SoK: Is Proof-of-Useful-Work Really Useful?

Pratyush Dikshit[1][0000−0001−6617−2831], Ashkan Emami[1][0000−0002−3378−2921], Johannes Sedlmeir[2][0000−0003−2631−8749], and Gilbert Fridgen[1][0000−0001−7037−4807]

[1] University of Luxembourg, Luxembourg
[2] University of Munster, Germany
{pratyush.dikshit,ashkan.emami,gilbert.fridgen}@uni.lu
{johannes.sedlmeir}@uni-muenster.de

Abstract. Proof-of-work (PoW)-based consensus mechanisms have long been criticized for their high resource (electricity, e-waste) consumption and reliance on hash puzzles which have no utility beyond cryptocurrencies [84]. Proof-of-Useful Work (PoUW) has emerged as an alternative whose mining objective is expected to provide societal utility. Despite numerous designs, PoUW lacks practical relevance and theoretical scrutiny [10]. In this paper, we provide a systematization of knowledge (SoK) on PoUW, focusing on security-economic trade-offs. We build the taxonomy to discuss core principles (difficulty adjustment, verifiability, etc.), architecture, trade-offs, and economic incentives. We examine more than 50 PoUW constructions where we find recurring shortcomings. We introduce a formal economic model of PoUW for miner incentives, solution reusability, and external market value to the security budget. To validate our hypothesis, we employ a Toulmin-based evaluation of claims on the security and energy efficiency of these constructions. Our finding show that PoUW is actually **not** as useful as expected, since the economic and societal utility do not contribute to the security budget. Finally, we highlight design recommendations for PoUW that integrate verifiable computation, partial incentive allocation, and utility-aware difficulty adjustment.

Keywords: Proof-of-Useful Work · Taxonomy · Security Budget

1 Introduction

Traditional Proof-of-Work (PoW) has long been scrutinized for consuming substantial energy to secure permissionless blockchains while performing easily verifiable but non-useful tasks [84,114,13]. In this regard, significant research has been done to utilize the computation of PoW to perform meaningful work. A particularly appealing mechanism is Proof-of-Useful Work (PoUW), which seeks to repurpose computational effort for valuable tasks for the real world, such as optimization, machine learning, or scientific simulations [55,36,95]. By design, PoUW aspires to simultaneously preserve the fair incentive structure and security properties of PoW while generating additional utility. Thus, PoUW gained traction as an alternative to PoW, and a large volume of articles has been dedicated to its application on social benefits [13,39,55]. While inspired by prior research on PoW and PoUW [16,13,114], we discuss the primary differentiation between PoW and PoUW with respect to the type of challenge (puzzle), its quality and randomness, time interval to add block in blockchain, redundancy in computation, and dependency on computing hardware in Table 1. We observe that PoUW struggles to generate fair and unbiased puzzles, to maintain uniform block time, and fails to address redundancy (see Section 2, 3).

As a result, despite more than a decade of proposals to utilize the "wasted energy", including Ofelimos [47], Primecoin (prime number chains)[65], Coinami (DNA sequencing) [60], CoinAI (deep learning) [11], and Proof-of-Solution (optimization), PoUW has not achieved large-scale practical deployment yet. We define the notion of "wasted energy" as energy is "wasted" if more money is spent on computing than the highest buy bidding amount of the solution. The key question remains unresolved: *can useful computation meaningfully contribute to the security budget of a blockchain, or does it merely repurpose energy without addressing the underlying economic-security foundations of PoW?* [55]. To answer this, we investigate the following research questions-

- **RQ1.** What are the dominant design classifications of PoUW mechanisms, and how do they differ from PoW in their approaches to security, economy, and efficiency?
- **RQ2.** To what extent do existing PoUW constructions offer a viable alternative to PoW in terms of security budget, incentive structure, energy consumption, and useful task generation?
- **RQ3.** What design dimensions are critical for future PoUW mechanisms?

This study is built on the argument that a computation is useful if someone is willing to pay for its solution in some external setting. A few research papers [91,118] have followed the same approach and designed systems that enable users to request real-world challenges that they need a solution to, and change the mining process to solve these problems. Though not all PoUW constructions permit user-uploaded challenges, some of the mechanisms let systems develop and distribute the challenges to the miners. To note, incentive and reward have been used interchangeably in the literature so far; to ease the readability and understanding, we use "incentive" in this paper.

Contribution. The systematization of knowledge on PoUW has been explored well beyond the literature review. We not only catalogue over 50 PoUW constructions, but also develop a four-layer taxonomy that exposes previously unarticulated trade-offs among core principles, architectural decisions, trade-offs, and incentive structures to understand the underlying characteristics and identify the dimensions of classical PoW, which influence the security, decentralization, and energy consumption. Building on this taxonomy, the study builds a formal economic model [40] in the form of a mathematical representation of PoUW to analyze the behavior, structure, and characteristics of PoUW, considering the economic structure and security budget while challenging the common assumption that useful computation automatically strengthens consensus. The connection between security and economic efficiency can be called `Security Budget`. In other words, the security budget is the cost involved in the potential successful attack on the main chain network. Further, the formal model is complemented with the Toulmin model for argumentation to evaluate claims of energy conservation, incentive structure, difficulty adjustment of the puzzle, and randomness in challenge assignment, making explicit where PoUW schemes fail to meet essential consensus guarantees, thereby identifying concrete research gaps and design levers for future protocols. Finally, we outline design recommendations for future PoUW protocols, emphasizing partial incentive allocation, the use of verifiable computation (e.g., succinct proofs), and utility-aware difficulty adjustment. While our findings unveil significant shortcomings in current PoUW mechanisms, they also highlight concrete design ideas that could guide the development of consensus mechanisms capable of combining blockchain security with social utilities. By combining comprehensive systematization with original economic analysis and security evaluation, this paper delivers the kind of novel insight, gap identification, and critical reassessment of the PoUW system.

Table 1. This table discusses the differences between PoW and PoUW consensus mechanisms

Categories	**Proof-of-Work (PoW)**	**Proof-of-Useful Work (PoUW)**
Puzzle/ Challenge	1. Cryptographic hash-based puzzle (e.g., finding nonce in Bitcoin mining) 2. The quality of the puzzle depends on the difficulty level and verification of the puzzle.	1. Computationally intensive tasks with real-world utilities - training machine learning models, protein folding, or weather simulations. 2. The quality of the puzzle impacts its utility. Poorly designed puzzles fail to provide a legitimate solution to a real-world problem.
Block Time interval	Block creation time is uniform, adjusted by the difficulty level. Particularly, block creation time is fixed (e.g., approx. 10 minutes for Bitcoin)	Depends on the complexity of the useful tasks, which vary in time duration to solve. Hence, this is challenging to maintain the fixed time for each block.
Randomness	The puzzle is uniform and designed for the purpose of fairness and randomness in mining.	The randomly generated useful task is the key purpose, by parameterizing the real-world challenge
Hardware	The nature of the puzzle is similar and hence do not require major hardware designing and architectural modifications.	The puzzles vary in nature and utilities and hence various kinds of hardware with different micro-architectural designing may be required.
Redundancy	Significant redundancy as several miners perform identical computations by solving the hash puzzle to compete for the incentive.	All miners consume energy for a useful task but only one gets the incentive. Hence, the energy consumption by the rest of the miners is wasted.

2 Related Work

In recent years, the wasteful energy consumption of blockchains, particularly Bitcoin, has been widely criticized worldwide. Several studies put forward the idea of adapting PoW to perform useful computations, aiming to improve energy efficiency while retaining its security properties [89,80,52,72,95] but failed to maintain the security budget. Moreover, to address controlling and maintaining the `difficulty` of the tasks provided to the miners, researchers proposed the optimization problem instances [79,81]. Later approaches included the justification of work done (similar to the PoW), e.g., Proof of Search [100], which

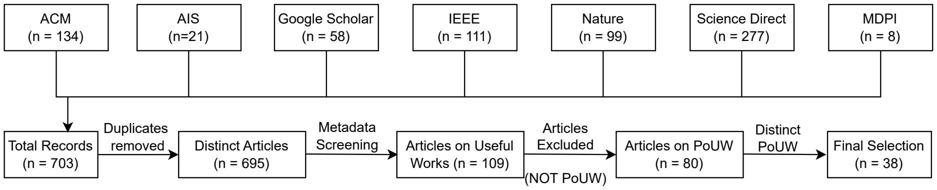


Fig. 1. Systematic Literature Review Process.

does not substantially seem useful as per PoUW. The details of existing studies are explained in the Appendix B.

Recently, Proof of Necessary Work (PoNW) was developed by Kattis et. al. [63]. PoNW is about replacing wasteful hash grinding with verifiable computations that the blockchain must perform anyway. Despite repurposing its usefulness, PoNW does not contribute to societal utility. Moreover, generating succinct proofs or complex state verifications requires highly specialized hardware and expertise, which demotivates the adoption. The most important point where PoNW lacks is the negligible demand for useful work in the external market. The miners will lose motivation if they do not foresee the possibilities of receiving even a partial incentive. Hoffmann [55] surveyed the existing projects that incorporate several theoretical, biological, and machine learning problems into the PoUW mechanism. The survey shows a *more usefulness, more challenge* phenomenon in the existing works. Dotan et al. [40] mathematically explain that the security of the system originates from the economic incentive, which is created by the demand for solutions to the real-world problems, but they lack fairness in the random assignment of the challenge to the miners. Cao et al. [24] claim that most existing studies rely on either specific problems or particular algorithms, and they lack comprehensive security analysis for optimization-based PoUW.

3 Literature Review: PoUW

We performed a hybrid search methodology for reviewing the literature in this study. We conducted a Systematic Literature Review (SLR) to gather the existing knowledge on the usefulness of several proposed PoUW mechanisms. The search was conducted for the published peer-to-peer articles from 7 different databases - IEEE Xplore, ACM Digital Library, Nature, Science Direct, AIS eLibrary (All repositories), MDPI, and Google Scholar for the time period of January 2015 to March 2025. The consolidated string is - *((("All Metadata":consensus OR DLT OR "Distributed ledger" OR blockchain) AND ("All Metadata":Useful Proof of Work OR PoUW OR (("All Metadata":"Proof-of" OR "Proof of") AND ("All Metadata":"useful task" OR "useful work")) OR ("All Metadata":PoX AND "useful")))).* We iteratively refined the query to capture synonyms and variants. Rather than presenting a single monolithic search string, which would not be executable across all databases, we document the representative keywords and logical operators to enable replication of our search logic on each database. Further, we did Snowballing [62] and wild card entries for the borderline research articles [115] to minimize the risk of missing primary studies on PoUW. This process encompasses identification, screening, eligibility assessment, and inclusion of sources to ensure rigor, which is quite similar to the method adopted by Bakshi et al. [10].

We realized that some articles address the useful work in consensus mechanisms such as Proof-of-Storage, but they are not computationally heavy like PoW, which harnesses the ability to solve real-world problems by replacing the random hash calculation. Hence, we excluded such articles from our study. Thus, we narrowed our search to look for PoUW only and got 80 articles. Inspired by [10], we expanded the horizon of classification. These articles are then classified into 12 categories *(Biomedical, Data Scheduling, Energy, EV, File-Storage System, Graph & Matrix, Intellectual Property, IoT, ML/AI, Optimization, Supply Chain, Uncategorised)* according to the useful work(s) performed, as shown in Figure 4, Appendix C. We observed that approximately 21% of the articles discussed the useful work in the domain of AI/ML, showcasing the inclination towards AI training models. Those PoUW that can be adopted in multiple use cases are classified as *Uncategorised PoUW.* Out of this set of articles, some articles solve the same real-world problem, e.g., the Travelling Salesman Problem, in different versions. Hence, we considered only the distinct articles addressing the same real-world problem. We have 48 research articles (38 from SLR + 10 from snowballing and wild card entry) on PoUW solving distinct real-world problem(s), of which we conducted an in-depth full-text analysis. The final list of articles is listed in Table 2, Appendix C.

