Journal Club Presentation

Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm
Elsevier, Computer Networks, 2022

Seungmin Kim

2024.01.10

Paper Introduction

- ✓ Lasla, N., Al-Sahan, L., Abdallah, M., and Younis, M.: **'Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm'**, Computer Networks, 2022, 214, pp. 109118
- ELSEVIER, Computer Networks, IF 5.6
- Keywords: Blockchain; Consensus algorithm; Proof-of-Work; Energy-efficiency

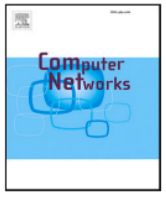
- Goal of Paper: Reducing overall energy consumption without compromising the security level of PoW

Computer Networks 214 (2022) 109118

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm

Noureddine Lasla [a,*], Lina Al-Sahan [a], Mohamed Abdallah [a], Mohamed Younis [b]

[a] Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar
[b] University of Maryland, Baltimore County, Baltimore, MD, USA

EDITION
Science Citation Index Expanded (SCIE)

CATEGORY
COMPUTER SCIENCE, HARDWARE & ARCHITECTURE
8/54

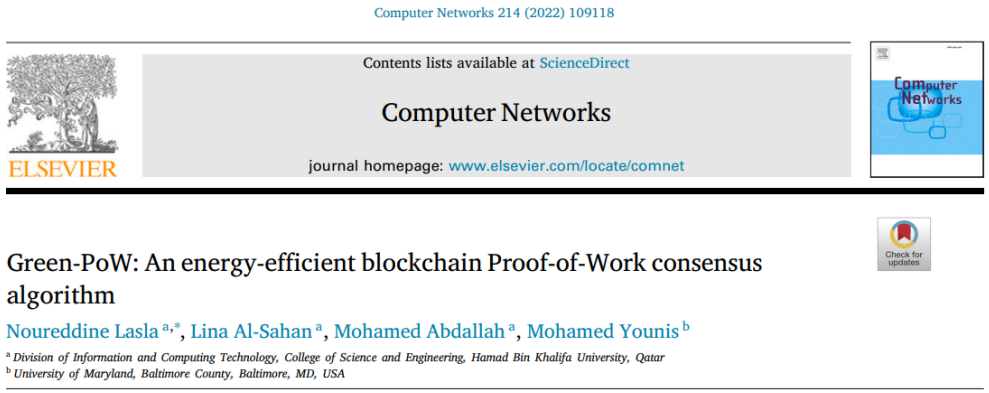
JCR YEAR	JIF RANK	JIF QUARTILE	JIF PERCENTILE
2022	8/54	Q1	86.1

Why this paper?

The purpose of this paper is consistent with the purpose of VRF-POW, which I study

=> Reducing energy consumption under a public proof-of-work blockchain (without proof-of-stake or identity authentication)

This is the most actively cited PoW energy saving paper recently.


Computer Networks 214 (2022) 109118

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm

Noureddine Lasla [a,*], Lina Al-Sahan [a], Mohamed Abdallah [a], Mohamed Younis [b]

[a] Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar
[b] University of Maryland, Baltimore County, Baltimore, MD, USA

Goal is Same!

=

검증 가능한 무작위 함수를 사용한 에너지 효율적인 VRF-작업증명 합의 알고리즘

김승민, 최해웅, 이흥노*
광주과학기술원

seungminkim@gm.gist.ac.kr, haeung@gist.ac.kr , *heungno@gist.ac.kr

Energy-Efficient VRF-Proof-of-Work Consensus Algorithm Using Verifiable Random Function

Seungmin Kim, Haeung Choi, Heung-No Lee*
Gwangju Institute of Science and Technology (GIST)

Introduction

PoW-based Bitcoin mining consumes enormous amounts of electricity, enough for a **small country like Denmark**[1].

...

In the literature, **more energy-efficient alternative mechanisms** [2], [3], [4] can be used in PoW, either by limiting the economic power of miners or by recycling the energy wasted on solving puzzles to perform other useful tasks [5].

...

However, this works still cannot meet the same level of security as the original PoW, which means it introduces new vulnerabilities compared to the original Nakamoto's consensus.

=> **Save energy while maintaining the same level of security.**

[1] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, Tech. rep., 2008.
[2] S. Deetman, Bitcoin could consume as much electricity as Denmark by 2020. 2016, 2017, URL https://Motherboard.vice.com/en_us/article/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. Retrieved March 18.
[3] C. Mora, R.L. Rollins, K. Taladay, M.B. Kantar, M.K. Chock, M. Shimada, E.C. Franklin, Bitcoin emissions alone could push global warming above 2 C, Nature Clim. Change 8 (11) (2018) 931–933.
[4] I.M. Ali, M. Caprolu, R. Di Pietro, Foundations, properties, and security applications of puzzles: A survey, ACM Comput. Surv. (ja) http://dx.doi.org/10.1145/ 3396374.
[5] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. 107 (2020) 841–853.

Preliminaries

Proof of work

When the **mining race** begins, **miners start competing** to **form a valid block**.

the **first miner** that finds the nonce is considered as the **leader** of the current round for creating the new block.

Such a miner **announces the block** to the rest of the network to get the reward.

