Quantum-Resistant Bitcoin Protocol with Equitable Wealth Distribution: A Novel Approach

Pavan R Kashyap
Student
PES University, Bangalore
pavanrkashyap@gmail.com

N Raghu Kisore
Associate Professor
Mahindra Ecole Centrale, Hyderabad
raghukishore.neelisetti@mahindrauniversity.edu.in

Abstract*—In this work, we introduce an enhanced Bitcoin protocol designed to withstand imminent quantum threats, all while upholding decentralization and ensuring equitable wealth distribution in the future landscape of widespread quantum computer adoption. In the quantum age, cryptographic constructs such as Merkle trees and Proof-of-Work are more vulnerable to attack. We suggest a novel strategy built on the Shortest Vector Problem (SVP) and lattice-based cryptography to address these issues. The protocol strengthens Merkle tree generation and verification by using SVP principles, making it quantum-resistant. Additionally, we ensure equitable distribution of crypto wealth by introducing verifiers—entities separate from miners—thereby boosting transparency and decreasing concentration of crypto wealth in the hands of few mining consortiums. In order to meet the demand for improved computing capabilities in the future, this protocol also pioneers the idea of computational power as an investment. Our study contributes to a block chain paradigm that is safe, decentralized, and geared towards the future.

***Index Terms*—Block chain protocol, Quantum computing, Proof-of-Work(PoW), Merkle trees, Proof-of-Quantum Verification(PoQuVe), Shortest Vector Problem (SVP), Lattice-based cryptography, Quantum-resistant, Decentralization, Wealth distribution, Fair incentives, Verifiers, Indexed-Voting Quorums**

I. Introduction

The evolution of quantum computing has cast a shadow over the security of existing block chain paradigms, necessitating novel solutions that can withstand computational power of quantum computers. Conventional block chain technologies that form building blocks of crypto currencies such as bitcoin , once regarded as robust against classical attacks, are now exposed to heightened vulnerabilities due to the potential computational prowess of quantum machines. The looming challenge of quantum attacks calls for a re imagining of block chain's fundamental components to ensure long-term security and decentralization from the perspective of better distribution of crypto wealth.

In response to this imperative, we present a forward-looking protocol that incorporates the principles of Shortest Vector Problem (SVP) and lattice-based cryptography to revolutionize block chain security and decentralization. By doing so, we address the potential menace of quantum computing head-on, while simultaneously tackling the existing issue of mining by few member groups (also called mining farms) that plagues many crypto currency networks. In this work, we outline our protocol's architecture, illustrating its distinctiveness from traditional approaches. We delve into the rationale behind leveraging SVP and lattice-based cryptography, elucidating their role in securing the protocol against quantum threats [2]. Furthermore, we introduce the concept of verifiers as an innovative mechanism to ensure decentralization and equitable reward distribution for the participants of a crypto currency system. Verifiers, distinct from miners, play a pivotal role in reinforcing the integrity of the block chain while contributing to a more balanced distribution of rewards among network participants.

Finally, we delve into the transformative concept of computational power as a strategic investment within the block chain ecosystem. This notion not only accentuates the burgeoning significance of advanced computing capabilities but also underscores the imperative for prospective stakeholders to proactively invest in these resources, as we transition into an era where formidable computational prowess stands as the prevailing norm. Within the framework of our protocol,this commitment is driven by the enticing prospect of reaping augmented rewards,as a verifier.

In the subsequent sections, we detail the protocol's key components, explain it's operation through agent-based simulations, and present empirical evidence of its effectiveness in mitigating wealth disparity and preventing centralization. By combining cutting-edge cryptography principles with innovative economic incentives, our protocol offers a comprehensive solution to the twin challenges of Quantum resistant bit coin protocol while ensuring a more equitable wealth distribution.

II. Critical Concerns with Traditional block chain Network

A. Brute-force attacks

Inherent in Proof-of-Work (PoW) is the reliance on nonce brute-forcing [6]. Meanwhile, the conventional Merkle tree, powered by traditional hash functions, remains susceptible to pre-image and second pre-image attacks—both rooted in brute-forcing identical hash outcomes. The rise of Grover's algorithm [12] multiplies quantum brute-forcing capabilities, a risk compounded by the potential impact of quantum error correction. As quantum computers inch closer to replacing

PoW, the foundation of security embodied by both PoW and Merkle trees confronts imminent danger from brute force vulnerabilities.

B. Wealth Disparity and Centralization

The present block chain landscape stands marred by concerning centralization trends [9]. While a select group of miners command substantial computational might, the broader participant community remains sidelined in the wealth distribution. The formidable barriers to entry for aspiring miners underscore a lopsided system that perpetuates the dominance of a privileged minority.

The consequence of this disarray is the burgeoning wealth disparity, where a handful of miners amass unprecedented riches while the broader network's potential remains untapped. Despite the increasing prominence of Bitcoin and other crypto currencies, the majority of participants are unable to benefit directly from the burgeoning block chain ecosystem.

III. Proof-of-Quantum Verification (PoQuVe)

N-Dimensionalization of Merkle Trees and Lattice Mapping with f() Function

In the realm of conventional block chain systems, Merkle trees typically reside within one or two dimensions. However, this innovative approach aims to transcend these limitations by ushering in an N-dimensional paradigm. This transformation entails the extension of the Merkle tree into N dimensions. To facilitate this, each transaction slated for validation undergoes a unique mapping process orchestrated by the f() function – the lattice mapping function.

