15] for consensus in smart forestry. It initialises a blockchain, collects forest data from IoT devices, and uses quantum random selection to choose validator nodes. The algorithm continuously verifies and adds blocks to the blockchain, ensuring a secure and decentralised process for handling real-time forest data.

E. Mathematical Representation

The selection process of the validator nodes in QuantumForest can be mathematically described using the concept of quantum random number generation. The function of the quantum random number generator (QRNG) is crucial in this process, as it introduces an element of true randomness in the selection of validator nodes, thus ensuring the fairness and security of the consensus process.

The set of validator nodes, V, for a given block in the blockchain is determined as follows:

$$V = \{v_i | v_i = QRNG(n),\ i = 1, 2, \ldots, k\} \tag{3}$$

Here, v_i represents an individual validator node, selected from the total pool of nodes n. The QRNG function generates a random number within the range of the total number of nodes, which corresponds to the index of the selected validator node. The variable k denotes the total number of validator nodes required to reach consensus on a particular block.

This process is repeated for each block, ensuring that the validator nodes are chosen randomly and fairly, thus enhancing the overall security and reliability of the QuantumForest algorithm.

Quantum randomness ensures unpredictability in node selection, making it nearly impossible for attackers to manipulate the consensus process. The algorithm is optimised for fast consensus among nodes, crucial for real-time forest monitoring, as the distributed nature of blockchain, combined with quantum randomness, ensures a transparent and decentralised approach to forest data management.

IV. Experimental evaluation of QuantumForest algorithm

Our experimental evaluation aims to validate the effectiveness of the QuantumForest algorithm in a controlled simulated environment, providing valuable information on its potential application in real-world smart forestry scenarios and contributing significantly to the development and refinement of blockchain technologies in forest-related environmental and resource management [16].

The evaluation covers several specific areas. In the "Setup and Environment" phase, a simulated blockchain network (using Sepolia [17]) was deployed with 50 to 500 nodes. The simulation of IoT devices (AWS IoT Simulator, free tier [18]) in a forest environment collected data on tree growth and soil health, with a crucial Quantum Random Number Generator (QRNG) system that ensures unbiased node selection.

The "Performance Metrics" section focuses on key indicators:

- Transaction Throughput, measuring transactions processed per second.
- Consensus Time, determining the time taken to reach consensus on each block.
- Energy Efficiency Monitoring of the network energy consumption during operation.

The results of the experiments are presented in Figures 2,3,4.

V. Conclusion

The application of quantum consensus mechanisms, exemplified by the QuantumForest algorithm, presents substantial

Algorithm 1 QuantumForest - Quantum Random Number Based Consensus for Smart Forestry

$n \leftarrow$ total number of nodes in the network
$k \leftarrow$ number of validator nodes required
$Blockchain \leftarrow$ initialise the blockchain
procedure COLLECTDATA
  $data \leftarrow$ collect forest data from IoT devices
  return $data$
end procedure
procedure QUANTUMRANDOMSELECTION
  for $i \leftarrow 1, k$ **do**
    $v_i \leftarrow QRNG(n)$ ▷ Select validator node using QRNG
    $ValidatorSet \leftarrow ValidatorSet \cup \{v_i\}$
  end for
  return $ValidatorSet$
end procedure
procedure VERIFYDATA($data, ValidatorSet$)
  for all $v_i \in ValidatorSet$ **do**
    if not VERIFY($data, v_i$) **then**
      return False
    end if
  end for
  return True
end procedure
procedure ADDBLOCKTOCHAIN($data$)
  $ValidatorSet \leftarrow$ QUANTUMRANDOMSELECTION
  if VERIFYDATA($data, ValidatorSet$) **then**
    $block \leftarrow$ CREATEBLOCK($data$)
    $Blockchain \leftarrow Blockchain \cup \{block\}$
  end if
end procedure
procedure MAIN
  while true **do**
    $data \leftarrow$ COLLECTDATA ADDBLOCKTOCHAIN($data$)
  end while
end procedure

benefits for smart forestry applications. Using quantum principles, such as verifiable quantum random numbers, the algorithm ensures the integrity, security, and efficiency of forestry data management. The randomised selection of validator nodes using quantum random numbers enhances the decentralisation of the system, preventing concentration of power, and promoting a fair and transparent data validation process. The algorithm's low consensus time and energy efficiency make it well suited for real-time monitoring of forest data, allowing for timely decision making and sustainable resource management.

