Enabling Computational Democratization: A Proof-of-Stake Bounty System for User-Proposed Problems and Solutions

Nishka Arora
Computing + Mathematical Sciences
California Institute of Technology
Pasadena, California, USA
naarora@caltech.edu

Sarah Hashash
Computing + Mathematical Sciences
California Institute of Technology
Pasadena, California, USA
shashash@caltech.edu

Kimia Hassibi*
Computing + Mathematical Sciences
California Institute of Technology
Pasadena, California, USA
khassibi@caltech.edu

2023 IEEE MIT Undergraduate Research Technology Conference (URTC) | 979-8-3503-0965-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/URTC60662.2023.10535013

***Abstract*—Traditional proof-of-work (PoW) based cryptocurrencies require miners to solve hash functions, resulting in enormous energy waste. Proof-of-stake (PoS) is an energy-efficient alternative to PoW. However, PoS alone fails to create incentives for PoW miners to switch away from PoW due to their existing hardware investments that provide a competitive financial advantage. Thus, we introduce a framework that replaces energy wasted on PoW cryptocurrencies with a modified PoS consensus mechanism that allows miners to be rewarded for solving user-proposed problems. This mechanism could serve as a decentralized cloud computing platform.**

***Index Terms*—proof-of-useful-work, proof-of-stake, consensus mechanism, cryptocurrency**

I. Introduction

Many cryptocurrencies, such as Bitcoin, rely on proof-of-work (PoW), which is a consensus mechanism in which participants, called miners, solve computationally intensive cryptographic puzzles, such as hash functions, to validate and add financial transactions to a ledger called the blockchain. Solving these hash functions is equivalent to repeatedly guessing random numbers. Since the solutions to these hash functions are random, the miner that finds a solution and is able to add transactions to the blockchain is randomly chosen. In this way, there is no single authority that decides which transactions are valid; instead, the cryptocurrency is decentralized.

The number of guessed solutions probabilistically required for a miner to solve a hash function makes finding this solution computationally expensive. As a result, miners invest in hardware equipment such as application-specific integrated circuits (ASICs) and graphics processing units (GPUs) that use immense amounts of energy. It is currently estimated that Bitcoin alone consumes 127 terawatt-hours a year [1].

Our desired cryptocurrency is **decentralized** and has its energy go towards solving socially **useful** problems. These problems must be **inexhaustible** and **unanticipatable**.

A. Existing Alternatives

To address the energy waste from PoW cryptocurrencies, researchers have proposed and implemented proof-of-useful-works (PoUWs). PoUWs are PoWs for which the computational power expended is socially beneficial.

A PoUW cryptocurrency, Primecoin, replaces the hash function with the goal of finding chains of prime numbers, such as Cunningham and bi-twin chains [2]. Cunningham chains are series of prime numbers that nearly double each time. However, the usefulness of such a chain is limited [3].

Coinami is a cryptocurrency that involves generating and analyzing huge datasets of disease DNA signatures [2]. Coinami relies on a 3-level multi-centric system with a root authority, sub-authorities, and miners. Miners receive from sub-authorities lists of DNA sequences to align. Their proof-of-work consists of mapping HTS reads to the reference genome and sending results back for verification. While Coinami problems are unanticipatable and inexhaustible, the 3-level multi-centric system lends itself to a high degree of centralization that forces miners to trust any sub-authority.

Cuckoo Cycle [4] is a consensus mechanism based on finding subgraphs with a particular structure in large random graphs. Specifically in [4], miners search for small n-cycles in a graph. The paper requires miners to randomly generate an Erdos-Renyi graph using the hash of the previous block in the chain until a graph with an n-cycle is found. The generalizability of this Cuckoo Cycle provides exciting avenues for further exploration. There may be real-world problems that involve finding subgraphs in large graphs, but because the graphs in Cuckoo Cycle are randomly generated, the majority of them may not have useful applications. Therefore, Cuckoo Cycle will still generate a significant amount of aimless computation.