The f() function, serving as the lattice mapping mechanism, orchestrates the transformation of each transaction and its associated metadata into a distinct point within an N-dimensional q-ary lattice. The inherent characteristics of the f() function are as follows:

A) **Non-Linear Mapping**: The transaction's mapping onto the N-dimensional q-ary lattice is non-linear and random yet distinct.

B) **Repeatability and Integrity**: For a specific N-dimensional q-ary lattice, each application of the f() function on a given transaction consistently yields the same lattice point ensuring both data integrity and reproducibility is upheld.

C) **Optimal Space Utilization**: The f() function optimizes lattice space by mapping transactions to all available (q+1) points across N dimensions before revisiting previously allocated points. This dynamic allocation aids in preventing pre-image attacks.

D) **Resilience against Attacks**: Potential attackers are compelled to await the completion of $(q+1)^N$ mappings before reattempting a remapping, significantly deterring pre-image attacks. This safeguard is especially potent when N and q assume large values, as the time delay hinders malicious actions.

This lattice mapping process paves the way for the introduction of a novel participant – the verifier. Verifiers play a pivotal role in the Proof-of-Quantum Verification mechanism, contributing to the security and efficiency of the block chain ecosystem.

*A. **Proof-of-Quantum Verification: Stages and Mechanism***

The Proof-of-Quantum Verification mechanism navigates several distinctive phases:

1. **Tree Creation**: Miners construct N-dimensional Merkle trees, meticulously integrating validated transactions.

2. **Optimized Spraying**: Miners ingeniously introduce supplementary dummy transactions to finely calibrate the tree's complexity, aligning it with the consensus-defined threshold and constraints.

3. **Quorum Call Broadcasting**: Miners reach out to a selected group of verifiers, known as a quorum, to collectively verify the integrity and validity of a constructed tree in the block chain network before its placement.

4. **Verification Process**: Verifiers methodically scrutinize the generated tree for integrity, subsequently casting their votes to affirm or challenge its legitimacy. The miner emerging victorious in achieving the fastest and most widely supported verification outcome secures coveted block chain placement.

5. **Reward Distribution**: Successfully securing block chain placement serves as a catalyst, triggering a well-deserved allocation of rewards to both miners and verifiers. The magnitude of these rewards is intricately shaped by the network's unique complexities and intricacies.

*B. **Tree Generation***

The initiation of tree construction involves the establishment of an N-dimensional binary tree framework, wherein individual transactions serve as the foundational leaf nodes. To address scenarios where transactional volume is insufficient, we introduce nonce dummy transactions, characterized by unique nonces that set them apart within the lattice structure. These nonce-laden entities are subjected to the specialized lattice mapping function $f()$, resulting in a distinctive and immutable placement within the lattice.

Miners are furnished with essential **basis vectors**, which underpin their operations within the lattice. The intricacy of these vectors, determining their proximity to one another, is dictated by the collective network constraints and consensus guidelines. A pivotal element of our quantum-resilient strategy lies in the strategic deployment of the Shortest Vector Problem (SVP) algorithm. At its core, the SVP algorithm involves identifying the optimal linear combination of basis vectors that yields a point of unparalleled proximity to a designated reference point.

The potency of the chosen basis vectors greatly influences the SVP's efficiency. Basis vectors exhibiting quasi-orthogonal characteristics facilitate a streamlined SVP solution, whereas the convergence of these vectors escalates the computational challenge. Employing cosine similarity, we generate and allocate deliberately suboptimal basis vectors to miners, preserving the intricate balance of the block chain network.

Upon the completion of the lattice-based mapping process, transactions positioned in close proximity are discerned, and their midpoint vector, denoted as R, is computed via an averaging process, precisely characterized by

$$R = \text{floor}\left(\frac{X+Y}{2}\right)$$

where X and Y embody distinct transaction points, ensconcing a rarefied nature that mitigates duplication over an extended period.

Leveraging R as a pivotal axis, the SVP algorithm is enacted, culminating in the extraction of the Shortest Vector point (SVp) for R. This SVp ascends to the status of the root for the ensuing transaction subtree. By iteratively perpetuating this algorithmic process, successive subtrees are aggregated into higher-level structures, ultimately leading to the generation of an N-dimensional binary tree within the lattice.

The preeminence of the SVP algorithm rests upon its innate resistance to quantum-based adversarial incursions, particularly in high-dimensional spaces. By adopting the SVP paradigm for N-dimensional Merkle tree generation, we ensure an impregnable fortification against the potential encroachments of Quantum Computers, reaffirming the unassailable integrity and security of the Merkle tree structure.

C. *SVp as a hash equivalent*

The SVP algorithm leverages lattice mappings to identify the smallest linear combination of basis vectors that corresponds to a point nearest to the given point. This inherent property aligns with the essence of hash functions – **effective representation of underlying data** while maintaining compactness. Much like traditional hash functions consolidate information, the SVp of R captures the unique characteristics of transactions, akin to a hash at the root of a subtree.

The SVp's distinctive nature stems from the **inherent uniqueness** of the R vector. As R is derived from a specific pair of transactions, each SVp is distinct, thereby ensuring the representation of subtrees is both unique and unambiguous. This characteristic mirrors the **collision resistance** property of hash functions, where no two SVps can be identical due to their origin in unique transaction pairs.