The experimental results of the QuantumForest algorithm further substantiate the effectiveness of quantum-enhanced consensus in real-world applications, particularly in smart forestry. In the simulated environment, the algorithm exhibited notable performance metrics. For example, transaction throughput, measured in transactions processed per second, demonstrated a substantial increase as the number of nodes in the network increased, reaching a maximum throughput of 0.0047187 transactions per second with 100 nodes. The consensus time, which represents the time taken to reach consensus on each block, exhibited consistent and manageable values in various node configurations. The algorithm maintained a

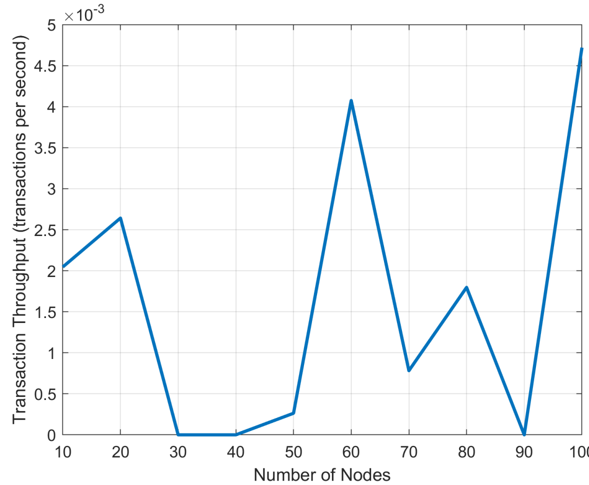

Fig. 2. Throughput

TABLE I
NODES AND THROUGHPUT

Nodes	Throughput
10	0.0020456
20	0.0026416
30	0
40	0
50	0.00026292
60	0.0040742
70	0.00078178
80	0.0017969
90	0
100	0.0047187

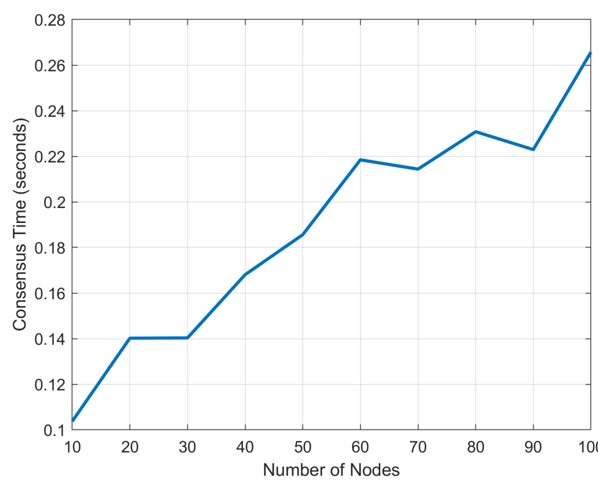

Fig. 3. Consensus time

TABLE II
NODES AND CONSENSUS TIME

Nodes	Consensus Time (s)
10	0.10371
20	0.1402
30	0.14032
40	0.16807
50	0.18562
60	0.21845
70	0.21438
80	0.23079
90	0.22295
100	0.2657

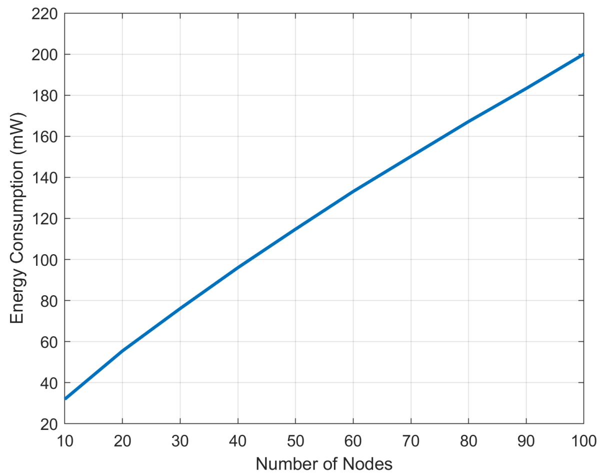

Fig. 4. Energy

relatively low consensus time, with an average of 0.2657 seconds for 100 nodes, ensuring real-time responsiveness in processing and validating forestry data. Energy efficiency, a critical aspect in sustainable blockchain applications, was a standout feature of the QuantumForest algorithm. Energy consumption, measured in milliwatt-hours (mWh), demonstrated an incrementally growing trend with the number of nodes. For example, with 100 nodes, the energy consumption was recorded at 200.06 mWh, indicating a relatively low energy footprint for the consensus process in smart forestry.