Every other miner that receives the new block immediately **desists mining** the current block and **start mining the next one**

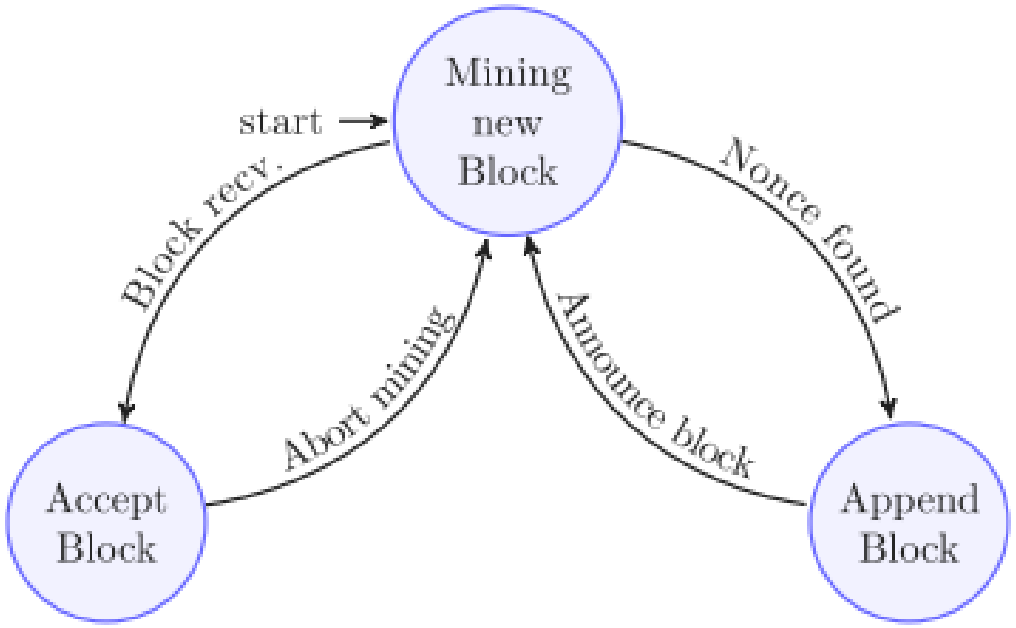


Fig. 1. The state diagram of a miner in the original PoW.

Preliminaries

Mining difficulty

A measure of how difficult it is to find a Nonce of a valid block.

The **difficulty will increase** when the **average block time is less than expected**, as it indicates that the **network's computational power** has **increased** and miners have become capable of generating new blocks in less than 10 min.

the relation between the **previous average block time** and the **difficulty** level:

$$F = \frac{T_E}{T_{Avg}}$$

$$D_{(i+1)} = D_{(i)} \times F$$

Related work

Survey studies made so far in order to mitigate the energy inefficiency of the PoW algorithm. There are **two main categories of solutions**.

1. Either recycling the power spent during the mining process in serving **other useful real problems** or **modifying the consensus protocol** flow while maintaining the cryptographic puzzle.

2. **Completely different and consensus algorithms** such as Proof of Stake (PoS), Proof of Elapsed Time (PoET), and Proof of Retrievability (PoR). While this class of solutions can achieve considerable energy saving, yet it cannot reach the same security level as the well tested PoW.

The **green-PoW** consensus mechanism can be classified in the first category

⇒**Therefore, the focus on the first category**

[6] C. Badertscher, P. Gaži, A. Kiayias, A. Russell, V. Zikas, Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability, in: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 913–930.
[7] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, Consensus in the age of blockchains, 2017, arXiv preprint arXiv: 1711.03936.
[8] A. Miller, A. Juels, E. Shi, B. Parno, J. Katz, Permacoin: Repurposing bitcoin work for data preservation, in: 2014 IEEE Symposium on Security and Privacy, IEEE, 2014, pp. 475–490.

Related work

the surveyed studies fall short in effectively addressing the power consumption of PoW.

Existing approaches either replace the crypto-puzzle with different types of useful work which adds complexity to the consensus process or alter the ledger's structure and consensus flow drastically, which degrades the network's security.