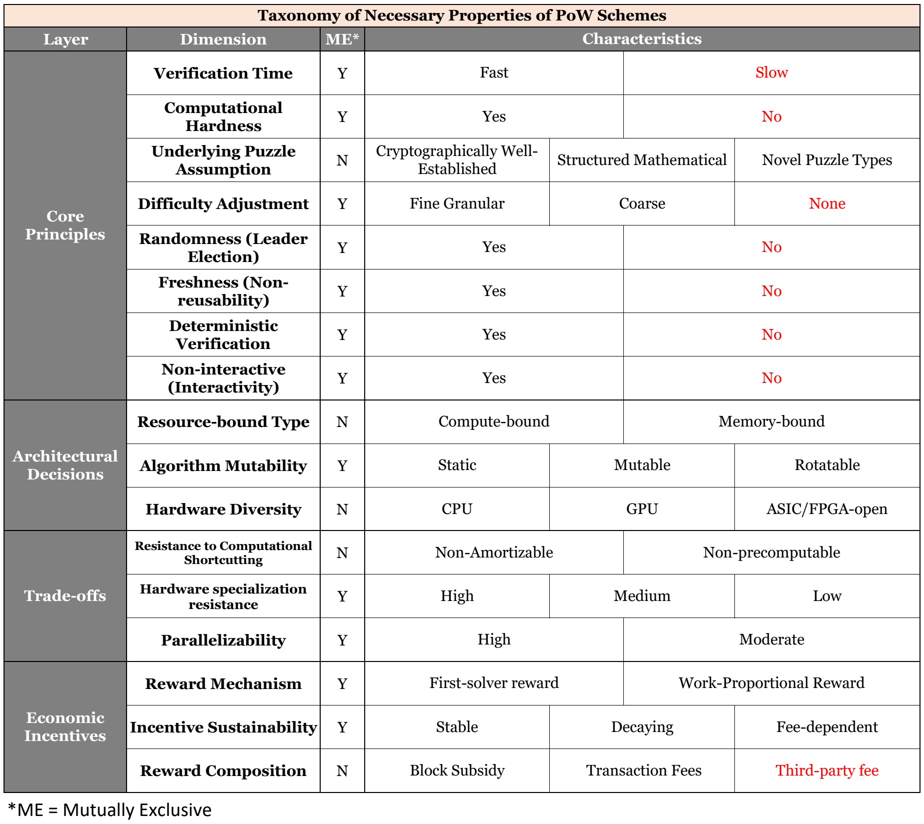
4 Taxonomy of PoW

As part of this research, we identify and classify how PoW operates across several real cryptocurrencies empirically. The purpose of the taxonomy is to identify which critical security and design factors are important in a PoW scheme in order to determine whether those factors have been successfully translated to PoUW schemes and where new vulnerabilities or compromises may arise. It is necessary to understand the viability of PoUW and to determine whether it is an adequate alternative to PoW.

Selection Method. As a first step in building the taxonomy, we examined practical PoW cryptocurrencies. From the list on CryptoSlate[3], we selected a subset of coins (see Table 3, Appendix D) and reviewed their technical documentation-whitepapers, mining algorithms, and difficulty rulesto derive the dimensions of our taxonomy.

Analysis Method. We analyzed the following key dimensions for each PoW scheme: (1) puzzle/work type, (2) difficulty adjustment method, (3) verification

[3] https://cryptoslate.com/cryptos/proof-of-work/



Taxonomy of Necessary Properties of PoW Schemes

Layer	Dimension	ME*	Characteristics		
Core Principles	Verification Time	Y	Fast	Slow	
	Computational Hardness	Y	Yes	No	
	Underlying Puzzle Assumption	N	Cryptographically Well-Established	Structured Mathematical	Novel Puzzle Types
	Difficulty Adjustment	Y	Fine Granular	Coarse	None
	Randomness (Leader Election)	Y	Yes	No	
	Freshness (Non-reusability)	Y	Yes	No	
	Deterministic Verification	Y	Yes	No	
	Non-interactive (Interactivity)	Y	Yes	No	
Architectural Decisions	Resource-bound Type	N	Compute-bound	Memory-bound	
	Algorithm Mutability	Y	Static	Mutable	Rotatable
	Hardware Diversity	N	CPU	GPU	ASIC/FPGA-open
Trade-offs	Resistance to Computational Shortcutting	N	Non-Amortizable	Non-precomputable	
	Hardware specialization resistance	Y	High	Medium	Low
	Parallelizability	Y	High	Moderate	
Economic Incentives	Reward Mechanism	Y	First-solver reward	Work-Proportional Reward	
	Incentive Sustainability	Y	Stable	Decaying	Fee-dependent
	Reward Composition	N	Block Subsidy	Transaction Fees	Third-party fee

*ME = Mutually Exclusive

Fig. 2. *Taxonomy of necessary properties of PoW schemes including core principles, architectural Decisions, Trade-offs, and Economic incentives, highlighting dimensions and characteristics with limitations.*

nature, (4) incentive mechanisms and sustainability, (5) resource binding (which resource is consumed by the work), and (6) resistance to shortcuts or hardware specialization. Hybrid schemes were discovered and removed from the pure-PoW classification. The classification was based on consensus among the authors in the case of uncertainties, which were cross-checked from multiple sources.

We categorize the required PoW dimensions into four levels: Core Principles, Architectural Decisions, Trade-offs, and Economic Incentives. As depicted in Figure 2, some characteristics are highlighted in *red*, which denote properties that are incompatible with pure PoW consensus schemes. They are included as negative flags: if a scheme exhibits any of these properties (e.g., slow verification, interactive proof verification, etc.), it fails one or more of the necessary principles of PoW (such as cheap deterministic verification, non-interactivity, native incentive alignment). This assists in identifying which characteristics are disqualifying a pure PoW scheme from a PoUW.

4.1 Core Principles and Foundation

The security of a blockchain, whether PoW or PoUW, rests on a set of core, non-negotiable principles. If any of the principles is violated, the scheme ceases to provide security guarantees.

Verification Time. Verification must be fast to maintain the asymmetry between expensive mining and quick validation [56].
Computational Hardness. The puzzle must be computationally infeasible to solve in a short period of time without significant resources [6]. Without this property, a malicious actor could rapidly generate new blocks, censor transactions [1], or perform a 51% attack [7] with minimal cost. The entire security model, which is based on the economic cost of mining, may collapse.
Underlying Puzzle Assumption. It is possible to categorize the assumptions that underlie the puzzle as Cryptographically Well-Established (e.g., SHA-256 preimage resistance [37]), Structured Mathematical (e.g., Equihash [19], memory-hard functions), and Novel Puzzle Types (less established).
Difficulty Adjustment. This dynamic regulator of PoW [90] ensures that the time to find a new block remains relatively constant, regardless of the total computational power of the network. In the absence of this adjustment, rapid block generation leads to chain instability, whereas low difficulty allows trivial forks and attacks, which can result in unpredictable block intervals that can disrupt transaction confirmation times, may lead to 51% attacks [7], selfish mining [97], and block incentives being distributed faster, which harms the coin supply [61,9,35,90].
Randomness (Leader Election). In PoW, the probability of winning a block must be proportional to the amount of work expended, and its absence would violate the principle of fairness [78].
Freshness. A puzzle solution must be bound to a specific block or challenge context and may not be reused or replayed in subsequent rounds [22]. As a result, each unit of work contributes uniquely to consensus and prevents adversaries from reusing existing proofs.
Deterministic Verification. The validity of any solution must be deterministically and cost-effectively verified by any node once it has been provided [94].
Non-Interactive. A miner, having solved the puzzle, can unilaterally present their solution to the network for validation [6]. This characteristic eliminates the need for complex, real-time communication protocols between miners, preventing network congestion and miners‘ collusion.

4.2 Architectural Decisions

Resource-Bound Type. It is possible to construct the puzzle in many ways: Compute-Bound, which relies on computational power (e.g., Hashcash) ; Memory-Bound, which relies on latency during memory access (e.g., Equihash [19]); and finally a combination of these methods [6]. This determines how mining is modeled and what type of hardware advantage can be obtained. The traction towards resource consumption is claimed as the primary appeal of PoUW, aiming to repurpose energy for a productive goal [10].

Algorithm Mutability. This relates to whether the underlying PoW puzzle remains fixed over time or not. Static schemes select a PoW function once and preserve it throughout the life of the chain (e.g., Bitcoin's SHA-256). While this may ensure stability and broad hardware optimization, it will also result in predictable hardware specialization and the eventual dominance of ASICs. By contrast, mutable schemes deliberately alter their PoW algorithms through scheduled hard forks or developer interventions. For instance, Monero has repeatedly changed its PoW algorithm to maintain CPU/GPU mining accessibility [92]. Some protocols adopt rotatable designs, where the system rotates among multiple PoW algorithms by design (e.g., DigiBytes multi-algo rotation [68]).

Hardware Diversity. This dimension captures the extent to which different classes of hardware (e.g., CPUs, GPUs, ASICs, FPGAs) can efficiently participate in mining. When hardware diversity is high, it promotes decentralization and enables broader participation. It is important to note that once ASICs become dominant, diversity collapses [64]. Thus, hardware diversity reflects both a protocol designers choice of target resource and a long-term factor shaping decentralization and security as hardware ecosystems mature.

4.3 Trade-offs and Emergent Properties

Resistance to Computational Shortcutting. This dimension is concerned with the shortcuts from being exploited by adversaries that reduce the intended computational cost of puzzles. Two key characteristics are required to protect against this exploitation. First is the negligible benefit from solving one puzzle, which makes it cheaper to solve additional puzzles called "Non-amortizable". Second is "non-precomputable", preventing miners from precompiling solutions in advance. This dimension reflects a trade-off in fairness and decentralization, highlighting how susceptible a scheme is to amortization or precomputation strategies that reduce the effective cost of mining.

Hardware Specialization Resistance. Hardware diversity and hardware specialization resistance are closely related but not identical. Diversity reflects an architectural decision regarding which hardware types the protocol seeks to support, whereas specialization resistance measures the emergent effectiveness of that choice over time[51]. For example, Monero deliberately targets CPUs and enforces this through periodic algorithm changes [20], sustaining high resistance. Bitcoin, conversely, is ASIC-dominated by design, with low resistance [108].

Parallelizability. Parallelizability refers to the ease with which the mining workload of the puzzle can be distributed across multiple processors or machines. High-parallel algorithms are more susceptible to efficiency gains associated with large-scale mining, leading to concentration of computing power [54,8].

4.4 Economic Incentives

The Economic Incentives layer provides an overview of how PoW aligns miner incentives with the security of the Blockchain. Despite strong cryptography, a scheme will fail if miners do not receive adequate incentives to behave honestly.
Incentive Allocation Mechanism. Typically, the first miner to find a valid block receives the entire block incentive. The Work-Proportional model is used by some mining pools to distribute incentives based on the hash rate contributions of each miner, which encourages smaller miners to participate [98]. Miners may act selfishly as a result of a flawed incentive structure, prioritizing their own interests over the security of the network [44].
Incentive Sustainability. It refers to the ability of a PoW scheme to maintain miner incentives over the long term. Incentive sustainability ensures the incentive structure continues to provide adequate economic incentives even as block subsidies decline [103,106]. As a result, it has the key characteristics in the form of stability, decaying subsidy (e.g., halving in Bitcoin [46]), and fee-dependence (including transaction fee & block generation fee).
Incentive Composition. This dimension describes what makes up the total miner incentive. While the incentive composition is not a core requirement of PoW, it does influence the participation of the miners. The major sources of incentives are Block subsidy, transaction fee, and other sources (third-party payments).

5 Evaluation of PoUW According to the Taxonomy

By applying the taxonomy to a wide set of PoW schemes, we can classify PoUW mechanisms according to their alignment or deviation from necessary PoW properties across four layers, as discussed: core principles, architectural decisions, trade-offs, and economic incentives.
Core Principles. In traditional PoW, puzzles ensure computational hardness, cheap deterministic verification, non-interactivity, and stable difficulty adjustment, making block creation costly but validation efficient and predictable. By contrast, PoUW struggles to uphold these principles: verification may require re-execution, undermining efficiency, and non-interactivity is weakened by reliance on external datasets or off-chain verifiers. Moreover, adapting difficulty for real-world tasks remains challenging, limiting PoUWs ability to match the robustness of PoW.
Architectural Decisions. Both PoW and PoUW tie mining to resources: PoW uses computation or memory-hardness, while PoUW extends this to useful tasks. PoW schemes are mostly static or rotate, whereas some PoUW designs require frequent reconfigurationthough mutability remains optional. Unlike PoWs predictable hardware path, PoUW tasks can vary in efficiency even on the same hardware, complicating fairness [18].
Trade-offs. PoW puzzles are naturally non-amortizable and non-precomputable. PoUW tasks, however, may allow structural shortcuts (e.g., partial result reuse),

weakening fairness. PoW puzzles are highly parallelizable, enabling large-scale mining. Some PoUW tasks may not parallelize as efficiently, or parallelization may create uneven advantages, complicating fair participation.