While Cuckoo Cycle has a cryptographic puzzle that can have useful solutions, the paper "Difficulty Scaling in Proof of Work for Decentralized Problem Solving" (DIPS) [5] takes a different approach. It proposes a framework where miners are incentivized to solve a useful NP-complete problem because this gives them an advantage that reduces the computation

*NA, SH, KH are listed in alphabetical order and contributed equally

979-8-3503-0965-2/23/$31.00 ©2023 IEEE

required to solve the hash function necessary to add a block. DIPS involves storing a list of NP-complete problems on the genesis block of the blockchain. A miner solves one of these NP-complete problems by proposing a better solution than any pre-existing solution on the chain. The NP-complete problems chosen to be in the genesis block can be ones that have specific real-world applications. Therefore in DIPS, miners have the option to swap useless computation with more useful work. However, most of the computation in DIPS is still solving a traditional hash function. Another issue is that the number of problems on the genesis block is finite and immutable. Therefore, if all problems are exhausted, DIPS is a regular PoW.

Table 1 demonstrates the lack of coexistence between unanticipatibility, usefulness, inexhaustibility, and decentralization in current cryptocurrency consensus mechanisms. Existing alternatives are only able to provide fully useful work by having some level of centralization. Other solutions have been able to remain decentralized and offer unanticipatable problems through randomly generating problems. However, it is not always possible to find a use for a problem that is randomly chosen from an inexhaustible set of problems.

An alternative consensus mechanism to PoW is proof-of-stake (PoS), which significantly reduces the energy expended when running a cryptocurrency. Instead of requiring agents to do computationally intensive work in order to be given the privilege to add transactions to the blockchain, PoS cryptocurrencies probabilistically pick these agents using staking. As a result, PoS uses significantly less energy than PoW.

Specifically, in Ethereum, each agent that wants to add transactions to the blockchain must first deposit some ETH cryptocurrency as stake [6]. After staking, the agent joins an activation queue that periodically chooses agents to become validators. The activation queue chooses these agents at random, with agents that stake higher having an increased likelihood of being picked. As a validator, an agent has the ability to vote, or give an *attestation*, about the validity of a block of transactions. Gaining a certain threshold of attestations means that the block is valid and can be added to the blockchain. Some of the validators in the voting group are picked at random to put together transactions in the blocks that all the validators vote on.

While PoS significantly reduces the amount energy required, a majority of PoW miners have not switched to PoS currencies. This is due to many miners having existing hardware investments that provide them with a competitive financial advantage in PoW that does not exist in PoS.

B. Impact

Currently, no available cryptocurrency fully addresses these requirements. Typically, a trade-off exists between preserving decentralization and the overall usefulness of the hash function. Cryptocurrencies that are designed to only spend energy on solving useful problems fail to have problem sets that are inexhaustible [2]. Once exhausted, they default to solving energy-wasteful hash functions, violating the desired characteristics. Additionally, some cryptocurrencies fail to be decentralized due to having central authorities in the network in order to validate solutions and to ensure the safe exchange of currencies [2].

To address the current lack of a comprehensive alternative, we present a decentralized framework, called QAExchange, for solving an inexhaustible set of useful problems. QAExchange has a PoS bounty system in which users can propose any type of problem and receive a solution, in turn. These problems will be useful by design since a user is willing to pay for the solution. QAExchange will allow any individual to have access to computational resources at a market-determined rate. We seek to lay the groundwork of a system that will allow users to make peer-to-peer transactions and to access cloud computing.

In summary, we propose an alternative to PoW cryptocurrencies. The goal is to give current PoW miners a financial incentive to switch to QAExchange because their compute power can win bounties for solving problems. Since all the energy expended in QAExchange is spent on keeping track of financial transactions and solving user-proposed problems, the work done is useful.

The remainder of the article is divided into three sections. The next part of the paper (Section 2) highlights the key features of QAExchange and its implementation. Section 3 discusses the safety of the system against attacks. In the last section, we conclude with a discussion of the environmental and social usefulness of QAExchange.