The function f() seamlessly transforms transactions of varying sizes, along with their associated metadata, into **precise lattice coordinates**. Through truncation, the SVp is intentionally structured to encompass coefficients across all dimensions. The amalgamation of SVp and f() guarantees a **uniform output length** for varying transaction sizes, mirroring the standard behavior of hash functions.

Crucially, the SVP algorithm, coupled with the lattice mapping function f(), imparts the SVp with the property of **pre-image resistance**. An attacker's attempt to reverse-engineer the underlying subtree from the SVp is computationally daunting. The inability to deduce transaction specifics from the SVp adds a layer of security akin to the **one-way property** of traditional hash functions.

The SVp's immunity to pre-image attacks is further solidified by the distinctiveness of R and the infeasibility of introducing alternate points to reproduce the same SVp. The unique mapping of R, even in an N-dimensional lattice, prevents attackers from crafting alternative points that lead to identical SVps.

In essence, the SVp emerges as a **quantum-resistant equivalent** to conventional hash functions. Its properties, inherited from the SVP algorithm and lattice mapping, establish it as a robust representation of subtrees within the N-dimensional binary tree framework.

D. *Optimal Spraying*

In the process of N-dimensional Merkle tree construction, achieving network-specified dimensions necessitates a strategic approach known as optimal spraying. This phase involves two key steps to align the tree's structure with predefined difficulty criteria.

Firstly, the network establishes the difficulty level, dictating the desired dimensions and coefficients for non-zero coefficients in the final Merkle tree. This selection can encompass contiguous dimensions, specific extremes, or a combination, reflecting diverse consensus requirements. Higher difficulties may even mandate precise co-efficient values, further challenging miners.

Secondly, to transform the existing tree into the prescribed dimensions, miners introduce miner dummy transactions (m-transactions). Unlike the immutable nonce dummy transactions (n-transactions), m-transactions grant miners the flexibility to strategically position them within the lattice. Each m-transaction serves as a pivot point, steering the tree towards the desired dimensions.

Miners can introduce multiple m-transactions, though the optimization strategy is vital. Optimization involves deciding whether to experiment with different m-transaction placements or to commit m-transactions and generate new pivots. A miner's prudent choice balances computational resources with accuracy. Brute-force techniques, ubiquitous in Proof-of-Work, give way to more strategic and resource-efficient optimization strategies in PoQuVe.

Iterative steering continues until the root Shortest Vector Point (SVp) of the entire tree is achieved, aligning with the network's difficulty-defined specifications. Notably, the skewed structure, introduced by m-transactions, serves solely to meet difficulty criteria, safeguarding the integrity and security of the transaction tree.

Optimal spraying exhibits miner-driven adaptability and resource-consciousness, contrasting with the deterministic monotony of Proof-of-Work. The miner's role shifts from exhaustive linear search to fine-tuning mappings within the lattice, embodying a dynamic and intricate process that embraces the complexity of quantum-resistant verification.

E. *Verifier's Roles and Responsibilities*

Verifiers are essential to ensure the reliability of the block chain network. Unlike traditional PoW setups where verification is simplistic and miners can easily seek alternate verification, our protocol necessitates verifiers to invest computation power in calculating the root node Shortest Vector point (SVp). This added complexity demands a unique incentive structure to motivate verifiers to participate actively in the verification process.

Without incentivizing verifiers, the block chain network risks disruption, as insufficient participation in the verification process could lead to potential vulnerabilities. Recognizing this, our protocol distinguishes verifiers as distinct entities and offers incentives to encourage their engagement in verifying N-dimensional Merkle trees.

Participation as a verifier is open to any entity within the block chain network possessing the requisite computational capacity. This open-entry approach fosters a free market for verification roles. Importantly, entities in the network must choose to fulfill either the role of a verifier or a miner, and cannot vacillate between the two.

Verifiers are held to stringent ethical standards to ensure the trustworthiness of the verification process. Engaging in malicious activities is met with severe consequences, including potential permanent suspension from the block chain network. This ensures that verification remains a robust and dependable process, safeguarding the integrity of the entire network.

In our protocol, a clear demarcation exists between verifiers and miners, and once an entity assumes the role of a miner, transitioning to a verifier, or vice versa, is not permissible. This demarcation safeguards against fluid role changes and maintains the distinct identities of miners and verifiers. The relationship between miners and verifiers is structured in a manner where the actions of each group act as counterbalances to the other, effectively thwarting the potential for dominance by any single entity.

Miners remain uninformed about the specific verifiers responsible for authenticating their N-dimensional Merkle trees, and conversely, verifiers remain unaware of the identity of the miners whose trees they are scrutinizing. This intentional separation and anonymity uphold the integrity of the verification process and prevent collusion between miners and verifiers. The protocol's stringent enforcement of these distinctions serves to reinforce the autonomy of miners and verifiers as separate, independent entities within the network.

The primary role of a verifier centers on meticulously verifying the validity and integrity of the N-dimensional Merkle tree. To facilitate this process, miners provide verifiers with the SVp of the transaction tree, alongside details of dummy transactions' coordinates and depth. Critically, the verifier is not privy to the specific transactions composing the N-dimensional Merkle tree, preserving the anonymity of these transactions.