Economic Incentives. On the economic side, PoW operates under a relatively straightforward incentive mechanism, a first-solver model, combining block subsidies and transaction fees. PoUW schemes, by contrast, define more complex incentive compositions that simultaneously incentivize network security and useful task completion. This dual-purpose incentive structure often results in unstable or fee-dependent sustainability, raising questions about the adequacy of long-term security budgets. Moreover, PoUW introduces a unique secondary market problem where the useful work has external market value, miners may prefer to sell results outside the blockchain rather than contribute them to consensus, thereby weakening the security budget (see section 6).

Nevertheless, for the incentive allocation mechanism, PoUW's economic model is more complex. Incentives should not only incentivize miners for securing the network, but also for performing useful calculations. Thus, new questions arise, including *how to value the useful work, how to prevent "cheating" and how to align the incentive mechanism with the security of the network and the integrity of the utility.*

These differences suggest that PoUW may not be a straightforward drop-in replacement for PoW but a fundamentally distinct design space, requiring re-evaluation of nearly all consensus-layer dimensions. Despite its promise to repurpose computational waste for socially beneficial outcomes, PoUW has not yet achieved the robustness of PoW in providing secure and decentralized consensus [10]. Taken together [60,65,11,45,32], the structural, functional, and economic limitations explain why PoUW, in its current form, remains inadequate to fully replace PoW in permission-less blockchain systems.

6 Economics of PoUW

This section explores the economic viability of PoUW mechanisms, addressing the necessity of economic incentives for sustained network liveness and security in continuation of Section 5. Based on economic attacks on Bitcoin, challenges addressed by Hoffman et al. [55], and arguments on incentives for security of the PoUW mechanism by Dotan et al. [40], this study builds an analytical view of PoUW considering the economic incentives of miners. The attacks on systems like Bitcoin exploit economic reasoning, such as the `Selfish Mining` attack [43], which results in energy wastage, caused by faulty miner behavior. However, these aspects are not discussed in detail in existing research in the economic context of PoUW. We assert that a carefully designed incentive structure is needed for the success of PoUW. A central question for any consensus protocol is whether the economic incentives of participants sustain the desired security properties. In PoW, the security budget directly determines the cost of a 51% or double-spend attack (see Section 4). PoUW aims to redirect that expenditure toward computations with external value, but it remains unclear whether the additional utility strengthens or weakens the underlying security guarantees.

6.1 Workflow of PoUW

We discuss the economy of miners in PoUW for two different cases: (*i*). if the challenge-solution is non-reusable, and (*ii*). If the solution can be traded offline outside the blockchain network, exploiting reusability. One of the major challenges in the existing PoUW mechanisms is designing the problem/task. Ideally, the real-world problem given to the miners must involve parameters that cannot be guessed beforehand. All nodes must be able to agree on how these parameters are to be adjusted so that the problem sets are adjusted over time, and it can be decided whether a given PoUW is valid for some time interval. If the mechanism is carefully designed in a non-reusable construction, miners cannot reliably trade the solution of the real-world challenge outside the blockchain network, as discussed in Section 4. From the off-chain buyer's point of view, the solution can be traded off-chain at a bargain rate, which may influence off-chain trading.
The tasks can also be submitted by users in the form of an instance x, a randomized algorithm (often called $Gen(x)$) produces a challenge C_x. This ensures that even if a user submits an easy or pre-solved task, the actual challenge remains unpredictable and hard to solve. The system can enforce required difficulty levels for submitted problems, rejecting trivial or pre-solved instances [13]. In case multiple users submit problems, the system can randomly select a problem to which instances are issued as tasks, or batch and rotate among them to avoid bias. To be noted, the process of task selection and assignment is transparent and verifiable by the network, which reduces the risk of manipulation [109]. Figure 3 exhibits the intricate relationships between various actors and economic forces within a PoUW ecosystem. In general, users/system submit real-world problems in the form of mining objectives along with associated fees, while miners solve these problems and create blocks, and earn incentives if the solution is validated. The liveness of the system depends on the fact that miners are sufficiently incentivized to participate actively [40]. If the sum of block incentives, mining objective fees, and transaction fees is less than the combined cost of energy needed to mine and the value of solutions obtainable in the external market, miners will lack motivation. They would rather favor solving such useful tasks offline while leaving the main network, thereby harming both network security and liveness due to reduced miner participation. Therefore, introducing user-uploaded mining objectives must be economically sensible. This necessitates optimal algorithms for solving mining objectives and minimizing any overhead beyond direct problem-solving, focusing on energy efficiency.

6.2 Model Overview

We consider a blockchain with N rational miners competing to append blocks of target interval τ. Each miner i expends computational effort e_i on a useful task U. A task yields four types of payoffs:

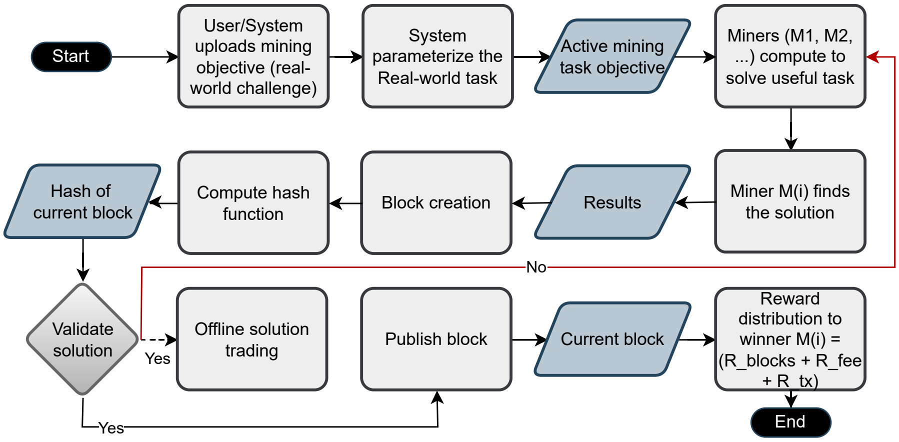

Start
User/System uploads mining objective (real-world challenge)
System parameterize the Real-world task
Active mining task objective
Miners (M1, M2, ...) compute to solve useful task
Miner M(i) finds the solution
Results
Block creation
Compute hash function
Hash of current block
Validate solution
No
Yes
Offline solution trading
Yes
Publish block
Current block
Reward distribution to winner M(i) = (R_blocks + R_fee + R_tx)
End

Fig. 3. Workflow of PoUW ecosystem: This flowchart demonstrates the key interactions within the PoUW system with solution validation, miner competition, and incentive distribution.

- R_{block}: block creation incentive.
- R_{tx}: the transaction fee paid by the users for adding the transactions to the block.
- R_{fee}: the fee paid by the users for solving the challenge.
- $V_{external}$: the value of the solution in the external/off-chain market.

Let c_i be the miner i's unit cost of computation. Analogous to the hash-rate-based classical PoW, the aggregated honest security budget per unit time is:

$$B = \sum_{i=1}^{N} c_i e_i \tag{1}$$

6.3 Assumptions

To keep the analysis intact, we build some explicit assumptions as follows:

- **A1, Effort equivalence:** Useful tasks can be subdivided into comparable units of work so that effort is well-defined. For a given difficulty parameter D, one unit of computational effort in PoW is equivalent to the effort required to perform one unit of useful computation in PoUW.
- **A2, Equal energy consumption:** For all D, the average energy cost per unit time of one unit of computational effort in PoW equals the cost of one computational step in PoUW: $\mathbb{E}(t_{hash}) = \mathbb{E}(t_{comp})$, and $\mathbb{E}(e_{hash}) = \mathbb{E}(e_{comp})$, where t_{hash} and t_{comp} are the time utilised in finding hash value in PoW and in evaluating one unit of computation in PoUW. Also, e_{hash} and e_{comp} are the energy expended by the PoW and PoUW system in one unit of hash and useful computation, respectively.

- **A3, Verifiability:** The proposed solution of a real-world problem can be verified with negligible cost relative to generation.
- **A4, Rationality:** Miners maximize expected profit, though adversaries may deviate strategically but they remain economically motivated.

6.4 Definitions

We analytically criticize the PoUW along three dimensions including (*i*) the coupling between useful work and the blockchains security budget, (*ii*) the implications on security and decentralization arising from non-cryptographic problem domains, and (*iii*) the design of incentive structures and their sensitivity to real-world problem characteristics. We address these dimensions by formally investigating the properties of economics and the security of the PoUW mechanism. The proposed model accounts for miners' costs and incentives, security budget, and the impact of solution reusability (offline trading). Accompanied by the traditional PoW, this model demonstrates the limitations of existing PoUW mechanisms in terms of utility and security. To facilitate a detailed analysis of mining behavior and difficulty adjustments in PoUW systems, we introduce some foundational definitions.

Definition 1. ***Block Generation Time.*** *Let $P = \sum_{i=1}^{n} e_i$ be the total computation power, and e_i is the computation power of miner i of the network in which the difficulty D (e.g., D=256 for 256-bit puzzles) is dynamically set so that the expected time to find a valid solution (block) matches the target τ, such that $\tau = \frac{2^D}{P}$. Simplifying gives $D = log_2(P.\tau)$*

Definition 2. ***Incentives.*** *The winner receives total incentives R, constituting*

- *the transaction fee paid by the users for adding the transactions in the block (R_{tx}),*
- *block creation incentive (R_{block}),*
- *the fee paid by the users for solving the challenge (R_{fee})*

Additionally, the value of the solution in the external/off-chain market, if traded offline, is $V_{external}$. Such that $R = R_{tx} + R_{block} + R_{fee} + V_{external}$. Let C_{fixed} be the fixed cost incurred due to hardware setup and maintenance. To be noted, the fixed cost is a one-time setup cost assumed to be bounded by a fixed duration Y (say, 2 years). Thus, the setup cost can be spread across the computational cost uniformly in Y years. The energy cost, $C_{energy} = k.D$ scales with the difficulty of the challenge, where k is the unit energy cost per unit of difficulty. As such, the gross earning, G_{earn} of a miner over a time horizon of t rounds (or blocks) can be defined as:

$$G_{earn,t} = t.p_i.R - t.C_{energy} - C_{fixed} \tag{2}$$

With the winning probability of miner i is p_i, we define the miner's expected gain over time as:

$$\mathbb{E}[G_{earn,t}] = t.\Big(p_i(R_{tx}+R_{block}+R_{fee}+V_{external})+(1-p_i)V_{external}-C_{energy})\Big)-C_{fixed} \tag{3}$$

A miner chooses to participate if $\mathbb{E}[G_{earn,T}] > 0$*, i.e., when the total expected incentive outweighs both operational and capital costs, keeping the assumption A4 intact. Depending on the reusability condition of the solution,* $\mathbb{E}[G_{earn}] \in \{0,1\}^N$*, the miner decides to leave the main chain network to find the solution off-chain* $\forall 1$*. Whereas the miner has two possibilities* $\forall 0$ *- either the winner adds the solution to main public chain, or the winner may consider adding the block with solution in the private chain and hence developing selfish mining [43]. As such, the expected gain of a miner, according to Eq.* [2]*, should satisfy:*

$$\mathbb{E}[G_{earn}] = p_i(R_{tx} + R_{block} + R_{fee}) - (C_{energy} + C_{fixed}) > 0 \tag{4}$$

7 Economic Security Analysis

7.1 Economic Security in PoUW

$V_{external}$ becomes critical in cases where the blockchain incentive alone does not justify participation. It provides an alternative incentive stream by allowing miners to derive value from the output, even if their solution is not included in the main chain.

Hypothesis 1. *The difficulty,* D*, of the challenge provided by the system varies with respect to the incentives expected on-chain* R *and the external value of the solution* $V_{external}$ *(if the* $V_{external}$ *is known).*

Proof. According to Dotan et al. [40], probability of miner i solving the challenge, $p_i = \frac{e_i}{P}$. Without loss of generality, let computational power equal the energy spent in computing the challenge. Considering uniform computational power and letting the energy consumed $e_i = k.D$, and the total network power is $P = N.k.D$. Building upon the assumption A1 (Effort equivalence), each miner has uniform computing power equal to $k.D$. Substituting into the expected gain equation over a single round:

$$\frac{1}{N}(R_{tx}+R_{block}+R_{fee}+V_{external})+\frac{(N-1)}{N}V_{external}-(k.D+C_{fixed}) > 0 \cdots \tag{5}$$

Simplifying equation 5 while solving for D, we get,

$$D < \frac{1}{k}(\frac{1}{N}(R_{tx} + R_{block} + R_{fee}) + V_{external} - C_{fixed}) \cdots \tag{6}$$

$$D < \frac{1}{k}(\frac{1}{N}(R_{tx} + R_{block} + R_{fee}) - C_{fixed}) \cdots \tag{7}$$

Thus, in the absence of external value, the burden of sustaining difficulty falls entirely on transaction and block fees. If these incentives are insufficient, miners will be disincentivized, leading to a decrease in network participation and consequently, a reduction in difficulty. This is especially critical in PoUW, where real-world problems may vary in difficulty and, hence, challenging to maintain a constant block creation time considering solution reusability. □

This hypothesis is proven under the stated assumptions and highlights a fundamental challenge, as difficulty in PoUW systems must adapt not only to energy expenditure but also to the expected economic value of solving the problem. Unlike PoW, where difficulty is adjusted solely to maintain a constant block interval, PoUW must incorporate variable problem utility, which affects miner motivation and system security.