TABLE I
COMPARISON OF CRYPTOCURRENCY PROPERTIES

	Properties			
Mechanism	***Inexhaustible***	***Unanticipatable***	***Useful***	***Decentralized***
Primecoin	✓	✓	✗	✓
Cuckoo Cycle	✓	✓	✗	✓
DIPS	✗	✗	✓	✓
Coinami	✓	✓	✓	✗

II. SOLUTION

Rather than listing pre-decided useful problems or randomly generating problems that may not be useful, QAExchange allows validators to propose problems that can be solved on the blockchain for a bounty. QAExchange uses the PoS consensus mechanism and converges to only PoS if no problems are proposed.

There are two types of entities: users and validators.

1) **Users** exchange currency via transactions.
2) **Validators** verify and add blocks of transactions to the blockchain in exchange for a fee. There are two subcategories of validators: (a) proposers and (b) solvers.
    a) **Proposers** have the capability to propose problems in the block they create.
    b) **Solvers** have the capability to solve a problem proposed in the blockchain and add the solution to the block they create.

Visualizations of the blocks that proposers and solvers create are shown in Fig. 1. In their block, a proposer includes a set of valid transactions, the problem, the problem's ID, and a bounty. The bounty is the offer that the proposer makes for the correct solution. When the proposer creates a block, the bounty is withdrawn from the proposer's wallet and is inaccessible until it is transferred to the solver that offers a correct solution. A solver's block includes a valid set of transactions, a solution to an unsolved problem on the blockchain, and the problem's ID.

As in a typical PoS cryptocurrency, agents deposit cryptocurrency as *stake* in order to become a validator. An algorithm probabilistically determines who the next group of validators will be, with agents that stake more having a higher chance of becoming validators. Out of the group of validators, a select few are randomly chosen to each create a block of transactions that will be added to the blockchain. These block creators can become proposers or solvers and add a problem or a solution to the block, respectively. The group of validators is tasked with giving attestations on whether or not these prospective blocks have valid transactions. If a block is invalid, the validator that created it will lose a portion of its stake, and the block will not be added to the blockchain. In the case that the block creator is a solver, the group of validators also gives attestations on whether or not the solver's solution is correct. If it is correct, then the bounty of the problem will be sent to the solver. If it is incorrect, then the problem will remain unsolved on the blockchain for another solver to offer up a solution. All validators are rewarded if the block they put on the chain has correct information. Fig. 2 depicts this process.

So far, there are no restrictions on the type of problems that may be added to the blockchain. However, for the scope of this paper, it is useful to limit the possible problems to those in the complexity class NP. Problems in NP can be verified in polynomial time, allowing validators to verify the correctness of a proposed solution quickly. To this end, proposers must include in their problem encoding the process in which a solution can be verified.

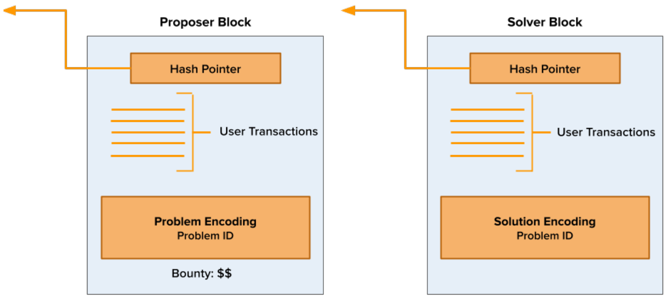

Fig. 1. Diagram of Proposer and Solver Blocks

A. System Architecture

The system architecture of QAExchange can be seen in Fig. 3. QAExchange has a low-level blockchain class with definitions for transactions, blocks, hashing, and encryption.

