Crowdsourcing Work as Mining: A Decentralized Computation and Storage Paradigm

Canhui Chen∗
Tsinghua University
Beijing, China

Zerui Cheng∗
Tsinghua University
Beijing, China

Shutong Qu
Tsinghua University
Beijing, China

Zhixuan Fang†
Tsinghua University, Beijing, China
Shanghai Qi Zhi Institute, Shanghai, China

ABSTRACT
In this paper, we propose a novel and energy-efficient blockchain system, CrowdMine, which exploits useful crowdsourcing computation to achieve decentralized consensus. CrowdMine solves user-proposed computing tasks and utilizes the computation committed to the task solving process to secure decentralized on-chain storage. With our designed “Proof of Crowdsourcing Work” (PoCW) protocol, our system provides an efficient paradigm for computation and storage in a trustless and decentralized environment. We also implement the system with 40 distributed nodes to demonstrate its performance and robustness.

CCS CONCEPTS
• Information systems ➔ Crowdsourcing; • Security and privacy ➔ Economics of security and privacy.

KEYWORDS
blockchains, proof-of-useful-work, mechanism design

1 INTRODUCTION
Blockchain, with Bitcoin and Ethereum as its prevalent representatives, is a decentralized ledger that commits consensus and trust among distributed participants. To coordinate the decentralized record generation, most blockchain systems adopt the Proof of Work (PoW) mechanism (e.g., Bitcoin). Specifically, PoW evaluates miners’ computing power in solving random cryptographic problems and chooses the next block creator in proportion to their computing power. Although the computation results are useless, the computational effort from miners is in general considered to be a guarantee for security.

To address the challenge of energy waste in blockchain, in this paper, we propose a new decentralized computing system, CrowdMine. The system is decentralized and permissionless. The key idea of our paradigm is that we utilize miners’ computation resources to solve actual computing tasks proposed by distributed problem proposers (i.e., users), instead of solving the meaningless hash puzzle in PoW. More importantly, we also utilize this useful computation to secure the transactions in the blockchain. We further show that CrowdMine can efficiently defend against the short-term 51% attack, the problem-constructing attack, and the solution-stealing attack, maintaining security in the long term. We summarize the design principles of the system as follows.

• A miner is eligible to create a new block if and only if the miner successfully finishes a computational task (i.e., solves a "problem"), either proposed by users or the system. Thus, we utilize miners’ resources for useful computation.

• We measure the miner’s computational contribution by the reward of the task, and propose the Maximum Aggregated Value protocol (MAV) to resolve forking branches.

• Eligible miners publish blocks according to the proposed Proof of Crowdsourcing Work (PoCW) protocol. PoCW chooses miners with probabilities in proportion to their computational contribution to users’ proposed tasks.

In our system, any user problem whose solution is easy to verify can be initiated and get solved by miners, and the value of each problem is determined by a computation power marketplace affiliated with our system. Compared with existing literature on Proof-of-Useful-Work [1][2][4], our system offers the maximum ever flexibility to users in the sense of both problem category and pricing, whereas the security, liveness, and decentralization of our system are still guaranteed.

2 SYSTEM ARCHITECTURE
Figure 1 demonstrates the workflow for users and miners. To propose a user problem, a user needs to initiate a transaction called ProposalTx (Proposal Transaction for brevity), which specifies the problem and its reward.

During the mining process, miners can either pick up one user problem to solve, or solve a system problem. To prevent the solution from being stolen, the miner should follow the Commit-Reveal...
In this paper, we design a blockchain-based permissionless and decentralized storage and computing paradigm. With the proposed Proof of Crowdsourcing Work (PoCW) mechanism, we show the energy efficiency and security of the system. We also implement the system with up to 40 decentralized nodes, and the experiment results demonstrate the excellent efficiency and performance of our proposed paradigm.

REFERENCES
[1] Marshall Ball, Alon Rosen, Manuel Sabin, and Prashant Nalini Vasudevan. 2017. Proofs of Useful Work. IACR Cryptol. ePrint Arch. 2017 (2017), 203.
[2] Mohamed Haouari, Mariem Mhiri, Mazen El-Masri, and Karim Al-Yafi. 2022. A novel proof of useful work for a blockchain storing transportation transactions. Information Processing & Management 59, 1 (2022), 102749.
[3] Joseph Poon and Thaddeus Dryja. 2016. The bitcoin lightning network: Scalable off-chain instant payments.
[4] Fan Zhang, Ittay Eyal, Robert Escriva, Ari Juels, and Robbert Van Renesse. 2017. REM: Resource-efficient mining for blockchains. In 26th {USENIX} Security Symposium ({USENIX} Security 17). 1427–1444.