F. Quorum Broadcasting

Upon the completion of tree generation by a miner, a pivotal phase commences with the initiation of a broadcast message. This message extends an invitation to all verifiers within the network, summoning their participation in a quorum for the verification process. The quorum, comprising a cohesive assembly of k entities, undertakes the critical task of rigorously examining the miner's N-dimensional Merkle tree. Dynamic and consensus-driven, the quorum's size adapts to the ever-fluctuating landscape of verifiers within the network.

The miner's call to action triggers a synchronized response, as verifiers join the quorum in readiness for the impending verification process. The initiation of the quorum is intricately aligned with the complexity of the basis utilized by the miner. A dynamically determined time period is allocated to the quorum for operation, wherein its constituents engage in the verification and casting of votes. A definitive timeline governs the quorum's activities, terminating under specific circumstances:

A)The quorum exhausts its allocated time span before achieving full participation and voting.

B)All members of the quorum complete the verification process well before the designated timeout.

C)A rival quorum successfully concludes the verification of a comparable block within a shorter time frame and with a more substantial positive consensus.

Verifiers are empowered to compute within the stipulated timeout duration. In instances where a verifier concludes computations ahead of schedule, voting is permissible, yet withdrawal from the quorum awaits the collective verification completion or the elapse of the quorum timeout. Following exit, a designated cooldown period ensues before the verifier can reengage with a subsequent quorum. This cooldown intermission, coupled with the binding of quorum timeout, deters excessive computation from verifiers and upholds the equilibrium of the network.

Significantly, the quorum's time frame is unaffected by the volume of dummy transactions integrated by the user. Instead, it is exclusively determined by the intricacy of the underlying basis and dimension-related complexities. Notably, the network refrains from regarding an influx of m-transactions as a credible measure of complexity. Rather, it emphasizes that a poorly structured, skewed N-dimensional Merkle tree emerges from imprudent miner choices, which may not necessarily signify arduous tree generation.

While configuring verifiers within the quorum, meticulous attention is accorded to their individual computational indices. This index, indicative of their computational prowess, guides verifiers to quorums best suited to their capabilities. This careful matching prevents needless participation in overly complex quorums that could undermine reward prospects or joining quorums that fail to challenge their capacity.

Simultaneously, miners orchestrate the initiation of a quorum, harnessing their computational index to strategically select the quorum's type. This decision balances potential rewards against the risk of heightened participation or prolonged timeout, thereby shaping their optimal quorum strategy.

While alignment with proportionate quorums ensures equity among verifiers, the prospect of heightened rewards incites verifiers to ascend the computational index ladder. Elevated participation in more challenging quorums necessitates a collateral stake, augmenting as quorum complexity intensifies. Triumph within these higher tiers warrants stake retrieval, enhanced rewards, and continued access to equivalent quorums with reduced stakes.

Unsuccessful verification invokes the forfeiture of stakes, while instances of suspected leeching trigger penalties, including compensation for quorum members' costs. This disincentive fosters a judicious approach to quorum selection, discouraging undue risk-taking by verifiers.

Scaling computational capacity can empower verifiers to access higher quorums, indicating readiness for heightened responsibility. While occasional deviations are permitted, preserving one's current index aligns with the balance between scaling and retaining benefits.

Quorum size remains a steadfast metric, resisting dynamic shifts with increases in verifier numbers. Dilution of individual rewards is circumvented, fortifying verifiers' incentives and maintaining a sustainable network framework. This design safeguards against network degradation and strives for a consistent rewarding experience.

Amidst potential variations in verifier count, quorum dimensions adjust only when the ratio of valid, consistent verifiers escalates by a predefined factor. This rescaling signifies an augmented involvement of committed entities, triggering quorum expansion to amplify security and efficacy. Correlatedly, declining stakes accompany the proliferation of reliable verifiers, motivating long-term commitment and bolstering block chain security.

G. *Verification Process*

The verification process unfolds through a series of well-defined stages, ensuring the robustness and validity of the miner's N-dimensional Merkle tree. At each stage, the **local (or quorum) management entity**, the entity managing the quorum orchestrates the distribution of essential attributes to participating verifiers, facilitating a meticulous validation process. The process encompasses the following key stages:

1. **M-Transaction Verification**: Verifiers meticulously examine the introduced m-transactions, ensuring their authenticity and role in steering the transaction tree. This step involves verifying that the miner's steering elements are indeed m-transactions, vital for accurate tree construction. The management entity efficiently discloses m-transaction details, promoting transparency and safeguarding against deceptive practices.

2. **First SVp Verification**: During the distinct optimal spraying phase, verifiers meticulously scrutinize the precision of the initial Shortest Vector point (SVp) calculation, separate from the tree creation process. Operating under the constraint of no direct access to the transaction tree, verifiers possess the transaction tree's SVp and its initial parent SVp—derived during the optimal spraying interval.

By leveraging the m-transaction situated at the greatest depth, the verifier computes the first parent SVp, subsequently contrasting it against the obtained parent SVp. This critical step assesses the miner's precision in SVp generation. Deviations from the expected outcome prompt the imposition of penalties, the gravity of which escalates proportionally with the extent of SVp divergence.

3. **Final SVp Verification**: Verifiers meticulously rebuild the steering tree, the tree that steers the transaction tree to the desired dimensions, before obtaining the final SVp, calculating and comparing it with the miner's provided value. The management entity ensures the anonymity of the miner by disseminating the final SVp details. Verifiers confirm the accuracy of the final SVp and compare it against the stored SVp, affirming consistent SVp generation by the miner. Inaccuracies prompt penalties, proportional to the degree of deviation.