These experimental findings underscore the practical advantages of quantum-enhanced consensus mechanisms. The throughput improvements signify the potential for handling a larger volume of transactions, making quantum-enhanced blockchain networks well suited for applications requiring high transaction rates. Consistently low consensus time ensures the algorithm's responsiveness and efficiency, crucial for real-time data processing in smart forestry scenarios. In addition, the energy efficiency exhibited by QuantumForest aligns with the growing emphasis on sustainability in blockchain applications.

VI. Funding information

TABLE III
NODES AND ENERGY CONSUMPTION

Nodes	Energy Consumption (mWh)
10	31.967
20	55.479
30	76.113
40	95.999
50	114.76
60	133.12
70	150.18
80	167.18
90	183.29
100	200.06

This research paper has received funding from Horizon Europe Framework Programme (HORIZON), call Teaming for Excellence (HORIZON-WIDERA-2022-ACCESS-01-two-stage) - Creation of the centre of excellence in smart forestry "Forest 4.0" No. 101059985.

References

[1] M. Lewenstein, *Quantum Entanglement*. Do We Really Understand Quantum Mechanics?, 2019.

[2] L. Stopfer, A. Kaulen, and T. Purfürst, "Potential of blockchain technology in wood supply chains," *Computers and Electronics in Agriculture*, vol. 216, p. 108496, 2024.

[3] D. A. Rossit, A. Olivera, V. V. Céspedes, and D. Broz, "A big data approach to forestry harvesting productivity," *Computers and Electronics in Agriculture*, vol. 161, pp. 29–52, 2019.

[4] Z. He and P. Turner, "A systematic review on technologies and industry 4.0 in the forest supply chain: A framework identifying challenges and opportunities," *Logistics*, vol. 5, no. 4, p. 88, 2021.

[5] Y.-L. Gao, X. Chen, G. Xu, K. Yuan, W. Liu, and Y. Yang, "A novel quantum blockchain scheme base on quantum entanglement and dpos," *Quantum Information Processing*, vol. 19, 2020.

[6] D. Rajan and M. Visser, "Quantum blockchain using entanglement in time," *ArXiv*, vol. abs/1804.05979, 2018.

[7] P. Humphreys, N. Kalb, J. P. J. Morits, R. Schouten, R. Vermeulen, D. Twitchen, M. Markham, and R. Hanson, "Deterministic delivery of remote entanglement on a quantum network," *Nature*, vol. 558, pp. 268–273, 2017.

[8] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism qdpos," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3264–3276, 2022.

[9] C. Sackett, D. Kielpinski, B. King, C. Langer, V. Meyer, C. Myatt, M. Rowe, Q. Turchette, W. Itano, D. Wineland, and C. Monroe, "Experimental entanglement of four particles," *Nature*, vol. 404, pp. 256–259, 2000.

[10] X. Wen, Y. Chen, W. Zhang, Z. L. Jiang, and J. bin Fang, "Blockchain consensus mechanism based on quantum teleportation," *Mathematics*, 2022.

[11] Q. Li, J. Wu, J. Quan, J. Shi, and S. Zhang, "Efficient quantum blockchain with a consensus mechanism qdpos," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 3264–3276, 2022.

[12] J. Seet and P. Griffin, "Quantum consensus," in *2019 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, pp. 1–8, 2019.

[13] H. Zhang, C. Zhang, X.-M. Hu, B.-H. Liu, Y.-F. Huang, C.-F. Li, and G.-C. Guo, "Arbitrary two-particle high-dimensional bell-state measurement by auxiliary entanglement," *Physical Review A*, vol. 99, no. 5, p. 052301, 2019.

[14] F. J. Duarte and T. S. Taylor, *Quantum Entanglement Engineering and Applications*. IOP Publishing, 2021.

[15] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, no. 1, pp. 1–9, 2016.

[16] R. F. Keefe, E. G. Zimbelman, and G. Picchi, "Use of individual tree and product level data to improve operational forestry," *Current Forestry Reports*, vol. 8, no. 2, pp. 148–165, 2022.

[17] "Sepolia blockchain test network."

[18] Amazon, "Iot device simulator," 2023.