Hypothesis 2. *In a PoUW blockchain network, if the network's computational power P increases (more miners, more hardware), the difficulty D increases proportionally to keep block times steady. Formally, $D \propto P$.*

Proof. We prove by contradiction. Let us assume that $D \propto P$ is not correct. But, from Definition 1, $\tau = \frac{2^D}{P}$. If P increases to $P^{'}$, then τ decreases to $\tau^{'}$, which is undesirable for a stable network. Hence, our assumption is not correct. Thus, to keep τ steady, the system must increase the value of D proportional to P.

In PoW, the difficulty target adjusts to keep block times τ. Useful tasks, however, are heterogeneous and may vary widely in finding solutions and verification, under the assumption A3 (Verifiability). Empirical evidence from heterogeneous puzzle systems such as Primecoin shows that block-time variance is higher than in hash-based PoW, which may result in selfish mining and timestamp attacks in PoUW-based systems. [43][97]. □

Hypothesis 3. *The security budget S_b of useful work in PoUW system does not contribute to the security of the chain.*

Proof. As discussed in Definition 2, the total cost is the combination of the fixed cost and the energy cost. That is, in the case of PoUW, $C_{PoUW} = P.(C_{fixed} + C_{energy})$. Considering the assumption A2, and contrasting the the PoW, where the computing is aligned with the security of the chain as the security budget depends only on the mining cost to secure the chain, some of the PoUW mechanisms [95,24] constitute the expenses/ efforts in solving the challenges as well as securing the chain [24].

Hence, $S_{PoW} = P.(k.D_{PoW} + C_{fixed})$

Let $\alpha > 0$ be the fraction of effort spent by a miner on solving the useful work challenge, then $(1 - \alpha)$ is used in securing the chain.

Thus, $S_{PoUW} = P.((1 - \alpha).(k.D + C_{fixed}))$. Hence, $S_{PoUW} < S_{PoW}$ for equivalent D. However, for those PoUW mechanisms where systems integrate useful work directly into the blockchain security [65], $S_{PoUW} = S_{PoW}$. □

If the solution is non-reusable, miners might be demotivated to put effort into useful work with reduced incentives. As such, the security budget of PoUW relies on the efforts in solving the useful work (α) and in securing the blockchain $(1-\alpha)$, as $S_{PoUW} = (1-\alpha).S_{PoW}$. This leads to a reduction in α and tends to approach the security of PoW, that is, $S_{PoUW} \approx S_{PoW}$ for $\alpha \rightarrow 0$. This, in return, defeats the purpose of PoUW.

In PoW, all energy spent is tied to solving a (cryptographic) puzzle (e.g., hash preimage) and the cost of redoing this work (e.g., in a 51% attack) is what secures the chain. Therefore, for the situation where miners spend energy, but that energy doesn't increase attack cost, the system is not secure-by-energy. It means that the energy spent might not increase the cost of attacks, and therefore does not secure the chain. Hence, Hypothesis 3 exposes a fundamental tension. When α is small, useful work provides no additional security relative to PoW. However, when α is large, the security budget may be influenced by the volatility of the external market. An attacker can therefore lower the cost of a 51% attack by not only reduced hash power but also by manipulating or short-selling the external market value.

Hypothesis 4. *The PoUW system does not contribute to substantial energy efficiency. That is, the total energy consumed by the network remains comparable to traditional PoW systems, and most of the computational effort is still consumed redundantly, resulting in limited or negligible net energy efficiency. Considering assumption A4, and there are no qualitative moral values behind solving the useful tasks in PoUW.*

Proof. The total energy spent in the PoUW, $E_{total} = N.C_{energy}$. Only the winner gets incentivized, and the energy consumed by the winner can rationally be considered as energy spent against the useful work. Thus, $E_{useful} = C_{energy}$. The rest of the energy burnt by miners is wasted since all other miners are redundant in performing the useful tasks. Thus, $E_{waste} = (N-1).C_{energy}$.

The net energy efficiency $\eta = \frac{E_{useful}}{E_{total}} = \frac{1}{N}$. This implies that the efficiency reduces with the surging number of miners in the network, i.e., as N increases, $\eta \rightarrow 0$. □

While addressing RQ1, this study introduces an extended incentive function that includes not only block and transaction fees but also external utility value ($V_{external}$), revealing new classes of PoUW schemes where miner incentives depend on both on-chain and off-chain incentives, thus enriching the taxonomy's *Incentive Allocation Mechanism* dimension. For RQ2, the section mathematically demonstrates critical inadequacies of PoUW: it shows that the security budget (S_b) in many PoUW systems is decoupled from security of the chain, and net energy efficiency (η) decreases as network size increases, undermining PoUWs energy-saving claims. These findings reinforce the taxonomy‘s concerns under *Computational Hardness*, and *Difficulty Adjustment*, highlighting how PoUW often fails to meet core consensus guarantees. Finally, for RQ3, the section outlines clear design constraints, such as the need for stable difficulty adjustment in response to utility variance and the importance of solution reusability, to ensure economic viability. It thus provides theoretical tools and measurable parameters (e.g., α, $V_{external}$, D) that guide the development of PoUW schemes capable of aligning real-world utility with the security requirements of permissionless blockchains.

7.2 Security Analysis

The economic model in Section 6 characterizes the rational and profitability of miners considering the security budget. However, the real deployments must also withstand strategic adversaries who are capable of manipulating both on-chain and off-chain markets. PoUW introduces new attack surfaces because consensus security is partially coupled to the external value of useful tasks. This is evident from the security budget as discussed above (see Section 6) where an adversary may choose not only to concentrate mining power but also to manipulate the external market for useful tasks, thereby lowering the cost of a successful attack. This section elaborates on the strategic behaviors enabled by this coupling of on-chain and off-chain incentives.

Threat. We assume an adversary $\mathcal{A}$ who can (i). dedicate computational effort as a miner, (ii). coordinate with other miners or pools, and (iii). trade in the external market where the output of useful tasks has value $V_{external}$. Such an adversary seeks either direct financial profit or the ability to violate the consistency and liveness of the blockchain. Unlike traditional PoW, where security depends solely on the cost of computation, PoUW exposes a second control point to the market valuation of useful work, which an adversary can influence through financial or operational tactics, such as short-and-attack strategies [49], wash trading [23], etc.

Collusion. Since the basic nature of PoUW tasks is heterogeneous, they differ in complexity and external value. As such, miners may have an incentive to select high-value tasks as cherry-picking or collude to monopolize. This develops centralization in the form of a cartel dynamics similar to what has been analyzed for mining pools in PoW by Eyal et al. [43]. Moreover, the coalition also leads to skewed incentive distribution and irregular block timing.

Cross-domain leverage. An $\mathcal{A}$ can simultaneously do mining, trading, and speculation, which may create a feedback loop. $\mathcal{A}$ can acquire or brokering high-value tasks at low price, mine them to obtain R_{fee}, R_{tx}, R_{block}, and $V_{external}$ and execute market trades that reduce $V_{external}$ just as an on-chain attack is launched. By profiting on both the short position and the successful double-spend, the $\mathcal{A}$ directs off-chain market manipulation into a funding source for on-chain consensus. This multi-domain leverage has parallels in cross-market manipulation discussed in [23] and raises regulatory as well as technical concerns.

8 Structured Critique of PoUW: Toulmin Model approach

To systematically evaluate the security and economic claims made by PoUW mechanisms, we adopt the Toulmin argumentation framework [112]. This section discusses PoUW through transparent, logically connected reasoning, justification, supporting evidence, and the boundaries or limitations of each claim. The detailed components as metadata are explained in Appendix E.

8.1 Unjustified Energy Conservation

Many PoUW research claim that redirecting mining power to socially useful tasks lead to superior energy efficiency. However, as our economic model shows, the security budget remains tied to the on-chain block incentive while failing to meet the bar of security and utility simultaneously (Hypothesis 3). The scale of wasted effort remains comparable to that of PoW. Thus, useful computation rarely reduces the energy required for equivalent security (see Appendix E.1).

8.2 Unfair incentive Structure

Previous PoUW proposals often claim that incentives remain fair and resistant to centralization. In practice, heterogeneous task complexity and varying task‘s value results into cherry-picking and may lead to cartel formation, creating incentive imbalances similar to selfish-mining in PoW [43]. Moreover, if the primary incentive for the useful computation is inadequate, miners may reduce investment in hardware, lowering the overall security budget and shifting effort to off-chain trading or secondary markets where partially completed solutions can still generate value. Although partial-incentive or modular task-sharing schemes have been proposed to mitigate this unfairness, such mechanisms remain uncommon and add complexity, so current PoUW designs provide limited assurance of equitable or stable incentives (see Appendix E.2).

8.3 Difficulty in Difficulty Adjustment

PoUW may have irregular task difficulty, producing unpredictable block times that undermine fairness and network stability. As such, some evidence from implementations like DLChain [30] and Proof-of-Solution [29] show that failed solutions of the challenge or delayed verification can surge block intervals. This lowers throughput and increases fork risk. While modularizing tasks or imposing time limits may mitigate the problem, such fixes add coordination overhead and risk centralization, leaving PoUW less robust than hash-based PoW in maintaining consistent block times (see Appendix E.3).

8.4 Lack of Degree of Randomness

PoUW often lacks randomness in challenge assignment. Since tasks are externally supplied, they can be pre-solved or tailored for miners with prior knowledge or specialized hardware. Random challenge selection is crucial for equal opportunity and resistance to manipulation, yet real-world problem submissions can be exploited through attacks such as precomputed-solution or model-stealing [114,119]. Though seeding tasks with blockchain-derived randomness can reduce these risks, such measures reduce the purpose of useful work and thus do not fully resolve the vulnerability (see Appendix E.4).

> In support of RQ2, the analysis demonstrates that PoUW fails to ensure energy savings and stable security budgets, despite its claim to repurpose useful computation. While the data supporting energy-efficiency or fairness claims may be correct in isolation (e.g., the computations do have scientific value), but such value strengthening consensus fails under our scrutiny. These arguments directly validate critiques outlined in the taxonomys *Difficulty Adjustment*, *Verification Time*, and *Economic Incentives* dimensions.

9 Design Recommendation for PoUW mechanism

This section discusses building a few primary recommendations that emerge to guide the design of PoUW mechanisms that are more practical, secure, and energy-efficient based on the critical analyses and formal modeling presented in our systematization.

A fundamental design principle is that the useful computational tasks must contribute directly to the security budget of the blockchain. The fraction of miner effort dedicated to useful work should not undermine the portion securing the chain. The PoUW protocols should integrate the useful work tightly with cryptographic proof structures so that all performed computations reinforce security guarantees, rather than treat useful tasks as additive but separable from core consensus. Moreover, PoUW mechanisms should include algorithms that dynamically adjust problem difficulty or workload partitioning in real-time, ensuring block times remain predictable and aligned with network capacity by using methods such as task modularization, adaptive sampling, or controlled delegation, which can support consistent consensus intervals while managing variability in task complexity.

Considering the incentive structure, rather than a winner-takes-all model, partial incentives for incremental or collaborative contributions improve miner motivation and reduce centralization risk. Transparent and proportional incentive allocation, potentially leveraging share-based or market-driven compensation models, will sustain network liveness and security by aligning incentives with actual computational effort and solution quality. While addressing the redundancy in mining, techniques such as solution-sharing, pooled mining approaches, or multi-winner consensus can improve overall energy efficiency without compromising security. In order to maintain the fairness in task assignment, PoUW designs should cryptographically seed task generation using unpredictable blockchain state data (e.g., previous block hashes) to prevent advantage concentration. However, parameterization must preserve the integrity and real-world applicability of the useful problems to avoid diminishing their utility. The verifiability of useful work remains a key challenge, especially in complex computations like AI model training. PoUW mechanisms should incorporate succinct proofs [117] or attestation schemes [70] that enable fast and deterministic verification of solutions while maintaining computational integrity and preventing cheating.