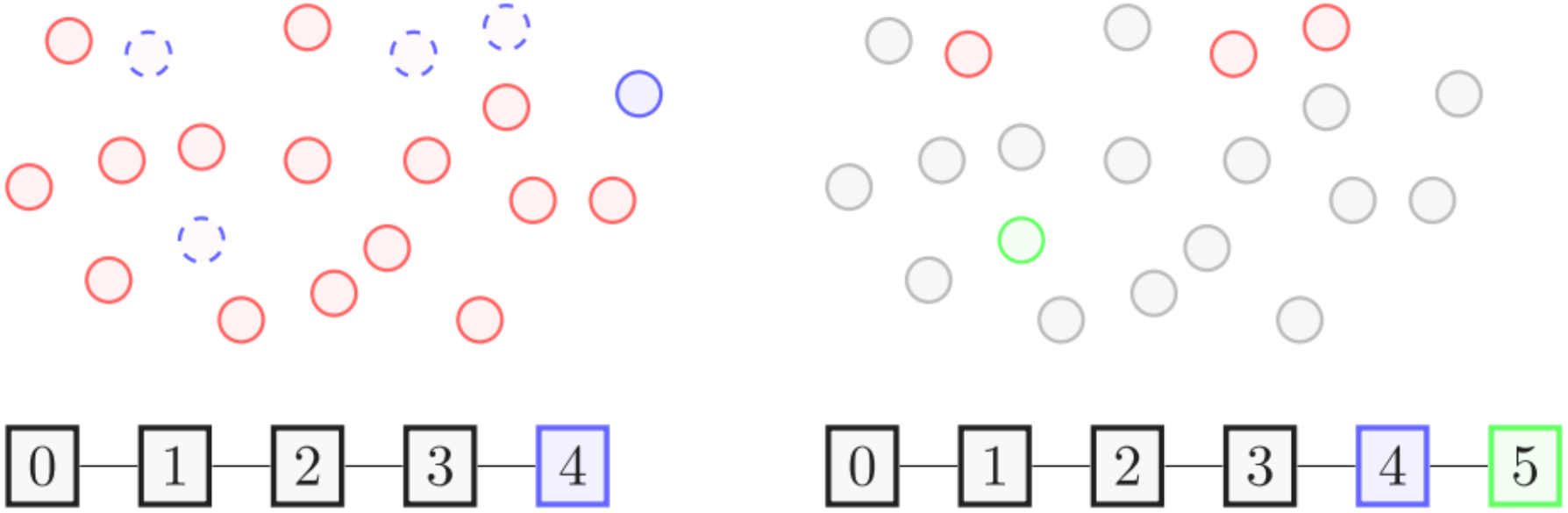
Table 1
Related work summary.

Solution	Energy consumption	Security Level
REM [9]	**[Moderate]** The consumed energy is equivalent to the energy required to execute the useful workload.	**[Moderate]** Rely on a central trusted execution environment. Yet REM claims that their statistics-based security framework eliminates this concern.
Proof of useful work [15–17]	**[High]** The required work to be done by the miners is computationally heavy (time consuming).	**[High]** The security level of this category is similar to the original Nakamoto's consensus.
Proof of learning [18,19]	**[Moderate]** The consumed energy is equivalent to that required to train and test a machine learning model.	**[Moderate]** The security of the protocol relies on the set of validators which are randomly chosen to evaluate the accuracy of the trained models.
Bitcoin-NG [21]	**[Moderate]** The consumed energy is reduced compared to the original Bitcoin since not all the created blocks require PoW.	**[Low]** The protocol is vulnerable to double-spending attacks.
PoS [6]	**[Low]** The protocol relies on the staked cryptocurrencies to prevent Sybil attack without incurring any extra work.	[Moderate] Vulnerable to the Nothing-at-Stake attack.
PoET [7]	**[Low]** Energy waste-free decentralized consensus.	**[Low]** Rely on a central trusted execution environment (SGX).
PoR [8]	**[Moderate]** The protocol consumes energy equivalent to that required for manufacturing and operating the storage units.	**[Moderate]** Rely on the security of the retrievable file storage and on the security of the miner's private keys storage.

Energy-efficient consensus algorithm

Green-PoW is an **energy-efficient consensus algorithm** that reduces the computation load to nearly 50% compared to the original Bitcoin's PoW algorithm, without affecting the other properties of the system.

The algorithm divides **time into epochs**, where each epoch consists of **two consecutive mining rounds**.



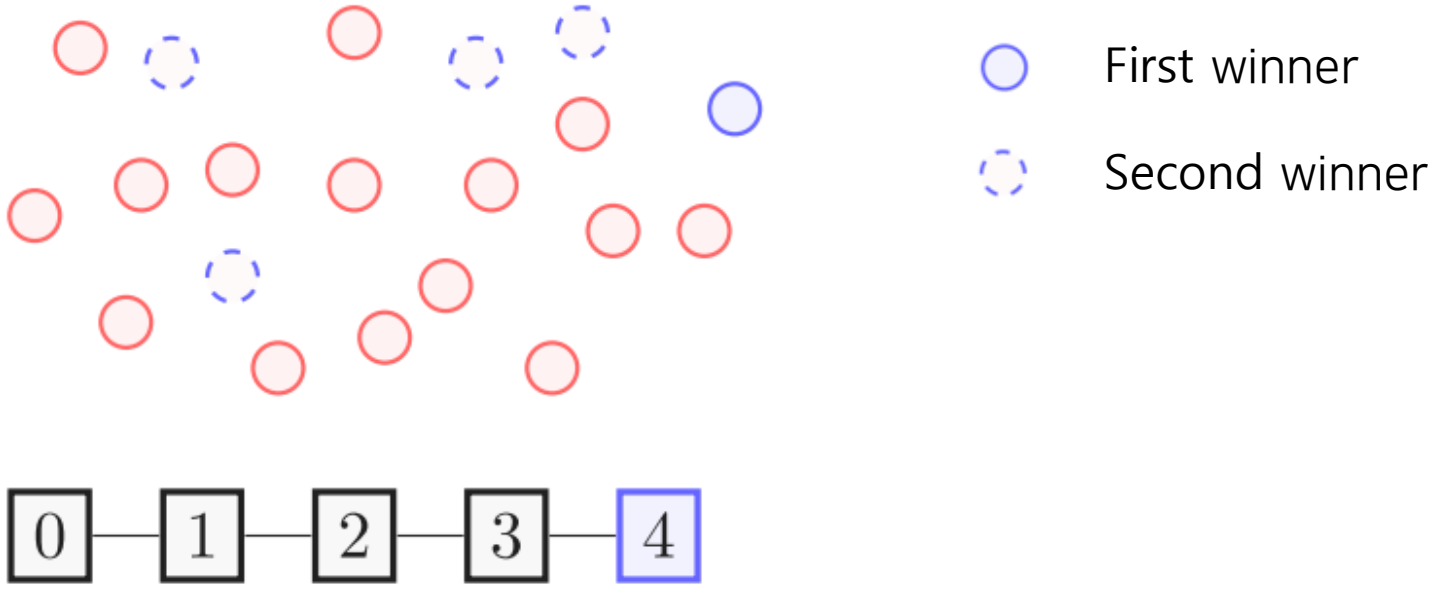
(a) First mining round ρ_2^1.