4. **Network Constraints Verification**: Verifiers rigorously validate the dimensions of the final SVp against network-specified constraints. The management entity supplies necessary data, allowing verifiers to assess compliance with fundamental requirements. Discrepancies trigger penalties, reinforcing the adherence to network constraints. Repeated violations result in escalated penalties, and consistent offenders may face suspension from future quorums.

5. **Voting and Consensus**: Verifiers engage in a final voting process, collectively determining the miner's block validity. Penalties are applied for contraventions, discouraging malicious activities and promoting quorum integrity.

Upon successful verification, verifiers transmit a **TrueVote** message, signifying the validation's success.The management entity's role extends to tallying votes and executing consensus. A majority of TrueVote messages confirms the miner's compliance with network expectations, culminating in quorum closure. On successful completion of the quorum's activity, the management entity initiates a diligent examination, scrutinizing the absence of prior blocks with equivalent or higher vote percentages. If no such competing blocks are detected within the quorum pool, a decisive blocking message is disseminated. This message effectively suspends quorums engaged in verifying similar transaction blocks, efficiently optimizing resource utilization.

Following this suspension, the miner is promptly notified of their verification success, and their block is appended to the block chain. The subsequent phase entails the equitable distribution of mining rewards among successful miners and verifiers, cementing collaborative efforts.

To ensure an inclusive reward allocation, successful participants – both miners and verifiers – observe an extended cooldown period. This interlude accommodates a broader spectrum of miners and verifiers, promoting a balanced and participatory block chain ecosystem.

Throughout each stage, the management entity ensures seamless attribute distribution, fostering a secure and efficient block chain environment while deterring violations through a graduated penalty framework.

H. *Reward distribution*

Unlike conventional block chain systems that exclusively reward miners, our approach involves equitable distribution of rewards between miners and verifiers, fostering a balanced ecosystem and preventing wealth centralization.

A pivotal question arises: Why would miners agree to share their rewards? The imminent advent of quantum computers poses risks to conventional protocols. Our solution addresses these concerns by incentivizing miners to adapt. While miners receive a greater portion of the reward, verifiers also play a crucial role, ensuring a robust network. This symbiotic relationship motivates miners to embrace the protocol to remain relevant in the evolving landscape.

As verifier computation indexes increase, their rewards grow. Opting for higher index quorums increases verifier rewards at the expense of miner's share. However, miners selecting lower index quorums risk time inefficiencies. If another miner successfully mines a similar block sooner, the victorious miner and their quorum claim rewards, rendering halted quorums unrewarded. Hence, rewards aren't guaranteed to all miners and verifiers.

This dynamic prompts miners to balance verification time and reward allocation while optimizing tree structures and selecting optimal quorums. Verifiers similarly strategize, choosing higher indexes for enhanced rewards. The counteracting goals of miners and verifiers maintain competitiveness, preventing collusion.

Two vital metrics, **Miner Power Index (MPI)** and **Verifier Power Index (VPI)**, are publicly accessible to foster competition. MPI reflects average miner computation power, allowing verifiers to gauge miners' scaling. Conversely, VPI reveals average verifier computation power to miners, aiding informed scaling decisions.

To avoid verifier dominance, VPI is capped below MPI. This safeguard maintains a balanced ecosystem. Verifiers' scaling must align with miners to ensure network stability. The ongoing push and pull between growth and limitation ensure competitiveness and prevent monopolies.

Considering quorums k1, k2, and k3, where k1 >> k2 >> k3, rewards distribution varies. Quorum K1, with the highest index, receives 80% of the total reward whilst K2 receives 50% and K3 at 20%. Table1 shows the reward distribution for every miner and verifier in that quorum if x is the amount of BTC received for every successful mining operation and N is the size of the quorum.

TABLE I
REWARD DISTRIBUTION IN POQUVE

Quorum Index	Reward per verifier (BTC)	Reward per miner (BTC)
K1	0.8x/N	0.2x
K2	0.5x/N	0.5x
K3	0.2x/N	0.8x

For verifiers transitioning from K3 to K1 ,there is a substantial increase in rewards(300% increase), illustrating the importance of scaling.

Loyal, consistent verifiers are also rewarded for steadfast contributions, particularly those in smaller index quorums. This acknowledges their dedicated effort and provides stability, indicating that scaling is not the sole motive for greater rewards. Rewards are sourced from lost staking on higher index quorums. A **global management entity** manages a reputation list, assigning rewards based on performance and consistency, incentivizing verifiers' loyalty. Consistent verifiers in lower quorums receive larger rewards than verifiers in higher quorums. This counterbalances the increased reward that higher quorums already get due to their greater computation capabilities.

Philanthropic miners and verifiers can contribute to a reward pool, fostering cooperation and an inclusive behavior. Distribution is discreet, preventing biases. These dynamics together promote a dynamic and competitive ecosystem, aligning miners' and verifiers' goals while discouraging collusion.

This approach ensures equitable rewards for miners and verifiers, maintaining balance, promoting competitive growth, and safeguarding network security. With the rise of quantum computers, this cooperative framework paves the way for a resilient block chain future.