Regarding RQ3, the Toulmin model highlights key design implications for improving PoUW supported by design recommendations incorporating randomness in challenge assignment, supporting verifiable partial incentives, and developing utility-aware difficulty scaling. Each argument structured through claim, data, warrant, and rebuttal, offers targeted insight into what dimensions must be refined to create economically secure and practically viable PoUW systems. The analysis complements the formal economic modeling by surfacing both qualitative and structural weaknesses in current PoUW protocols.

10 Conclusion and Future Work

This SoK paper critically examined PoUW as an alternative to traditional PoW. Through a taxonomy, formal modeling, and structured critique, we addressed the gaps in PoUW constructions particularly in difficulty adjustment, incentive structures, randomness in task generation, and energy efficiency. These shortcomings justify why the PoUW has yet to achieve practical deployment at scale, despite years of proposals.

This study revealed that the security of current PoUW mechanisms is at stake, as there are risks of economic centralization, gaps in difficulty adjustment, and possibilities of attacks due to the lack of randomness in task assignment. From a conceptual perspective, as energy savings remain negligible due to redundant computations, and that the economic utility of “useful” puzzles does not contribute to the blockchain’s security budget, thereby leaving the resource footprint issue unchanged. This study is limited with the assumption of equal energy per unit of work and quick verifiability which may not always be true (as in the case of ML/optimization problems). The core challenge is aligning useful computation with the security budget of the chain. Promising approaches include tightly integrating verifiable computation (e.g., via succinct proofs), designing proportional or partial incentive mechanisms that sustain miner motivation, and developing difficulty adjustment schemes that preserve predictable block intervals while accommodating heterogeneous tasks. Further research could include the analysis of the quality and security of useful tasks corresponding to each category described in Section 3. The assumption A1, Effort equivalence can be studied in detail per use case by empirical methods or sensitivity analysis.

In a nutshell, while existing PoUW mechanisms fall short of their promised utilities, careful redesign guided by security budget may enable such consensus protocols that are both practically useful and environmentally sustainable.

References

1. Abellán Álvarez, I., Gramlich, V., Sedlmeir, J.: Unsealing the secrets of blockchain consensus: A systematic comparison of the formal security of proof-of-work and proof-of-stake. In: Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing. pp. 278–287 (2024)
2. Abubakar, M., Jaroucheh, Z., Al-Dubai, A., Buchanan, B.: Ponw: A secure and scalable proof-of-notarized-work based consensus mechanism. In: ICVISP 2020: 4th International Conference on Vision, Image and Signal Processing, Bangkok, Thailand, December, 2020. pp. 58:1–58:8. ACM (2020). https://doi.org/10.1145/3448823.3448875, https://doi.org/10.1145/3448823.3448875
3. Adams, S.C., Zheng, Y.: A framework using useful work for transient committee selections in blockchain consensus. In: 2022 International Conference on IoT and Blockchain Technology (ICIBT). pp. 1–6. IEEE (2022)
4. Adams, S.C., Zheng, Y.: A framework using useful work for transient committee selections in blockchain consensus. In: 2022 International Conference on IoT and Blockchain Technology (ICIBT). pp. 1–6. IEEE (2022)
5. Akram, J., Akram, A., Jhaveri, R.H., Alazab, M., Chi, H.: Bc-iodt: blockchain-based framework for authentication in internet of drone things. In: Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, DroneCom 2022, Sydney, NSW, Australia, 17 October 2022. pp. 115–120. ACM (2022). https://doi.org/10.1145/3555661.3560874, https://doi.org/10.1145/3555661.3560874
6. Ali, I.M., Caprolu, M., Pietro, R.D.: Foundations, properties, and security applications of puzzles: A survey. ACM Computing Surveys (CSUR) **53**(4), 1–38 (2020)
7. Aponte-Novoa, F.A., Orozco, A.L.S., Villanueva-Polanco, R., Wightman, P.: The 51
8. Arnosti, N., Weinberg, S.M.: Bitcoin: A natural oligopoly. Management Science **68**(7), 4755–4771 (2022)
9. Azimy, H., Ghorbani, A.A., Bagheri, E.: Preventing proof-of-work mining attacks. Information Sciences **608**, 1503–1523 (2022)
10. Bakhshi, F., Ashtiani, M., Azgomi, M.A.: A systematic literature review on proof-of-useful work consensus algorithms. Blockchain: Research and Applications p. 100387 (2025)
11. Baldominos, A., Saez, Y.: Coin.ai: A proof-of-useful-work scheme for blockchain-based distributed deep learning. Entropy **21**(8), 723 (2019). https://doi.org/10.3390/E21080723, https://doi.org/10.3390/e21080723
12. Baldominos, A., Saez, Y.: Coin.ai: A proof-of-useful-work scheme for blockchain-based distributed deep learning. Entropy **21**(8), 723 (2019). https://doi.org/10.3390/E21080723, https://doi.org/10.3390/e21080723
13. Ball, M., Rosen, A., Sabin, M., Vasudevan, P.N.: Proofs of useful work. Cryptology ePrint Archive, Paper 2017/203 (2017), https://eprint.iacr.org/2017/203
14. Baniata, H., Anaqreh, A.T., Kertész, A.: DONS: dynamic optimized neighbor selection for smart blockchain networks. Future Gener. Comput. Syst. **130**, 75–90 (2022). https://doi.org/10.1016/J.FUTURE.2021.12.010, https://doi.org/10.1016/j.future.2021.12.010
15. Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G.: Sok: Consensus in the age of blockchains. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich,

Switzerland, October 21-23, 2019. pp. 183–198. ACM (2019). https://doi.org/10.1145/3318041.3355458, https://doi.org/10.1145/3318041.3355458

16. Bao, Q., Li, B., Wang, Y., Cao, D.: How do characteristic parameters affect the security of proof-of-work blockchain? IEEE Transactions on Network and Service Management (2025)
17. Bao, Z., Tang, C., Xie, X., Chen, G., Lin, F., Zheng, Z.: Toward green and efficient blockchain for energy trading: A noncooperative game approach. IEEE Internet Things J. **10**(22), 20021–20032 (2023). https://doi.org/10.1109/JIOT.2023.3283412, https://doi.org/10.1109/JIOT.2023.3283412
18. Bar-On, Y., Komargodski, I., Weinstein, O.: Proof of work with external utilities. arXiv preprint arXiv:2505.21685 (2025)
19. Biryukov, A., Khovratovich, D.: Equihash: Asymmetric proof-of-work based on the generalized birthday problem. Ledger **2**, 1–30 (2017)
20. Bit2Me Academy: Top algoritmos de minería más utilizados. https://academy.bit2me.com/en/top-algoritmos-de-mineria-mas-utilizados/, accessed: 2025-09-10
21. Bizzaro, F., Conti, M., Pini, M.S.: Proof of evolution: leveraging blockchain mining for a cooperative execution of genetic algorithms. In: IEEE International Conference on Blockchain, Blockchain 2020, Rhodes, Greece, November 2-6, 2020. pp. 450–455. IEEE (2020). https://doi.org/10.1109/BLOCKCHAIN50366.2020.00065, https://doi.org/10.1109/Blockchain50366.2020.00065
22. Blocki, J., Zhou, H.S.: Designing proof of human-work puzzles for cryptocurrency and beyond. In: Theory of cryptography conference. pp. 517–546. Springer (2016)
23. Brunnermeier, M.K., Oehmke, M.: Predatory short selling. Review of Finance **18**(6), 2153–2195 (2014)
24. Cao, W., Ling, X., Wang, J., Gao, X., Ding, Z.: Optimization-based proof of useful work: Framework, modeling, and security analysis. arXiv preprint **arXiv:2405.19027** (2024), https://arxiv.org/abs/2405.19027
25. Chatterjee, D., Banerjee, P., Mazumdar, S.: Chrisimos: A useful proof-of-work for finding minimal dominating set of a graph. In: 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 1332–1339. IEEE (2023)
26. Chatterjee, K., Goharshady, A.K., Pourdamghani, A.: Hybrid mining: exploiting blockchain's computational power for distributed problem solving. In: Hung, C., Papadopoulos, G.A. (eds.) Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, SAC 2019, Limassol, Cyprus, April 8-12, 2019. pp. 374–381. ACM (2019). https://doi.org/10.1145/3297280.3297319, https://doi.org/10.1145/3297280.3297319
27. Chaurasia, Y., Subramanian, V., Gujar, S.: Pupow: A framework for designing blockchains with practically-useful-proof-of-work & vanitycoin. In: Xiang, Y., Wang, Z., Wang, H., Niemi, V. (eds.) 2021 IEEE International Conference on Blockchain, Blockchain 2021, Melbourne, Australia, December 6-8, 2021. pp. 122–129. IEEE (2021). https://doi.org/10.1109/BLOCKCHAIN53845.2021.00026, https://doi.org/10.1109/Blockchain53845.2021.00026
28. Chen, C., Cheng, Z., Qu, S., Fang, Z.: Crowdsourcing work as mining: A decentralized computation and storage paradigm. In: Proceedings of the 7th Asia-Pacific Workshop on Networking, APNET 2023, Hong Kong, China, June 29-30, 2023. pp. 174–175. ACM (2023). https://doi.org/10.1145/3600061.3603177, https://doi.org/10.1145/3600061.3603177

29. Chen, S., Mi, H., Ping, J., Yan, Z., Shen, Z., Liu, X., Zhang, N., Xia, Q., Kang, C.: A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading. Nature Energy **7**(6), 495–502 (2022)
30. Chenli, C., Li, B., Jung, T.: Dlchain: Blockchain with deep learning as proof-of-useful-work. In: Ferreira, J.E., Palanisamy, B., Ye, K., Kantamneni, S., Zhang, L. (eds.) Services - SERVICES 2020 - 16th World Congress, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12411, pp. 43–60. Springer (2020). https://doi.org/10.1007/978-3-030-59595-1_4, https://doi.org/10.1007/978-3-030-59595-1_4
31. Chinnaperumal, S., Raju, S.K., Alharbi, A.H., Kannan, S., Khafaga, D.S., Periyasamy, M., Eid, M.M., El-Kenawy, E.S.M.: Decentralized energy optimization using blockchain with battery storage and electric vehicle networks. Scientific Reports **15**(1), 5940 (2025)
32. Chong, Z.K., Ohsaki, H., Ng, B.: Proof of useful intelligence (poui): Blockchain consensus beyond energy waste. arXiv preprint arXiv:2504.17539 (2025)
33. Dai, X., Xiao, J., Yang, W., Wang, C., Chang, J., Han, R., Jin, H.: Lvq: A lightweight verifiable query approach for transaction history in bitcoin. In: 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS). pp. 1020–1030. IEEE (Nov 2020). https://doi.org/10.1109/ICDCS47774.2020.00096
34. Davidovic, T., Todorovic, M., Sharma, B., Ramljak, D.: Exploring arbitrary real-life problems in proof-of-useful-work: Myth busting? In: Aloqaily, M., Otoum, S., Bouachir, O., Jararweh, Y., Ridhawi, I.A., Al-Begain, K., Alsmirat, M.A. (eds.) Fifth International Conference on Blockchain Computing and Applications, BCCA 2023, Kuwait, Kuwait, October 24-26, 2023. pp. 1–6. IEEE (2023). https://doi.org/10.1109/BCCA58897.2023.10338884, https://doi.org/10.1109/BCCA58897.2023.10338884
35. Davidson, M., Diamond, T.: On the profitability of selfish mining against multiple difficulty adjustment algorithms. Cryptology ePrint Archive (2020)
36. Davis, P.: (2024), https://asicmarketplace.com/blog/what-is-proof-of-useful-work/, aSIC MarketPlace
37. Dobraunig, C., Eichlseder, M., Mendel, F.: Security evaluation of sha-224, sha-512/224, and sha-512/256. Institute for Applied Information Processing and Communications, Graz University of Technology (2015)
38. Doku, R., Rawat, D.B.: IFLBC: on the edge intelligence using federated learning blockchain network. In: 6th IEEE International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, and IEEE International Conference on Intelligent Data and Security, BigDataSecurity/HPSC/IDS 2020, Baltimore, MD, USA, May 25-27, 2020. pp. 221–226. IEEE (2020). https://doi.org/10.1109/BIGDATASECURITY-HPSC-IDS49724.2020.00047, https://doi.org/10.1109/BigDataSecurity-HPSC-IDS49724.2020.00047
39. Dong, Z., Lee, Y.C., Zomaya, A.Y.: Proofware: Proof of useful work blockchain consensus protocol for decentralized applications. CoRR **abs/1903.09276** (2019), http://arxiv.org/abs/1903.09276
40. Dotan, M., Tochner, S.: Proofs of useless work - positive and negative results for wasteless mining systems. CoRR **abs/2007.01046** (2020), https://arxiv.org/abs/2007.01046