(b) Second mining round ρ_2^2.

Energy-efficient consensus algorithm

In the **original PoW**, when a puzzle-related block is solved by some miner, all the other network nodes desist the mining of that block and immediately start mining the next block.

In **Green-PoW**, if a valid block is found and the **first place winner is elected**, the race will continue between miners to also determine the **runner-up**, i.e., the node that has the **second place in the same block race**.



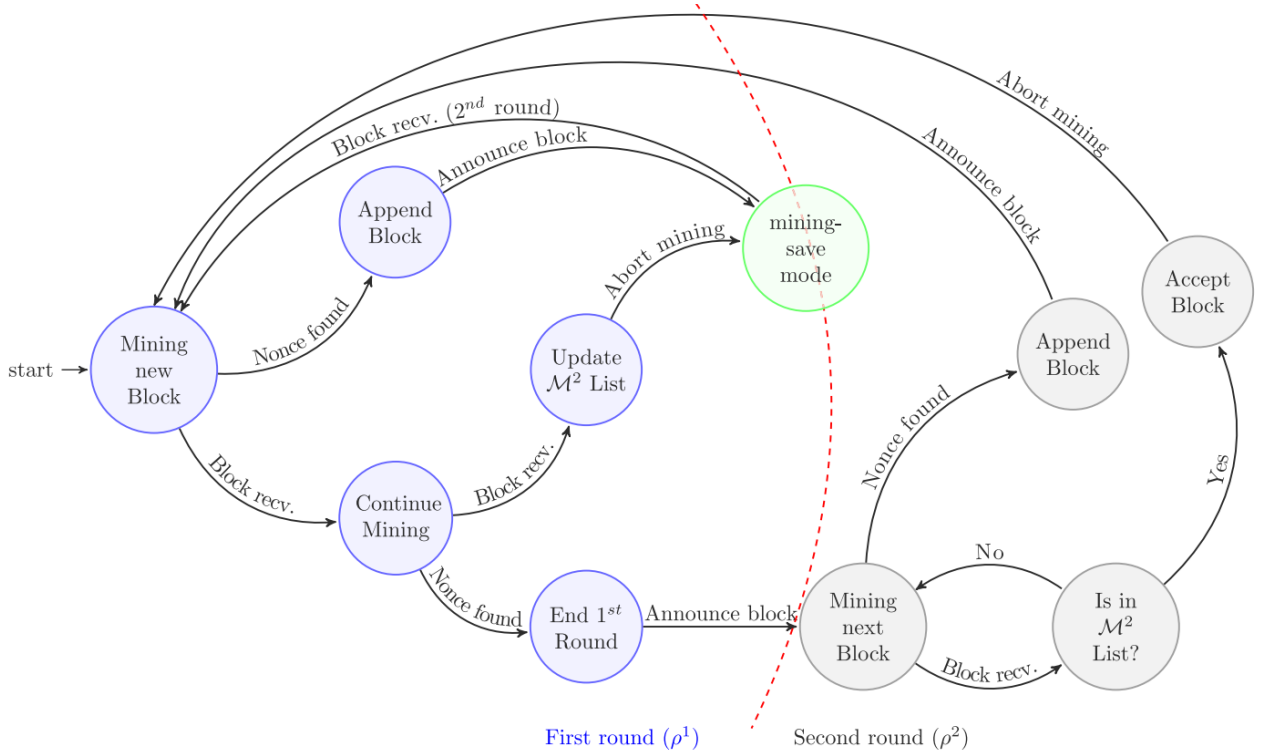
(a) First mining round ρ_2^1.

Energy-efficient consensus algorithm

In the **first round(ρ = 1)**, the miner starts searching for a valid nonce for the **next block b**.

If a nonce is found before a **valid block** is received from another node, the new block is added to the chain and announced to other nodes in the network.