IV. Mitigating Wealth Disparity and Ensuring Decentralization

The prevailing issue of wealth accumulation within conventional block chain networks, favoring a select group of miners, has ignited concerns about centralization and imbalanced distribution of assets. Our innovative protocol addresses this challenge by introducing measures that promote equitable rewards and prevent centralization, ensuring a balanced and competitive network.

In our approach, both miners and verifiers are recipients of rewards. Verifiers have unrestricted entry and exit, receiving consistent rewards evenly distributed across entities over extended periods. Although miners still command a substantial share of rewards, our protocol introduces variability. The distribution of rewards to miners deviates from the uniform pattern observed in existing crypto currency systems [13].

Similarly, verifiers enjoy steady, consistent rewards over time. Although their immediate gains may not parallel those of miners, the cumulative effect ensures a more proportional distribution of wealth over the long term.

Crucially, our protocol dismantles the notion of the rich becoming richer. It provides every entity with a fair chance to grow and reap rewards for their contributions. Vigorous penalties for malicious behavior further underscore the protocol's commitment to maintaining a fair ecosystem. Decentralization plays a pivotal role in addressing these concerns.

A highly decentralized network prevents dominance or monopoly, fostering a competitive landscape where participants vie for rewards. The multitude of entities competing within this framework averts concentration of wealth in a few hands, fostering a robust and fair environment.

This brings us to a crucial question: Does our protocol genuinely promote decentralization? Does it effectively incorporate the principles of a free, fair, and competitive market to mitigate wealth disparity?

Absolutely. Our protocol champions decentralization and introduces an innovative concept of investing in computation power to underpin its principles. Miners gravitate towards optimal quorums, where they strike a balance between reward allocation and verification efficiency. This behavior results in verifiers clustering around an optimal point.

Majority of verifiers cluster to this center by either scaling up or scaling down, to meet the demands of the miners. The proportion of entities who have very little computation power and very significant computation power form a very small part of the verifier population. Based on this nature of distribution, we believe that this protocol will foster a Gaussian distribution w.r.t verifiers.

Notably, this Gaussian distribution doesn't indicate centralization. It underscores a vibrant and competitive market with entities clustering around the optimal quorum mean. This equilibrium state reflects balanced competition, where quorums compete fervently to mine blocks and claim rewards. The intense competition at this optimal point averts centralization, exemplifying a thriving, decentralized network.

Moreover, our protocol's adaptability to changes preserves the decentralized nature. Verifiers and miners exhibit varying scaling behaviors, causing shifts in the Gaussian curve. Scaling up or down doesn't alter the curve's inherent structure, reinforcing the protocol's enduring decentralization.

By embracing this protocol, miners occupy a diverse spectrum. Their optimal behavior spans from non-optimal to exceptional, ensuring a continuous equilibrium between optimization and difficulty. The protocol effectively curtails the risk of centralization by ensuring a balanced distribution of rewards and fostering a dynamic, competitive landscape.

V. Agent-Based Simulation results

To thoroughly validate our hypothesis concerning the reduction of wealth disparity, we conducted an agent-based simulation comparing the conventional Proof-of-Work (PoW) mechanism with our innovative Proof-of-Quantum Verification protocol (PoQuVe). Through this simulation, we aimed to substantiate our claims and empirically demonstrate the significant enhancement in wealth distribution achieved by our protocol.

In the PoW model, we established a representative scenario in which miners constituted a mere 2.5% of the entire network, amounting to 50 miners within a pool of 2000 entities. These miners were rewarded with 1 BTC for each successful mining activity. To quantify wealth disparity, we employed the Gini index, defined by the formula:

$$\text{Gini index} = \frac{\sum_{i=1}^{n} (2(i+1) - n - 1) \cdot x_i}{\sum_{i=1}^{n} x_i \cdot n}$$

where x_i denotes the wealth (BTC in this case) held by entity i , and n denotes the total entities in the network.
Here, a Gini index of 0 signifies perfect wealth equality, while an index of 1 indicates extreme wealth concentration. By conducting multiple rounds of simulated-mining, we traced the Gini index's trajectory over time. Remarkably, within the PoW model, the Gini index exhibited marginal reduction, ultimately plateauing at a substantial value of 0.97718. This stagnant trend underscored the pronounced wealth disparity inherent in traditional PoW systems.

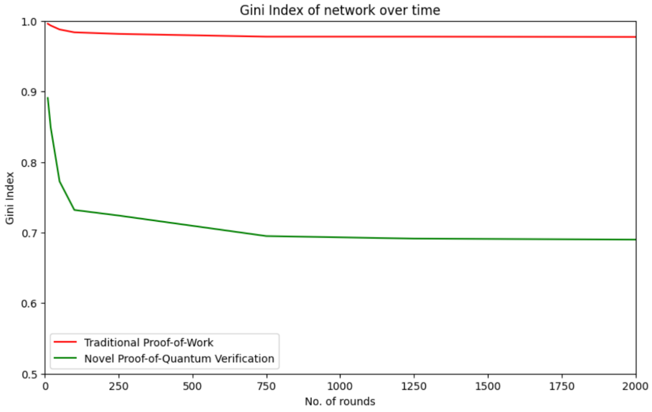

Fig. 1. Expected verifier distribution in PoQuVe

Transitioning to our proposed protocol, we engineered a simulation featuring randomized quorums, each composed of 310 verifier entities. We created five distinct quorums, assigning unique random reward percentages to each. The size of verifiers selected for verification was fixed at 62, equivalent to 20% of that verifier index quorum. In this context, miners dynamically selected quorums with varying reward percentages (20%, 30%, 50%, 60%, 80%) for collaboration. The resultant rewards were judiciously distributed among participating verifiers and the miner whilst 400 regular entities were retained as is.