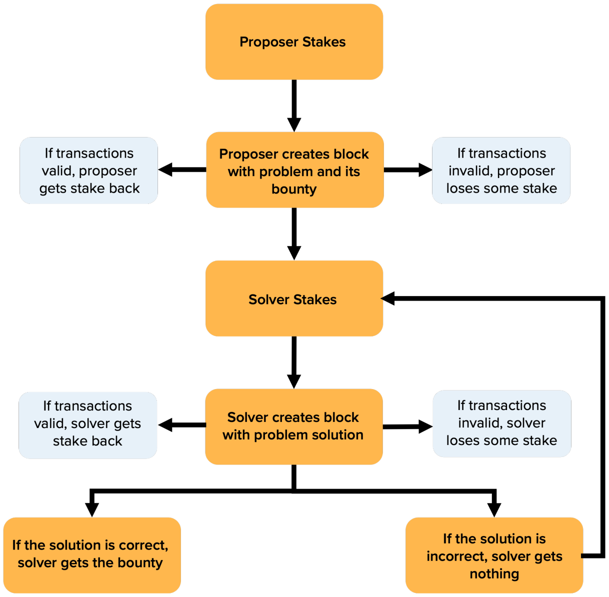
Proposer Stakes
If transactions valid, proposer gets stake back
Proposer creates block with problem and its bounty
If transactions invalid, proposer loses some stake
Solver Stakes
If transactions valid, solver gets stake back
Solver creates block with problem solution
If transactions invalid, solver loses some stake
If the solution is correct, solver gets the bounty
If the solution is incorrect, solver gets nothing

Fig. 2. Flowchart of Exchange

It also provides space for problem and solution encodings and IDs. Above this layer, there is a peer-to-peer (P2P) network layer where peer clients request the current state of the blockchain from other peers and carry out verification. This layer allows for the decentralized propagation of the blockchain. The consensus mechanism is implemented on top of the P2P network layer, enabling validators to communicate information, such as stakes and attestations. Finally, there is a consumer interface layer on the very top that allows clients to either become validators (proposers or solvers) or simply users of the currency [7].

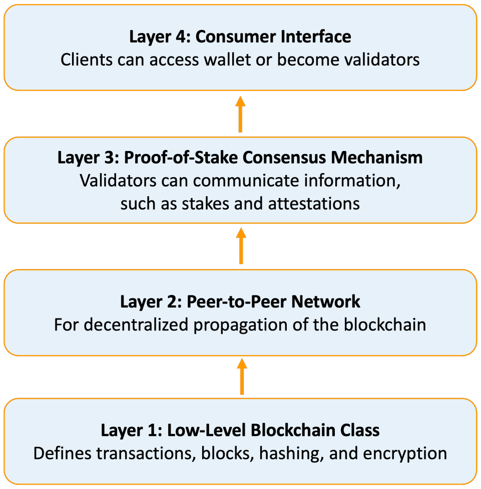
Layer 4: Consumer Interface
Clients can access wallet or become validators
Layer 3: Proof-of-Stake Consensus Mechanism
Validators can communicate information, such as stakes and attestations
Layer 2: Peer-to-Peer Network
For decentralized propagation of the blockchain
Layer 1: Low-Level Blockchain Class
Defines transactions, blocks, hashing, and encryption

Fig. 3. Layers of QAExchange Architecture

III. Discussion of Safety

This section explores some properties of QAExchange and addresses potential concerns about its safety.

A. QAExchange is at least as safe as other proof-of-stake architectures

The underlying architecture of QAExchange is PoS (if no agents propose or solve problems, QAExchange is a PoS currency). Therefore, QAExchange has the same protections in place as other cryptocurrencies that use the PoS consensus mechanism. These include protections against the 51% attack, Sybil attack, double-spend attack, and long-range attack.

B. System is unaffected by collusion between a proposer and a solver

There is a potential for a proposer, P, to reveal a problem to a specific solver, S, before P has added the problem to the blockchain. Knowing the problem beforehand, S can pre-solve the problem. Pre-solving does not lead to any attacks. Due to the random chance involved in staking, having a solution to a problem does not give S an increased chance to add a block to the chain. Thus, it is not possible for back-to-back blocks to be added to the chain by a party without other parties being able to check them. Therefore, when collusion occurs, the QAExchange architecture is not susceptible to an attack similar to the 51% attack.