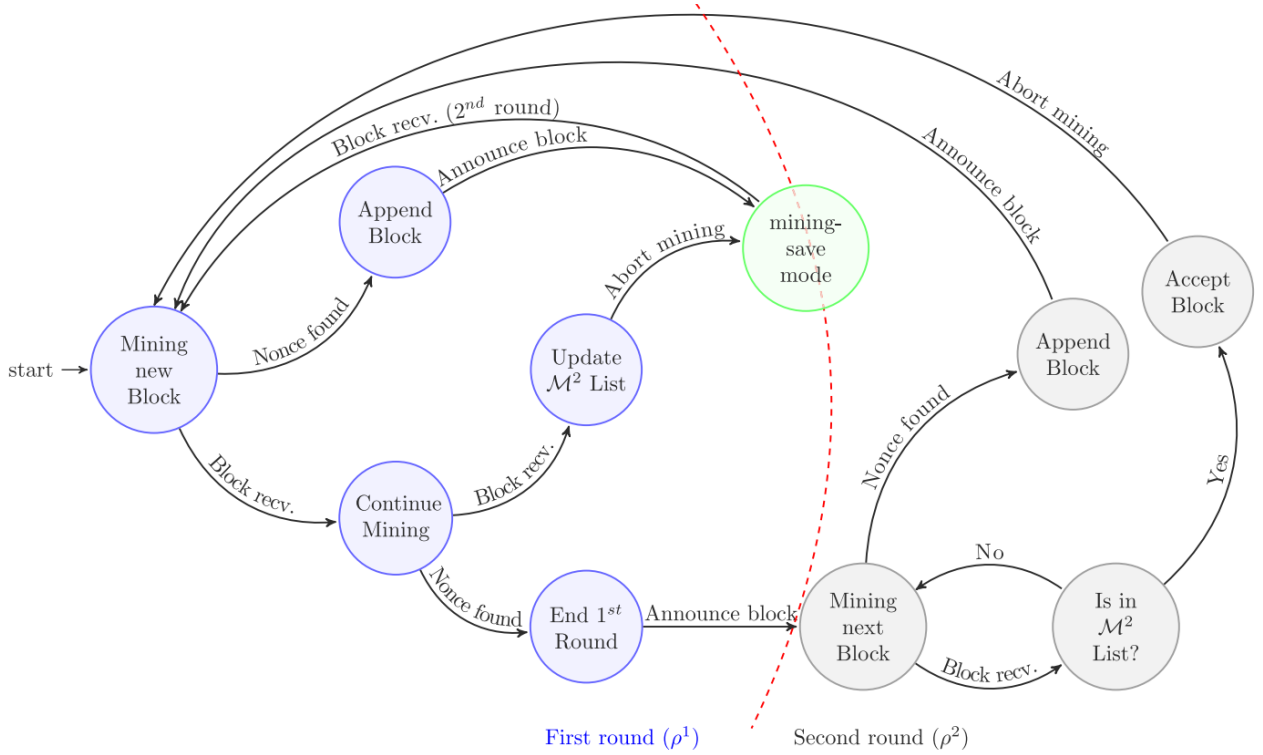
These winning miners go into **sleep mode** for the **second round(for ρ = 2)**.



Energy-efficient consensus algorithm

Once miners receive a block from the winner, **they continue mining the same block** from another miner claiming **runner-up**.

After receiving blocks from **other runner-up nodes**, it enters mining storage mode for the next round. Alternatively, instead of switching directly to **mine-save mode**, **miners can continue mining** with the goal of **joining the runner-up list.**



Energy-efficient consensus algorithm

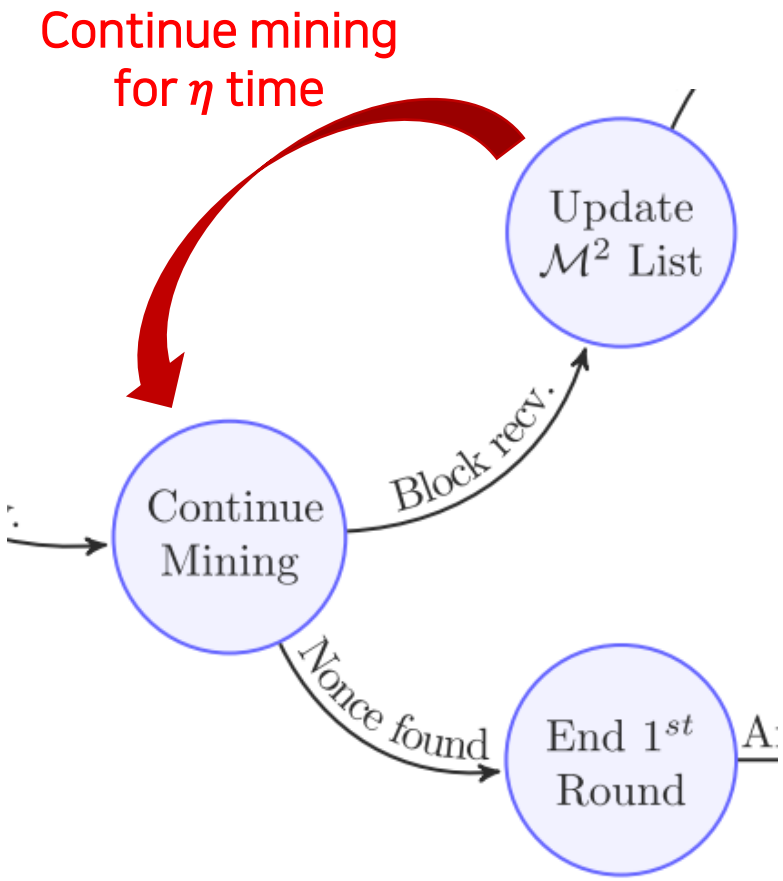
Liveness

In order to engage a sufficient number of participants in **round 2** even if one node has already claimed to be a **runner-up**, the other nodes can **still continue mining**.