41. Dragos, C.: Proof of useful work based on matrix computation. In: 2022 24th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC). pp. 108–116. IEEE (2022)
42. Du, Y., Leung, C., Wang, Z., Leung, V.C.M.: Accelerating blockchain-enabled distributed machine learning by proof of useful work. In: 30th IEEE/ACM International Symposium on Quality of Service, IWQoS 2022, Oslo, Norway, June 10-12, 2022. pp. 1–10. IEEE (2022). https://doi.org/10.1109/IWQOS54832.2022.9812927, https://doi.org/10.1109/IWQoS54832.2022.9812927
43. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8437, pp. 436–454. Springer (2014). https://doi.org/10.1007/978-3-662-45472-5_28, https://doi.org/10.1007/978-3-662-45472-5_28
44. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM **61**(7), 95–102 (2018)
45. F. Hoffmann: Challenges of Proof-of-Useful-Work (PoUW). In: 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain). pp. 1–5 (Nov 2022). https://doi.org/10.1109/iGETblockchain56591.2022.10087185, journal Abbreviation: 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)
46. Fabus, J., Kremenova, I., Stalmasekova, N., Kvasnicova-Galovicova, T.: An empirical examination of bitcoins halving effects: Assessing cryptocurrency sustainability within the landscape of financial technologies. Journal of Risk and Financial Management **17**(6), 229 (2024)
47. Fitzi, M., Kiayias, A., Panagiotakos, G., Russell, A.: Ofelimos: Combinatorial optimization via proof-of-useful-work: A provably secure blockchain protocol. In: Annual International Cryptology Conference. pp. 339–369. Springer Nature Switzerland (2022)
48. Fry, J., Serbera, J.: Quantifying the sustainability of bitcoin and blockchain. J. Enterp. Inf. Manag. **33**(6), 1379–1394 (2020). https://doi.org/10.1108/JEIM-06-2018-0134, https://doi.org/10.1108/JEIM-06-2018-0134
49. Gans, J.S., Halaburda, H.: Some economics of private digital currency. In: Economic Analysis of the Digital Economy, pp. 257–276. University of Chicago Press (2015)
50. Gopikrishnan, S., Priakanth, P., Srivastava, G., Joe, C.V.: SCHEISB: design of a high efficiency iomt security model based on sharded chains using bio-inspired optimizations. Comput. Electr. Eng. **111**(Part A), 108925 (2023). https://doi.org/10.1016/J.COMPELECENG.2023.108925, https://doi.org/10.1016/j.compeleceng.2023.108925
51. Han, R., Foutris, N., Kotselidis, C.: Demystifying crypto-mining: Analysis and optimizations of memory-hard pow algorithms. In: 2019 IEEE international symposium on performance analysis of systems and software (ISPASS). pp. 22–33. IEEE (2019)
52. Haouari, M., Mhiri, M., El-Masri, M., Al-Yafi, K.: A novel proof of useful work for a blockchain storing transportation transactions. Inf. Process. Manag. **59**(1), 102749 (2022). https://doi.org/10.1016/J.IPM.2021.102749, https://doi.org/10.1016/j.ipm.2021.102749

53. Haouari, M., Mhiri, M., El-Masri, M., Al-Yafi, K.: A novel proof of useful work for a blockchain storing transportation transactions. Information Processing & Management **59**(1), 102749 (2022)
54. Harvey-Buschel, J., Kisagun, C.: Bitcoin mining decentralization via cost analysis. arXiv preprint arXiv:1603.05240 (2016)
55. Hoffmann, F.: Challenges of proof-of-useful-work (pouw). In: 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGET-blockchain). pp. 1–5. IEEE (2022)
56. Hoffmann, F.: Challenges of proof-of-useful-work (pouw). CoRR **abs/2209.03865** (2022), https://doi.org/10.48550/arXiv.2209.03865
57. Hoffmann, F.: Gophy: Novel proof-of-useful-work blockchain architecture for high energy physics. In: 6th International Conference on Blockchain Computing and Applications, BCCA 2024, Dubai, UAE, November 26-29, 2024. pp. 630–634. IEEE (2024). https://doi.org/10.1109/BCCA62388.2024.10844433, https://doi.org/10.1109/BCCA62388.2024.10844433
58. Huang, J., Kong, L., Cheng, L., Dai, H., Qiu, M., Chen, G., Liu, X.S., Huang, G.: Blocksense: Towards trustworthy mobile crowdsensing via proof-of-data blockchain. IEEE Trans. Mob. Comput. **23**(2), 1016–1033 (2024). https://doi.org/10.1109/TMC.2022.3230758, https://doi.org/10.1109/TMC.2022.3230758
59. Hutter, F., Hamadi, Y., Hoos, H.H., Leyton-Brown, K.: Performance prediction and automated tuning of randomized and parametric algorithms. In: Benhamou, F. (ed.) Principles and Practice of Constraint Programming - CP 2006, 12th International Conference, CP 2006, Nantes, France, September 25-29, 2006, Proceedings. Lecture Notes in Computer Science, vol. 4204, pp. 213–228. Springer (2006). https://doi.org/10.1007/11889205_17, https://doi.org/10.1007/11889205_17
60. Ileri, A.M., Ozercan, H.I., Gundogdu, A., Senol, A.K., Özkaya, M.Y., Alkan, C.: Coinami: A cryptocurrency with DNA sequence alignment as proof-of-work. CoRR **abs/1602.03031** (2016), http://arxiv.org/abs/1602.03031
61. Ilie, D.I., Werner, S.M., Stewart, I.D., Knottenbelt, W.J.: Unstable throughput: when the difficulty algorithm breaks. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). pp. 1–5. IEEE (2021)
62. Jalali, S., Wohlin, C.: Systematic literature studies: database searches vs. backward snowballing. In: Proceedings of the ACM-IEEE international symposium on Empirical software engineering and measurement. pp. 29–38 (2012)
63. Kattis, A., Bonneau, J.: Proof of necessary work: Succinct state verification with fairness guarantees. In: Baldimtsi, F., Cachin, C. (eds.) Financial Cryptography and Data Security - 27th International Conference, FC 2023, Bol, Brač, Croatia, May 1-5, 2023, Revised Selected Papers, Part II. Lecture Notes in Computer Science, vol. 13951, pp. 18–35. Springer (2023). https://doi.org/10.1007/978-3-031-47751-5_2, https://doi.org/10.1007/978-3-031-47751-5_2
64. Kim, H., Kim, K., Kwon, H., Seo, H.: Asic-resistant proof of work based on power analysis of low-end microcontrollers. Mathematics **8**(8), 1343 (2020)
65. King, S.: Primecoin: Cryptocurrency with prime number proof-of-work (2013), https://primecoin.io/primecoin-paper.pdf
66. King, S., Nadal, S.: Ppcoin: Peer-to-peer cryptocurrency with proof-of-stake, aug. 2012. URL https://peercoin. net/assets/paper/peercoinpaper. pdf
67. Kiran, M., Patil, A.P., Premkumar, H., Hegde, P., Kumar, P.R.: Proof of solution: Implementation of work history as stake in blockchain applications. In: 2021 IEEE 18th India Council International Conference (INDICON). pp. 1–6. IEEE (2021)

68. Komodo Team: What is digibyte? p2p solution for crypto transactions. https://komodoplatform.com/en/academy/what-is-digibyte-dgb/ (Sep 2023), last updated: September 5, 2023; Accessed: 2025-09-05
69. Król, M., Sonnino, A., Al-Bassam, M., Tasiopoulos, A.G., Rivière, E., Psaras, I.: Proof-of-prestige: A useful work reward system for unverifiable tasks. ACM Trans. Internet Techn. **21**(2), 44:1–44:27 (2021). https://doi.org/10.1145/3419483, https://doi.org/10.1145/3419483
70. Kuang, B., Fu, A., Yu, S., Yang, G., Su, M., Zhang, Y.: Esdra: An efficient and secure distributed remote attestation scheme for iot swarms. IEEE Internet of Things Journal **6**(5), 8372–8383 (2019)
71. Kumari, T., Baranwal, G.: Collaborative vying in proof of useful work. In: 2024 IEEE 31st International Conference on High Performance Computing, Data and Analytics Workshop (HiPCW). pp. 109–110. IEEE (2024)
72. Lasla, N., Al-Sahan, L., Abdallah, M., Younis, M.F.: Green-pow: An energy-efficient blockchain proof-of-work consensus algorithm. Comput. Networks **214**, 109118 (2022). https://doi.org/10.1016/J.COMNET.2022.109118, https://doi.org/10.1016/j.comnet.2022.109118
73. Li, A., Wei, X., He, Z.: Robust proof of stake: A new consensus protocol for sustainable blockchain systems. Sustainability **12**(7), 2824 (2020)
74. Li, B., Chenli, C., Xu, X., Jung, T., Shi, Y.: Exploiting computation power of blockchain for biomedical image segmentation. In: IEEE Conference on Computer Vision and Pattern Recognition Workshops, CVPR Workshops 2019, Long Beach, CA, USA, June 16-20, 2019. pp. 2802–2811. Computer Vision Foundation / IEEE (2019). https://doi.org/10.1109/CVPRW.2019.00339, http://openaccess.thecvf.com/content_CVPRW_2019/html/BCMCVAI/Li_Exploiting_Computation_Power_of_Blockchain_for_Biomedical_Image_Segmentation_CVPRW_2019_paper.html
75. Li, B., Lu, Q., Jiang, W., Jung, T., Shi, Y.: A mining pool solution for novel proof-of-neural-architecture consensus. In: IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021, Sydney, Australia, May 3-6, 2021. pp. 1–3. IEEE (2021). https://doi.org/10.1109/ICBC51069.2021.9461067, https://doi.org/10.1109/ICBC51069.2021.9461067
76. Li, B., Shen, B., Lu, Q., Jung, T., Shi, Y.: Proof-of-federated-learning-subchain: Free partner selection subchain based on federated learning. In: Aloqaily, M., Otoum, S., Bouachir, O., Jararweh, Y., Ridhawi, I.A., Al-Begain, K., Alsmirat, M.A. (eds.) Fifth International Conference on Blockchain Computing and Applications, BCCA 2023, Kuwait, Kuwait, October 24-26, 2023. pp. 600–605. IEEE (2023). https://doi.org/10.1109/BCCA58897.2023.10338941, https://doi.org/10.1109/BCCA58897.2023.10338941
77. Li, G., Zhao, Q., Wang, Y., Qiu, T., Xie, K., Feng, L.: A blockchain-based decentralized framework for fair data processing. IEEE Trans. Netw. Sci. Eng. **8**(3), 2301–2315 (2021). https://doi.org/10.1109/TNSE.2021.3086332, https://doi.org/10.1109/TNSE.2021.3086332
78. Li, S.N., Yang, Z., Tessone, C.J.: Proof-of-work cryptocurrency mining: a statistical approach to fairness. In: 2020 IEEE/CIC international conference on communications in China (ICCC workshops). pp. 156–161. IEEE (2020)
79. Li, W.: Adapting blockchain technology for scientific computing. CoRR **abs/1804.08230** (2018), http://arxiv.org/abs/1804.08230
80. Liu, Y., Lan, Y., Li, B., Miao, C., Tian, Z.: Proof of learning (pole): Empowering neural network training with consensus building on blockchains. Comput. Net-

works **201**, 108594 (2021). https://doi.org/10.1016/J.COMNET.2021.108594, https://doi.org/10.1016/j.comnet.2021.108594