Our simulation yielded a striking departure from the PoW model. The Gini index under our Proof-of-Quantum Verification protocol experienced a substantial reduction, ultimately converging to 0.69001, as can be observed in Figure 1. This reduction of approximately 0.3 units emphatically demonstrated the protocol's significant positive influence on wealth distribution. Moreover, we emphasize that our simulation featured solely randomized quorum parameters, excluding nuanced considerations such as scaling dynamics. We confidently anticipate even more promising outcomes upon fine-tuning parameters to precisely align with the comprehensive protocol framework.

While achieving an exceptionally low Gini index (e.g., < 0.5) within block chain networks remains a formidable challenge, we emphasize that our protocol succeeds in meaningfully mitigating wealth disparity and eliminating wealth monopolization. The dynamic interplay between miners and verifiers, coupled with randomized quorum configurations, contributes to a competitive and decentralized ecosystem. By robustly addressing wealth disparity while maintaining a competitive environment, our protocol introduces a new paradigm in block chain dynamics and establishes a compelling precedent for equitable wealth distribution.

In order to deepen our comprehension of the model and protocol devised, we opted to construct a comprehensive portrayal through the plotting of distinct scenarios: the optimal, worst, and average case scenarios, which collectively unveil the spectrum of attainable Gini Indexes within the protocol.

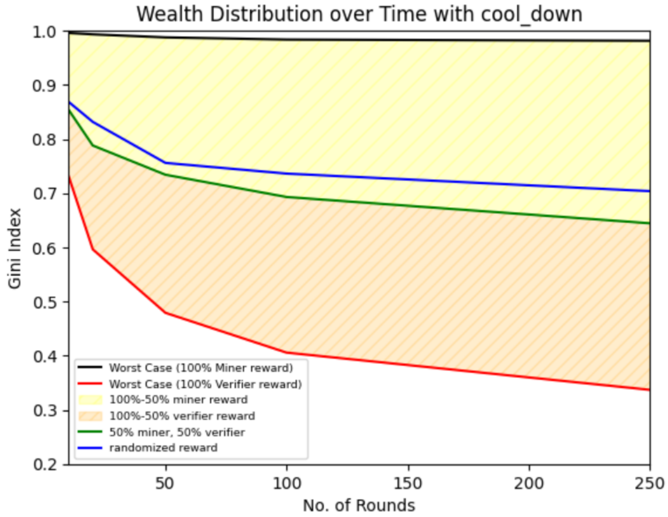

Fig. 2. Best case, Worst case and Average cases for Gini Index in PoQuVe

Firstly,we addressed the direst circumstance, in which the miner reaps the entirety of the rewards—a scenario reminiscent of the traditional Proof-of-Work (PoW) framework. In this instance, the Gini Index remains consistent with prior observations. Conversely, a contrasting extreme presents itself when verifiers exclusively receive the rewards, totaling 100%. Remarkably, the Gini Index, in this particular case, plummets to an impressively low value of 0.33693. While this outcome holds economic allure, it proves unrealistic within the context of a block chain network, as the essential role of the miner's computational efforts remains uncompensated. Thus, these worst-case scenarios function as crucial bounds that establish the outer parameters for the potential Gini Index.

Contrastingly, the best-case scenario unfolds when both the miner and the verifier equally partake in the rewards, each receiving 50%. While the Gini Index refrains from plummeting to 0.5 due to the division of verifier rewards among numerous entities (in contrast to the miner's exclusive reward acquisition), it still approximates the midpoint of this range. Notably, the best and worst cases shape the extremities, wherein the best case occupies intermediate position.

Ascertaining the average case scenario entails the miner's random selection of various quorums for verification—thus forging a blend of reward distribution proportions that transcend the binary extremes of 50% and 100%. This scenario, depicted by the blue curve, closely aligns with the best case line. Evidently, as the intricacies of all requisite parameters are systematically assimilated, the average case is anticipated to further converge towards the best case. The delineations marked by the orange and yellow regions underscore zones of potential curve fluctuations, ranging from 100% miner rewards to a balanced 50% distribution between miner and verifier, and finally, to 100% verifier rewards.

All of these data entries obtained for Figure 2 are obtained by modifying our original model to introduce a fixed cooldown time, that is set to 5 mining rounds. The primary reason for selecting that number is that, we considered the quorum size to be 20% of the verifier index size. Setting the cooldown to 5 ensures that a particular verifier only reaps rewards after everyone else in that index has got a chance to obtain rewards.

Intriguingly, the proximity of the random case curve to the best case line underscores a high degree of alignment between these two scenarios within our protocol. This observation serves as a constructive validation of our protocol's Gini Index outcomes, reinforcing its potential to engender substantial wealth distribution. In totality, these diverse scenarios provide comprehensive insights into the efficacy and redistributive potential of our protocol, affirming its capacity to mitigate wealth disparity and establish a dynamic equilibrium within block chain networks.

VI. Computation Power as an Investment

The landscape of technology is constantly evolving, with increasing computation power emerging as a pivotal asset for the future. Just as gold and stocks hold value today, this paper introduces the paradigm of investing in computation power as a valuable future asset. The proposed concept aligns with a free market model for verifiers, incentivizing entities to engage in verification and invest in computation power. This participation grants verifiers consistent, long-term rewards while adapting to network dynamics.