A miner that solves the **first round's block very late**, will have a **very small chance** to win as the others have started the mining earlier.

Once a node receives the first announcement of a **runner-up**, it continues mining only for a short period of time η.

η is subject to liveness and energy **trade-off** and is **expected** to be determined based on the rate of block generation in the network.



Energy-efficient consensus algorithm

Second round

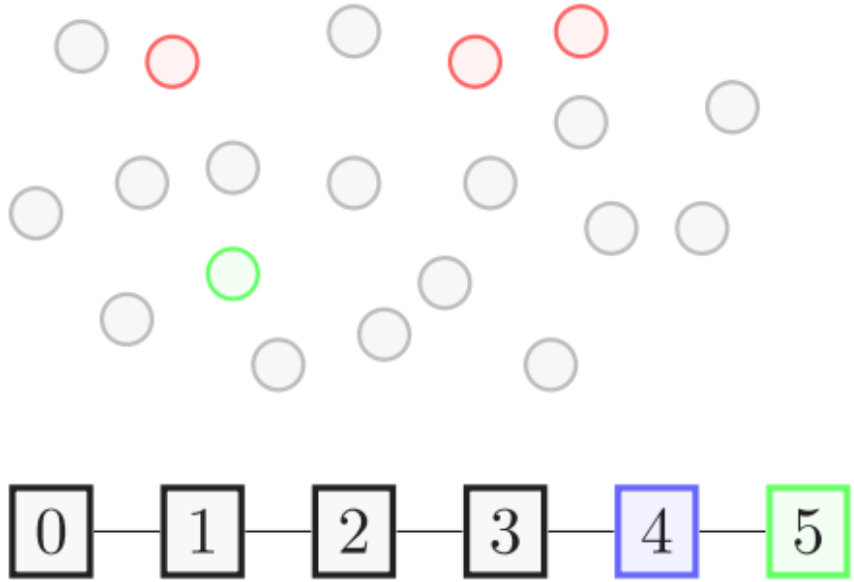
Since only some nodes may be included in the second round, the system may **deadlock** and the next block may not be produced.(no one Round 2 miner)

To mitigate this issue and ensure system liveliness, Green-PoW uses a timeout at the beginning of each **round 2**.

Since the **total hash power** decreases sharply with every second round of mining compared to the first round, **each difficulty** is determined independently by the block generation time of **Round 1** and the block generation time of **Round 2**.

$$D_j^1 = D_{j-1}^1 \left(\frac{T_E}{T_{Avg^1}} \right)$$

$$D_j^2 = D_{j-1}^2 \left(\frac{T_E}{T_{Avg^2}} \right)$$



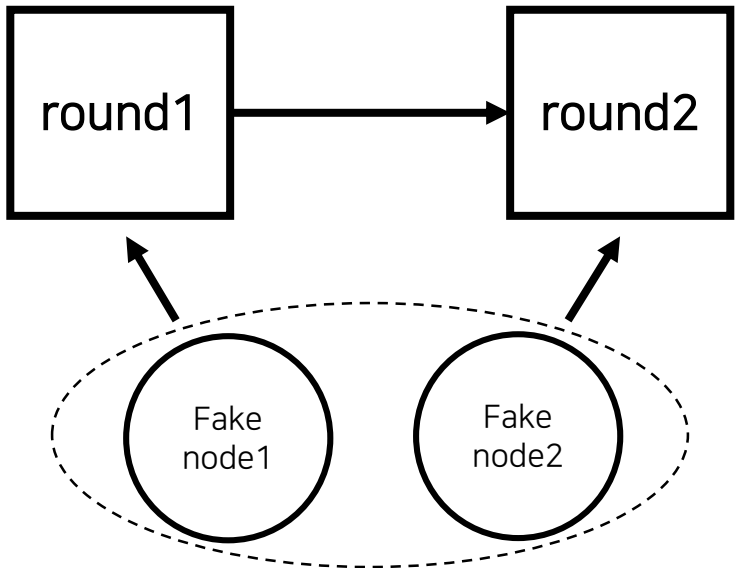
(b) Second mining round ρ_2^2.

Security analysis

Sybil attack resistance

In **Green-PoW**, a malicious miner may try to perform a **Sybil attack** in order to violate the established Green-PoW rule that prohibits a **first-round winner** from participating in the **second mining round**.

However, such an attack cannot succeed as the malicious node in this case needs to split the mining power between the two identities which significantly diminishes the probability of winning both the first-round block and runner-up membership.