In addition, a solver can only make as much money from solving a problem as the proposer gave as the bounty. Therefore, even if S is able to add a block to the chain with the solution to P's problem, this is simply equivalent to P transferring money directly to S.

C. System still works when problems are too hard to solve

When a problem is too hard to solve, there will either be no attempted solutions to it on the blockchain or there will be solutions that are all rejected. As such, a hard problem will remain unsolved as time goes on. This problem will exist earlier in the blockchain, indicating its difficulty to solvers that may decide that the problem is not worth trying to solve at the moment. As knowledge and technology progress, a solver may one day be able to add a correct solution for this problem to the blockchain. In addition, if the price of QAExchange rises over time, the older questions will become more valuable incentivizing solvers to attempt those hard problems.

D. Validators are disincentivized from lying

Validators check the correctness of transactions within a block. This idea is extended to include checking the correctness of the solutions in blocks posed by solvers. If the attestation of a validator is consistent with the majority of attestations, the validator receives a reward [8]. If instead, the validation work is incorrect, the validator incurs a penalty. This system of rewards and penalties incentivizes validators to act truthfully when verifying both transactions and solutions.

IV. Concluding Remarks

With the environmental harms of cryptocurrency mining in its current state, finding alternatives that harness the energy of mining to solve socially useful problems is important. QAExchange satisfies all 4 of the desired properties.

(1) QAExchange is **decentralized** because its consensus mechanism is PoS. (2) The work done is **useful** because it goes towards solving problems whose solutions are valuable, as demonstrated by the fact that users are willing to pay for these solutions. (3) The problems are **inexhaustible** because they can always be proposed on the blockchain. (4) The problems are **unanticipatable** because the parties proposing and solving problems are separate. For cases in which there is collusion between these parties, safety is maintained.

Our system extends the capabilities of existing cryptocurrency systems by doubling as a platform for computational access. Any individual with access to computational devices or with a need for computation can join the network. A forward look into the potential implications of this system is providing an alternative means of computational resources for startups and researchers.

Acknowledgment

The authors would like to thank Professor Adam Wierman for his guidance and encouragement.

References

[1] R. Mills. “Cryptocurrency's energy consumption problem.” (Jan. 2023), [Online]. Available: https://rmi.org/cryptocurrencys-energy-consumption-problem/.

[2] F. Hoffmann, “Challenges of proof-of-useful-work (pouw),” in *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain Beyond (iGETblockchain)*, Jun. 2022, pp. 1–5. DOI: 10.1109/iGETblockchain56591.2022.10087185.

[3] S. King, “Primecoin: cryptocurrency with prime number proof-of-work,” Jul. 2013. [Online]. Available: https://primecoin.io/primecoin-paper.pdf.

[4] J. Tromp, “Cuckoo Cycle: A Memory Bound Graph-Theoretic Proof-of-Work,” in *Financial Cryptography and Data Security*, M. Brenner, N. Christin, B. Johnson, and K. Rohloff, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 49–62, ISBN: 978-3-662-48051-9.

[5] P. Philippopoulos, A. Ricottone, and C. G. Oliver, “Difficulty scaling in proof of work for decentralized problem solving,” *Ledger*, vol. 5, Aug. 2020. DOI: 10.5195/ledger.2020.194.

[6] Corwin Smith, Joseph Cook, Masoud Ghorbanzadeh, *et al.* “Proof-of-stake (pos).” (May 2023), [Online]. Available: https://ethereum.org.

[7] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, *et al.*, “A survey on blockchain technology: Evolution, architecture and security,” *IEEE Access*, vol. 9, pp. 61 048–61 073, 2021. DOI: 10.1109/ACCESS.2021.3072849.

[8] Paul Leydier, Sebastian Supreme, Pedro Simon, Paul Wackerow, and Joseph Cook. “Proof-of-stake rewards and penalties.” (Jul. 2023), [Online]. Available: https://ethereum.org.