Drawing an analogy to stocks, verifiers seek greater rewards, motivating them to invest in computation power by scaling up to higher index quorums, akin to buying when stock prices rise. Conversely, when miners favor lower index quorums, verifiers scale down, resembling selling during stock price declines.

The model introduces a dynamic investment approach, shaping a more equitable and competitive landscape for future technological advancements.

VII. Future Work

Our future endeavors will delve into a comprehensive exploration of the underlying Gaussian distribution dynamics within the network. Additionally, we plan to establish a rigorous mathematical framework to quantify the efficacy of the SVp. To advance the protocol's practical implementation, we aim to devise an optimized architectural scheme. Furthermore, an in-depth analysis will be conducted to discern the intricate balance between security enhancements and the temporal efficiency of block mining.

VIII. Conclusion

In conclusion, our novel Proof-of-Quantum Verification protocol presents a promising avenue for addressing quantum threats, wealth disparity and centralization issues in block chain networks. By introducing a dynamic equilibrium between miners and verifiers, we create a competitive and decentralized ecosystem. The concept of investing in computation power as a future asset offers opportunities for sustained growth and application across diverse domains.

References

[1] Wasim Wahid,"An analysis of the impact of quantum computing on consensus algorithms and the security of blockchain networks," *International Journal of Cyber Criminology*,vol. 01, Jan. 2023,

[2] N. Kappert, E. Karger, and M. Kureljusic, "Quantum Computing - The Impending End for the Blockchain?", in *Proceedings of the International Conference on Computer Science and Technology*, June 2021.

[3] K. Venu and B. Krishnakumar, "Challenges and Research Perspective of Post–Quantum Blockchain", in *Advances in Computers and Communication Engineering*, pp. 127-172, July 2022.

[4] H. Bennett, "The Complexity of the Shortest Vector Problem", *ACM SIGACT News*, vol. 54, pp. 37-61, February 2023.

[5] S. Velliangiri and P. Karthikeyan, "Blockchain Technology: Challenges and Security issues in Consensus algorithm," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*,

[6] Dan A. Bard, Joseph J. Kearney, and Carlos A. Perez-Delgado, "Quantum Advantage on Proof of Work," arXiv preprint arXiv:2105.01821, 2021.

[7] Daniel Yost, "Lattice-Based Cybersecurity In the Quantum Era: An Exploration of the Future's Security," May 15, 2020.

[8] Daniele Micciancio and Oded Regev, "Lattice-based Cryptography," July 22, 2008.

[9] Ashish Rajendra Sai, Jim Buckley, Brian Fitzgerald, and Andrew Le Gear, "Taxonomy of centralization in public blockchain systems: A systematic literature review," *Information Processing & Management*, vol. 58, no. 4, pp. 102584,2021,

[10] Ashish Rajendra Sai, Jim Buckley, and Andrew Le Gear, "Characterizing Wealth Inequality in Cryptocurrencies," *Frontiers in Blockchain*, vol. 4,2021,

[11] Yael Eisenberg, Itamar Rot, and Muli Safra, "On the Shortest Lattice Vector vs. the Shortest Basis," arXiv preprint arXiv:2305.19777, 2023.

[12] P. Shrivastava, K. K. Soni and A. Rasool, "Evolution of Quantum Computing Based on Grover's Search Algorithm," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944676.

[13] B. Kusmierz and R. Overko, "How centralized is decentralized? Comparison of wealth distribution in coins and tokens," 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS), Barcelona, Spain, 2022, pp. 1-6, doi: 10.1109/COINS54846.2022.9854972.

[14] Nikos Leonardos, Stefanos Leonardos, and Georgios Piliouras, "Oceanic Games: Centralization Risks and Incentives in Blockchain Mining," in *Mathematical Research for Blockchain Economy*, Springer International Publishing, 2020, pp. 183–199, isbn: 978-3-030-37110-4.

[15] Qinwei Lin,Chao Li, Xifeng Zhao,and Xianhai Chen, School of Computer and Information Technology, Beijing Jiaotong University, China, Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, China, arXiv:2101.10699v2 [cs.CR], 2 Feb 2021.

[16]] Chao Li and Balaji Palanisamy. Comparison of decentralization in dpos and pow blockchains. In International Conference on Blockchain, pages 18–32. Springer, 2020.

[17] Gochhayat, Sarada & Shetty, Sachin & Mukkamala, Ravi & Foytik, Peter & Kamhoua, Georges & Njilla, Laurent. (2020). Measuring Decentrality in Blockchain Based Systems. IEEE Access. 8. 10.1109/ACCESS.2020.3026577.

[18] J. Niu, F. Gai, R. Han, R. Zhang, Y. Zhang and C. Feng, "Crystal: Enhancing Blockchain Mining Transparency with Quorum Certificate," in IEEE Transactions on Dependable and Secure Computing, 2022, doi: 10.1109/TDSC.2022.3216749.

[19] G. A. F. Rebello, G. F. Camilo, L. C. B. Guimarães, L. A. C. de Souza and O. C. M. B. Duarte, "Security and Performance Analysis of Quorum-based Blockchain Consensus Protocols," 2022 6th Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 2022, pp. 1-7, doi: 10.1109/CSNet56116.2022.9955597.