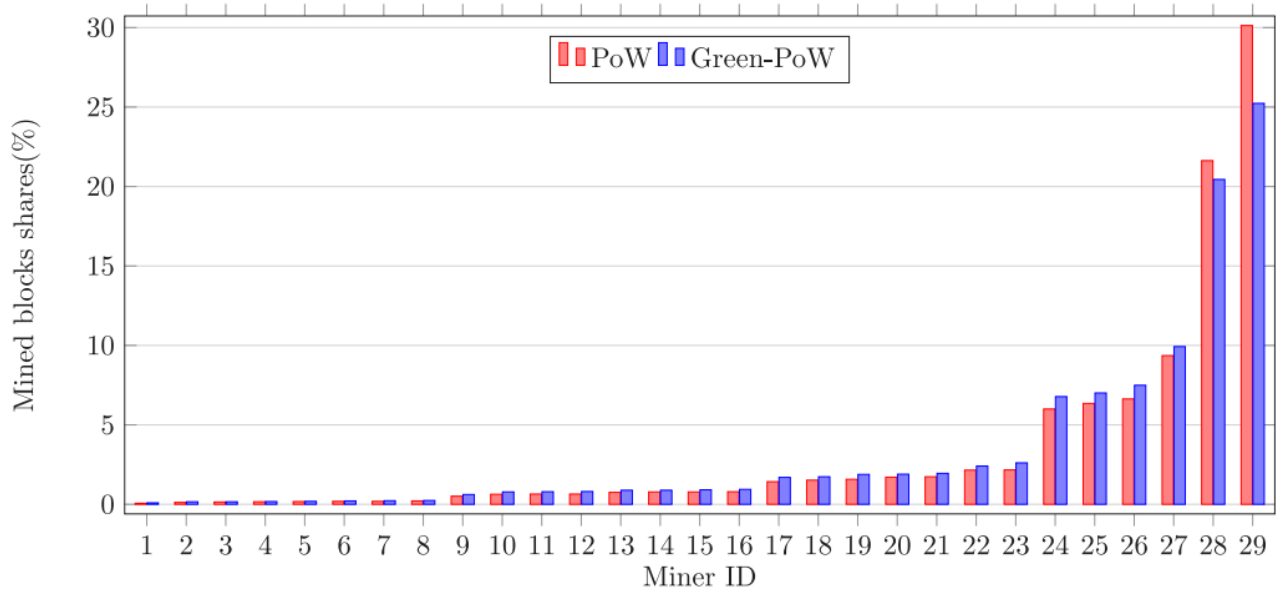
Security analysis

Mining centralization

Green-PoW can reduce the **monopoly of powerful miners**, since generating consecutive blocks by the same miner is likely not possible.

A miner that wins the mining race in round 1 is not allowed to participate in round 2 , and consequently gives the **other nodes the chance to win with less competition**.

the corresponding **shares of the most powerful miners**, in Green-PoW are reduced, compared to the case of the original PoW.



Performance evaluation

Fig. 5 : the ratio of power saving

When only one node mines the block in the second round, the saving power is nearly 50% regardless of the size of the network.

Fig. 6 : the total energy consumption

Green-PoW consumes more energy than PoW in the first round. Nonetheless, the average of the first and second rounds is about 30–50% less than PoW.

Fig. 7 : the impact of distribution of the hashing power on the energy-saving.

When the power is equally distributed among miners, Green-PoW achieves its maximal saving.

Fig. 8: the time needed in order to have a specific size of round 2

If the distribution is not uniform, η increases significantly because less powerful nodes need more time to mine blocks and wait for other miners to be able to join.

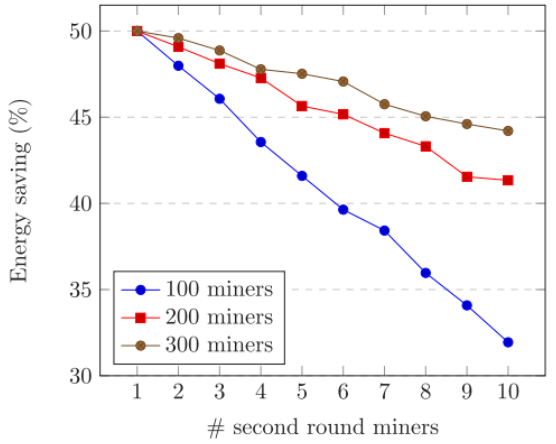


Fig. 5. Energy saving ratio Vs. number of second round miners.

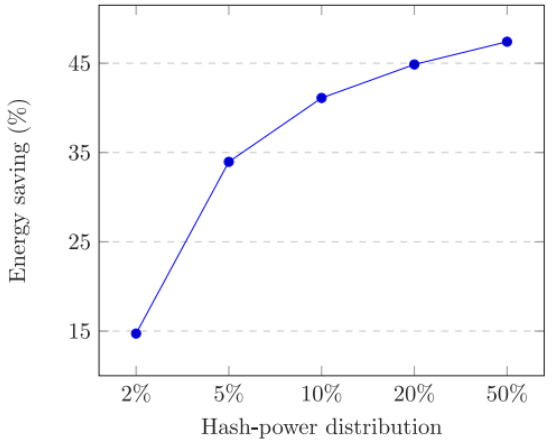


Fig. 7. Energy saving ratio Vs. hash-power distribution.