81. Loe, A.F., Quaglia, E.A.: Conquering generals: an np-hard proof of useful work. In: Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, CRYBLOCK@MobiSys 2018, Munich, Germany, June 15, 2018. pp. 54–59. ACM (2018). https://doi.org/10.1145/3211933.3211943, https://doi.org/10.1145/3211933.3211943
82. Ma, Z., Zhao, Q., Yuan, J., Zhou, X., Feng, L.: Fork probability analysis of pouw consensus mechanism. In: 2020 IEEE International Conference on Smart Internet of Things (SmartIoT). pp. 333–337. IEEE (2020)
83. Mahmoud, M.N.: Putting proof of work to work. Nature Energy **7**(6), 474–475 (2022)
84. Mail, C.J.: Pricing via processing. In: Advances in CryptologyCRYPTO92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 1620, 1992. Proceedings. Lecture Notes in Computer Science, vol. 740, p. 139. Springer (1992)
85. Males, U., Ramljak, D., Krüger, T.J., Davidovic, T., Ostojic, D., Haridas, A.: Controlling the difficulty of combinatorial optimization problems for fair proof-of-useful-work-based blockchain consensus protocol. Symmetry **15**(1), 140 (2023). https://doi.org/10.3390/SYM15010140, https://doi.org/10.3390/sym15010140
86. Mauri, L., Damiani, E., Cimato, S.: Be your neighbor's miner: Building trust in ledger content via reciprocally useful work. In: 13th IEEE International Conference on Cloud Computing, CLOUD 2020, Virtual Event, 18-24 October 2020. pp. 53–62. IEEE (2020). https://doi.org/10.1109/CLOUD49709.2020.00021, https://doi.org/10.1109/CLOUD49709.2020.00021
87. Merlina, A.: Blockml: a useful proof of work system based on machine learning tasks. In: Nawab, F., Rivière, E. (eds.) Proceedings of the 20th International Middleware Conference Doctoral Symposium, Middleware 2019, Davis, CA, USA, December 09-13, 2019. pp. 6–8. ACM (2019). https://doi.org/10.1145/3366624.3368156, https://doi.org/10.1145/3366624.3368156
88. Milutinovic, M., He, W., Wu, H., Kanwal, M.: Proof of luck: an efficient blockchain consensus protocol. IACR Cryptol. ePrint Arch. p. 249 (2017), http://eprint.iacr.org/2017/249
89. Mittal, A., Aggarwal, S.: Hyperparameter optimization using sustainable proof of work in blockchain. Frontiers Blockchain **3**, 23 (2020). https://doi.org/10.3389/FBLOC.2020.00023, https://doi.org/10.3389/fbloc.2020.00023
90. Noda, S., Okumura, K., Hashimoto, Y.: An economic analysis of difficulty adjustment algorithms in proof-of-work blockchain systems. Available at SSRN 3410460 (2019)
91. Oliver, C.G., Ricottone, A., Philippopoulos, P.: Proposal for a fully decentralized blockchain and proof-of-work algorithm for solving np-complete problems. arXiv preprint arXiv:1708.09419 (2017), https://arxiv.org/abs/1708.09419
92. Purkovic, S., Mekic, E., Kuk, K., Gostimirovic, L.: Empirical analysis of silent mining operation in the monero system. Studies in Informatics and Control **30**(4), 99–108 (2021)
93. Qu, X., Wang, S., Hu, Q., Cheng, X.: Proof of federated learning: A novel energy-recycling consensus algorithm. IEEE Trans. Parallel Distributed Syst. **32**(8), 2074–2085 (2021). https://doi.org/10.1109/TPDS.2021.3056773, https://doi.org/10.1109/TPDS.2021.3056773

94. Rebello, G.A.F., Camilo, G.F., Guimaraes, L.C., de Souza, L.A.C., Thomaz, G.A., Duarte, O.C.M.: A security and performance analysis of proof-based consensus protocols. Annals of Telecommunications **77**(7), 517–537 (2022)
95. Sabry, N., Shabana, B., Handosa, M., Rashad, M.: Adapting blockchains proof-of-work mechanism for multiple traveling salesmen problem optimization. Scientific Reports **13**(1), 14676 (2023)
96. Sabry, N., Shabana, B., Handosa, M., Rashad, M.: Adapting blockchains proof-of-work mechanism for multiple traveling salesmen problem optimization. Scientific Reports **13**(1), 14676 (2023)
97. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 515–532. Springer Berlin Heidelberg (2016)
98. Schrijvers, O., Bonneau, J., Boneh, D., Roughgarden, T.: Incentive compatibility of bitcoin mining pool reward functions. In: International Conference on Financial Cryptography and Data Security. pp. 477–498. Springer (2016)
99. Sehar, N.U., Khalid, O., Khan, I.A., Rehman, F., Fayyaz, M.A., Ansari, A.R., Nawaz, R.: Blockchain enabled data security in vehicular networks. Scientific Reports **13**(1), 4412 (2023)
100. Shibata, N.: Proof-of-search: Combining blockchain consensus formation with solving optimization problems. IEEE Access **7**, 172994–173006 (2019). `https://doi.org/10.1109/ACCESS.2019.2956698`, `https://doi.org/10.1109/ACCESS.2019.2956698`
101. Shibata, N.: Proof-of-search: Combining blockchain consensus formation with solving optimization problems. IEEE Access **7**, 172994–173006 (2019). `https://doi.org/10.1109/ACCESS.2019.2956698`, `https://doi.org/10.1109/ACCESS.2019.2956698`
102. Shoker, A.: Sustainable blockchain through proof of exercise. In: 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA). pp. 1–9. IEEE (2017)
103. Smajgl, A., Schweik, C.M.: Advancing sustainability with blockchain-based incentives and institutions. Frontiers in Blockchain **5**, 963766 (2022)
104. Sokhankhosh, A., Rouhani, S.: Proof-of-collaborative-learning: A multi-winner federated learning consensus algorithm. In: IEEE International Conference on Blockchain, Blockchain 2024, Copenhagen, Denmark, August 19-22, 2024. pp. 370–377. IEEE (2024). `https://doi.org/10.1109/BLOCKCHAIN62396.2024.00055`, `https://doi.org/10.1109/Blockchain62396.2024.00055`
105. Song, H., Zhu, N., Xue, R., He, J., Zhang, K., Wang, J.: Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection. Information processing & management **58**(3), 102507 (2021)
106. Soria, J., Moya Velasco, J., Mohazab, A.: Financial incentives of proof-of-work cryptocurrency mining. Available at SSRN 4225047 (2023)
107. Stoll, C., Klaaßen, L., Gallersdörfer, U.: The carbon footprint of bitcoin. Joule **3**(7), 1647–1661 (2019)
108. Taylor, M.B.: The evolution of bitcoin hardware. Computer **50**(9), 58–66 (2017)
109. Todorovic, M., Matijevic, L., Ramljak, D., Davidovic, T., Urosevic, D., Krüger, T.J., Jovanovic, D.: Proof-of-useful-work: Blockchain mining by solving real-life optimization problems. Symmetry **14**(9), 1831 (2022). `https://doi.org/10.3390/SYM14091831`, `https://doi.org/10.3390/sym14091831`
110. Toulemonde, A., Besson, L., Goubin, L., Patarin, J.: Useful work: a new protocol to ensure usefulness of pow-based consensus for blockchain. In: GoodIT 2022:

ACM International Conference on Information Technology for Social Good, Limassol, Cyprus, September 7 - 9, 2022. pp. 308–314. ACM (2022). https://doi.org/10.1145/3524458.3547248, https://doi.org/10.1145/3524458.3547248

111. Venkatesan, K., Rahayu, S.B.: Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Scientific Reports **14**(1), 1149 (2024)
112. Verheij, B.: The toulmin argument model in artificial intelligence: Or: how semi-formal, defeasible argumentation schemes creep into logic. In: Argumentation in Artificial Intelligence, pp. 219–238. Springer US, Boston, MA (2009)
113. Wang, S., Shi, L., Shi, H., Zhang, Y., Hu, Q., Cheng, X.: Proof of user similarity: The spatial measurer of blockchain. IEEE Trans. Serv. Comput. **17**(3), 1114–1125 (2024). https://doi.org/10.1109/TSC.2023.3347716, https://doi.org/10.1109/TSC.2023.3347716
114. Wijewardhana, D., Vidanagamachchi, S., Arachchilage, N.A.G.: Examining attacks on consensus and incentive systems in proof-of-work blockchains: A systematic literature review. CoRR **abs/2411.00349** (2024). https://doi.org/10.48550/ARXIV.2411.00349, https://doi.org/10.48550/arXiv.2411.00349
115. Wohlin, C., Kalinowski, M., Felizardo, K.R., Mendes, E.: Successful combination of database search and snowballing for identification of primary studies in systematic literature studies. Information and Software Technology **147**, 106908 (2022)
116. Wu, Y., Choi, S., Liu, G., Wang, X.: Proof of directed guiding gradients: A new proof of learning consensus mechanism with constant-time verification. In: IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2023, Dubai, United Arab Emirates, May 1-5, 2023. pp. 1–3. IEEE (2023). https://doi.org/10.1109/ICBC56567.2023.10174890, https://doi.org/10.1109/ICBC56567.2023.10174890
117. Xie, T., Zhang, J., Zhang, Y., Papamanthou, C., Song, D.: Libra: Succinct zero-knowledge proofs with optimal prover computation. In: Annual International Cryptology Conference. pp. 733–764. Springer (2019)
118. Zhang, F., Eyal, I., Escriva, R., Juels, A., Van Renesse, R.: REM: Resource-Efficient mining for blockchains. In: 26th USENIX Security Symposium (USENIX Security 17). pp. 1427–1444 (2017)
119. Zhao, Z., Fang, Z., Wang, X., Chen, X., Zhou, Y.: Proof-of-learning with incentive security. CoRR **abs/2404.09005** (2024). https://doi.org/10.48550/ARXIV.2404.09005, https://doi.org/10.48550/arXiv.2404.09005

Appendix

A PoW vs PoUW

This section addresses the fundamental concepts of PoW and PoUW mechanisms considering possible differences in terms of puzzle/challenge to be solved, randomness of the challenge, incentive structure, security of chain, etc. These characteristics can fundamentally undermine PoUW and jeopardize blockchain security. In theory, this consensus model may be attractive, but the question arises - "can it effectively address operational problems?"
Several research has been done in addressing the major differences in PoW and PoUW [83,55,13]. We discuss the differences based on five categories as shown in Table 1 which details the differences between PoW and PoUW with respect to the type of challenge (puzzle), its quality and randomness, time interval to add block in blockchain, redundancy in computation, and dependency on computing hardware. We see that the purpose of solving a puzzle is useful and meaningful in the case of PoUW, but it lacks uniform block time interval and quality of puzzle. Moreover, energy consumption is similar in both the cases due to high redundancy. Moreover, PoUW may demand higher and variable setup cost as it needs specialized hardware according to the challenge to be solved.

B Related Work

Fry et al. [48] quantitatively discovered that the energy consumption of the Bitcoin market may exceed its long-term benefit, particularly when considering environmental externalities. Stoll et al. [107] noted the severe carbon footprint of Bitcoin for sustainability issues. In response to the energy consumption issue, Proof of Stack (PoS) has been proposed as an alternative [66]. PoS dynamically adjusts the puzzle difficulty for each node based on the token holdings, favoring nodes with more token age consumed (TAC) to validate blocks. Moreover, other consensus protocols such as Proof of Luck [88] and Robust Proof of Stake [73] offer energy-efficient and sustainable solutions for blockchain networks. Despite these proposed consensus protocols, PoW remains widely accepted, particularly in permissionless blockchain architectures. There have been several studies done on developing usefulness in PoW. To capitalize on the surplus energy from hashing, several studies put forward the idea of adapting PoW to perform useful computations, aiming to improve energy efficiency while retaining its security properties [89]. Liu et al. [80] presented Proof-of-Learning (PoLe), which repurposed computing power to facilitate neural network training. Haouari et al. [52] leveraged PoW to solve the challenge by employing a concave cost function formulated as a mixed-integer nonlinear programming problem, reducing the transportation cost by 35%. Lasla, et al. [72] proposed Green-PoW, preserving energy consumption by up to 50%. Sabry [95] et al. employed PoUW to optimize the Travelling Salesman Problem (TSP) by reducing the block generation time by approximately 11%. Moreover, to address controlling and maintaining the `difficulty` of the tasks provided to the miners, researchers proposed the optimization problem instances [79,81]. However, it was deduced that the size of the instance did not always directly correspond to the runtime of the selected optimization algorithm [59]. Therefore, some of the later approaches included a request to provide proof of the respective work done, such as Proof-of-Search [100], where the miners are requested to solve an optimization problem instance as well as a cryptographic hash puzzle (same as PoW).