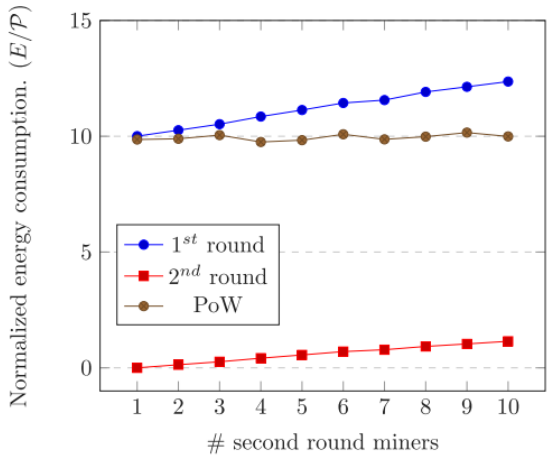


Fig. 6. Normalized energy consumption Vs. number of second round miners.

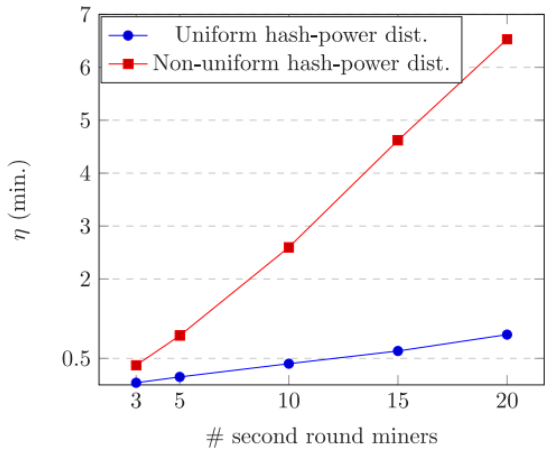


Fig. 8. Average time (η) between the first and last considered runner-up to be include in M_i^2.

Performance evaluation

Fig. 9 : the required time for a block to be mined in the second round.

For example, to mine a block with probability between [0.7, 0.9], a network with $\lambda = 1/10$ would have to wait between [12, 23] minutes. On the other hand, a network with $\lambda = 1/5$ must wait between [6, 12] minutes.

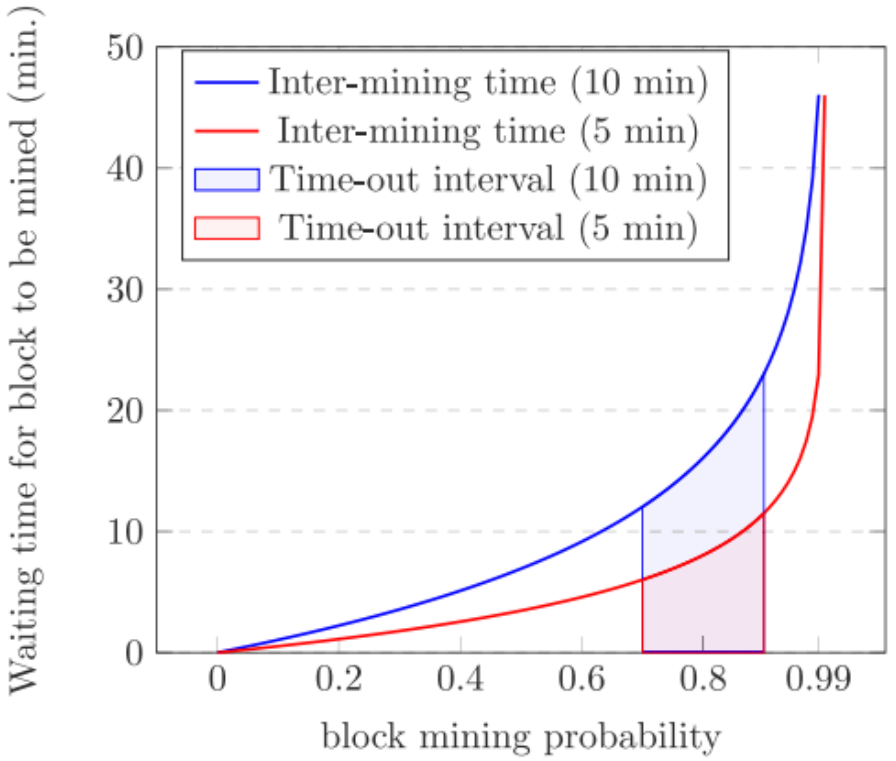


Fig. 9. Time to wait for a block to be mined in the second round Vs. the corresponding probability.

Conclusion

In this paper, we propose a new consensus algorithm called Green-PoW for public blockchain.

In Green-PoW, time is divided into epochs consisting of two mining rounds.

The first round is similar to mining in original PoW.

In the second round, only miners elected in the previous round have the right to participate and compete to form new blocks.

Results demonstrate the effectiveness of the solution, which can save up to 50% of mining energy in large networks with evenly distributed hashing power