Recently, Proof of Necessary Work (PoNW) was developed by Kattis et. al. [63]. PoNW is about replacing wasteful hash grinding with verifiable computations that the blockchain must perform anyway. Despite repurposing its usefulness, PoNW does not contribute to societal utility. Moreover, generating succinct proofs or complex state verifications requires highly specialized hardware and expertise, which demotivates the adoption. The most important point where PoNW lacks is the negligible demand for useful work in the external market. The miners will lose motivation if they do not foresee the possibilities of receiving even a partial incentive. Hoffmann [55] surveyed the existing projects that incorporate several theoretical, biological, and machine learning problems into the PoUW mechanism. The survey shows a *more usefulness, more challenge* phenomenon in the existing works. In this direction, the Primecoin [65] has been the most advanced and deployed on chain, but the number-theoretical problem in Primecoin may be of limited interest to the general public, except mathematicians. Whereas, Coinami [60,11] proposes a solution to solve DNA sequencing problems, but it needs a centralized authority. Dotan et al. [40] mathematically explain that the security of the system originates from the economic incentive, which is created by the demand for solutions to the real-world problems, but they lack fairness in the random assignment of the challenge to the miners. Cao et al. [24] claim that most existing studies rely on either specific problems or particular algorithms, and they lack comprehensive security analysis for optimization-based PoUW.

C Existing PoUW mechanisms

Table 2 details the existing PoUW mechanisms in several categories with their references, which are studied and considered in this paper. Figure 4 shows the classification of the existing PoUW approaches in various domains.

D PoW based Cryptocurrencies

To ensure that our sample reflects real, operational networks rather than purely theoretical ones, we chose the set of PoW coins listed on CryptoSlate[4] under 'Proof-of-Work Cryptocurrencies' (see Table 3)

[4] https://cryptoslate.com/cryptos/proof-of-work/

Categories	Useful Work(s) in PoUW	References
Biomedical	Training Deep Neural Network, securing IoMT, and optimising via Genetic Algorithms in Biomedical	[21], [74], [50]
Data Scheduling	Data scheduling in decentralised data fairness and Proof-of-Data	[77], [58]
Energy	Optimizing and trading energy via Proof-of-Solution, Proof-of-energy, and HEP using Gophy	[57], [17], [29], [83]
Electric Vehicles	EV networks consensus algorithms such as Proof of Lightweight Hash	[31], [99]
File & Storage Systems	File & Storage systems implementing Proof-of-revocation, Proof-of-authority through Interplanetary File System (IPFS) networks	[5], [3], [4]
Graph & Matrix	Matrix-based computation by Proof-of-eXercise and Proof-of-Computation, and a useful PoW to find a minimal dominating set of real-life graph	[41], [102], [25]
Intellectual Property	IP protection by the development of Proof-of-Computation	[105]
Internet of Things	Fork probability analysis of PoUW in low-level energy devices and Internet of Things (IoT)	[82]
Machine Learning/ Artificial Intelligence	Training models in Proof-of-(collaborative/federated/deep learning verifying the training integrity of pool workers	[104], [111], [87], [42], [12], [116], [76], [93], [38], [75], [104], [86], [67]
Optimization	Optimizing MST anonymously, Multiple TSP Problem, and combinatorial optimization by, e.g., Proof-of-Search	[14], [34], [96], [85], [101]
Supply Chain & Logistics	Solving the NP-hard optimization problem of minimizing the total cost in supply chain	[53]
Unspecified PoUW Protocol	Real-world solution in HashCash, decentralized computation using Proof-of-Crowdsourcing Work, utilising energy by Proof-of-Prestige, energy recycling consensus mechanism called Proof-of-User-Similarity, etc.	[15], [2], [26], [69], [56], [110], [27], [28], [113], [71]

Table 2. PoUW Literature references in a nutshell

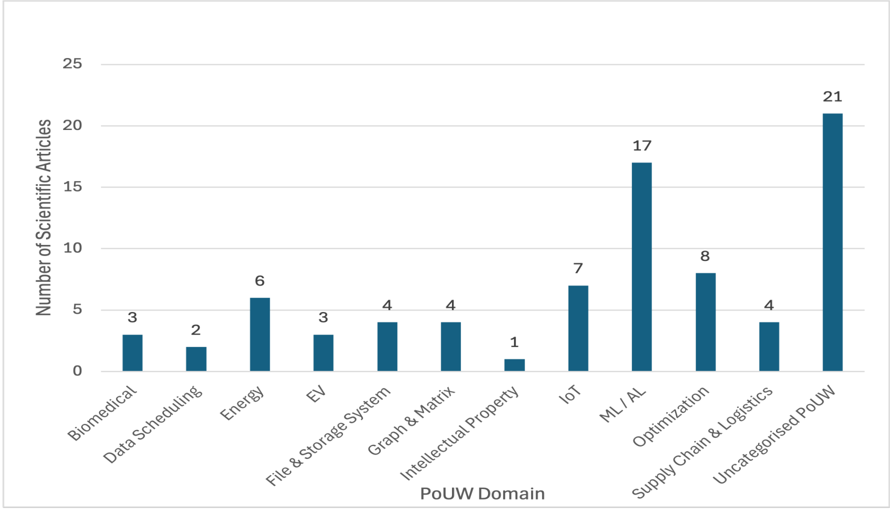


Fig. 4. Number of Scientific Articles categorized as per the useful work performed in PoUW challenges

E Toulmin Model

The Toulmin model [112] is a structured framework for argumentation. It systematically builds the components of an argument in the form of claim, data, warrant, backing, qualifier, and rebuttal which address the assertion, and why and under what circumstances the argument holds following the framework showcased in Figure 5. The details of the claims are as follows:

E.1 Unjustified Energy Efficiency

Claim. The PoUW mechanism does not achieve meaningful energy efficiency compared to traditional PoW, despite its intended purpose.
This claim stands with strong `Data` as described in Hypothesis 4, and `Backing` of studies on implementations such as Primecoin[65] and CoinAI[11] that confirm that most computational effort is discarded, undermining claims of energy savings. The `Warrant` explains that a consensus mechanism can only be considered energy-efficient if the majority of effort contributes meaningfully to both security and utility, yet PoUW fails to meet this bar as discussed in Hypothesis 3. As `Qualifier`, this argument holds for PoUW mechanisms with competitive incentive structure with single-winner incentive scheme, and whose solution is not reusable. There exists a weak counter-argument as a `Rebuttal` on the moral ground that PoUW at least produces some useful work, but rationally the scale of wasted effort remains comparable to that of PoW.

Table 3. Status of Evaluated Proof-of-Work Cryptocurrencies

Category	**Cryptocurrencies**	**Count**
Fully Evaluated (Pure PoW)	Bitcoin (BTC), Dogecoin (DOGE), Bitcoin Cash (BCH), Litecoin (LTC), Monero (XMR), Ethereum Classic (ETC), Kaspa (KAS), Zcash (ZEC), Bitcoin SV (BSV), Nervos Network (CKB), Ravencoin (RVN), Siacoin (SC), EthereumPoW (ETHW), Zano (ZANO), DigiByte (DGB), Kadena (KDA), Verge (XVG), Ergo (ERG), Flux (FLUX), Alephium (ALPH), MonaCoin (MONA), Grin (GRIN), Bytecoin (BCN), Litecoin Cash (LCC), Groestlcoin (GRS), Luckycoin (LKY), Handshake (HNS), Vertcoin (VTC), Beam (BEAM), Bitcoin Gold (BTG), XELIS (XEL), Namecoin (NMC), Mochimo (MCM), MicroBitcoin (MBC), Nexa (NEXA), Epic Cash (EPIC), Clore.ai (CLORE)	37
Partially Covered (Limited Documentation)	Dingocoin (DINGO)	1
Excluded (Hybrid / Not Pure PoW)	Dash (DASH), Firo (FIRO), Syscoin (SYS), Pirate Chain (ARRR), Peercoin (PPC), Conflux (CFX)	6

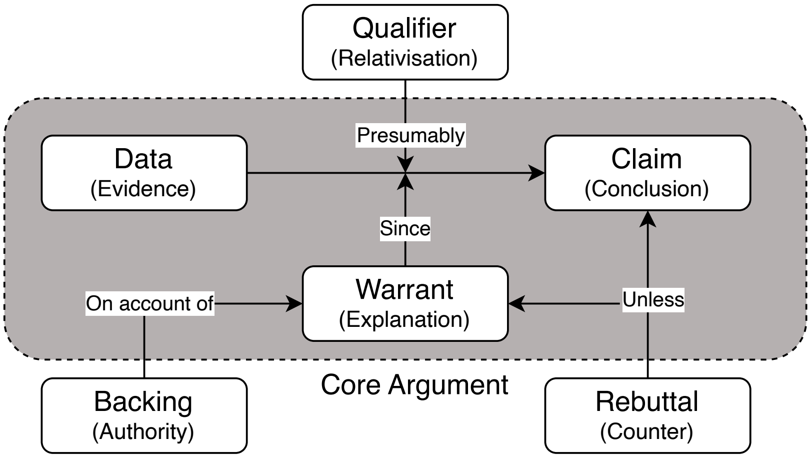


Fig. 5. Toulmin model.

E.2 Unfair incentive Structure

Claim. The unfair incentive structure in PoUW may develop economic instability leading to lack of miners' participation.
The `Data` is available demonstrating that PoUW incentivizes participation only when expected on-chain incentives and potential market value of solutions exceed operational costs according to Hypothesis 3. Nevertheless the `Warrant` holds as concentration of incentives at a single winner. Most miners face unincentiveed

losses and may turn to off-chain trading. Moreover, if the primary incentive for solving the designated real-world problem is perceived as inadequate, miners may reduce investing in the computational resources and specialized hardware leading to a decline in the network's overall security budget. However the `Qualifier` for this claim stands with the successful miner who retains ownership of the solution. This allows them to engage off-chain if there is a demand in the secondary market. Specifically, those miners who are not the primary winner, but are successful in solving the full or partial tasks, are more prone to participate in the secondary market, potentially leading to the proliferation of solutions within a off-chain market due to the lack of a formalized incentive mechanism in the PoUW mechanism. This could introduce vulnerabilities and security risks. This data has `Backing` which addresses the economic viability of sustained miner involvement, unless all the miners gets equal opportunity to participate and proportionate chance of being incentiveed fairly the inherit incentive structure continues possessing unfairness. There exists a moderate `Rebuttal` for mechanisms like partial incentive schemes or modular task-sharing have been suggested, but they introduce complexity and remain rare, meaning that most PoUW systems cannot ensure equitable or stable incentives.

E.3 Difficulty in Difficulty Adjustment

Claim. The inability to reliably regulate task difficulty leads directly to unpredictable block times, which undermines fairness and network stability.
The `Data` is evident in implementations e.g., DLChain [30] and Proof-of-Solution [29] which shows that when solutions fail or verification stalls, block times fluctuate dramatically, sometimes doubling, and this weakens throughput while raising the likelihood of forks and chain splits. Since `Warrant` holds for a blockchain stability, both the probability of solving a challenge and the timing of block creation must be predictable so that incentives are distributed fairly and the risk of forks or instability is minimized. This is supported by `Backing` of prior studies [43,33] and case analyses confirm that block time fluctuations in PoUW not only reduce throughput but also create persistent inequalities among miners with different hardware or task-specific advantages. This has `Qualifier` which applies primarily to competitive PoUW schemes with complex or externally submitted tasks, where runtimes cannot be standardized, it may be less severe in systems using narrow, domain-specific problems. Though, a moderate `Rebuttal` can be considered where some argue that splitting tasks into subtasks or imposing strict time limits can mitigate these issues, but such fixes introduce coordination overhead and risks of centralization, leaving PoUW unable to match PoWs proven robustness in regulating block times at scale.

E.4 Lack of Degree of Randomness

Claim. PoUW mechanisms lack sufficient randomness in challenge assignment, which creates risks of bias and centralization in the mining process.

The Data shows PoUW relies on externally provided problems, and these tasks can be biased, pre-solved, or manipulated, allowing miners with prior knowledge or specialized hardware to gain an unfair advantage. This is because the Warrant states that randomness in challenge selection is essential to ensure fairness, equal opportunity, and protection against manipulation, without which consensus loses its resistance to adversarial influence. This is backed by Backing of prior research which shows that real-world problem submissions in PoUW can be controlled by malicious parties, enabling attacks such as the known-model attack, where a problem with a precomputed solution is submitted, or the model-stealing attack, where a miner reuses work trained by others [119]. The claim is legit under Qualifier where the weakness is most pronounced in permissionless PoUW systems with external problem providers, whereas restricted or domain-specific implementations may reduce, but not eliminate, the risk. There exists a strong Rebuttal in the randomness reintroduction by parameterizing problems with blockchain-derived seeds (e.g., using the previous block hash), such measures diminish the original utility of the task, undermining the very usefulness objective that PoUW aims to achieve.