I. J. Computer Network and Information Security, **2024, 6, 32-44**
Published Online on December 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.06.03

Proof of Notoriety: A Promised Consensus Mechanism for the Blockchain-based Copyright System

Ahmed Mounsif Kebir
University of Science and Technology of Oran-Mohamed Boudiaf /Computer Science, Oran, Algeria
E-mail: kebir.moncef2000@gmail.com
ORCID iD: https://orcid.org/0009-0007-6025-6541

Asmaa Boughrara*
University of Science and Technology of Oran-Mohamed Boudiaf /Computer Science, LSSD Laboratory, Oran, Algeria
E-mail: asmaa.boughrara@univ-usto.dz
ORCID iD: https://orcid.org/0009-0000-4076-9250
*Corresponding author

Received: 06 July 2023; Revised: 11 October 2023; Accepted: 29 December 2023; Published: 08 December 2024

Abstract: In blockchain technology, copyright protection can be achieved through the use of smart contracts and decentralized platforms. These platforms can create a tamper-proof, timestamped record of the creation and ownership of a work, as well as any subsequent transactions involving that work. The choice of platform or type of blockchain is mainly dependent upon the type of consensus algorithm. This article presents a novel approach to copyright protection using blockchain technology. The proposed approach introduces a new consensus mechanism called Proof of Notoriety (PoN) to enhance the security and efficiency of copyright registration and verification processes.
The Proof of Notoriety consensus mechanism leverages notoriety scores to determine the validity and credibility of the participants in the copyright registration process. Participants with higher notoriety scores are given more weightage in reaching a consensus on the validity of copyright claims. This ensures that only reputable entities are responsible for registering and verifying copyright, thereby reducing the risk of fraudulent claims and unauthorized use.

Index Terms: Consensus Mechanism, Copyright Protection, Blockchain, Proof of Notoriety, Reputation Score, Authority, Nodes.

1. Introduction

In recent years, the increasing digitization of creative works and the ease with which they can be reproduced and distributed have led to significant challenges in protecting the rights of creators. Traditional approaches to copyright protection, such as registration with centralized authorities, have proven to be insufficient in the digital age. Compared with physical works, digital works can be copied, modified, and distributed on a large scale with just a few clicks, facilitating unauthorized sharing and copyright infringement. Moreover, the emergence of the Internet has created additional challenges in terms of jurisdiction and geographical reach. In response, blockchain technology has emerged as a promising solution, offering secure, decentralized, and transparent record-keeping that could help to ensure that creators receive fair compensation for their work.

This article is organized into five main sections. The second section provides a comprehensive overview of blockchain technology, the concept of consensus, an overview of the current state of copyright protection, and the existing research and approaches related to consensus blockchain-based copyright protection. Section 3 describes in detail the proposed approach, which involves the consensus proposed approach. Section 4 contains the implementation step of the proposed approach, including tests and evaluations. Finally, section 5 discusses the limitations and challenges of the approach and provides suggestions for future research.

2. Background

2.1. Blockchain Technology

Blockchain technology is a decentralized and distributed digital ledger technology that enables secure, transparent, and tamper-proof storage and transfer of data and digital assets without the need for a trusted intermediary or central authority. Blockchain technology is an advanced database mechanism. The data are stored in blocks that are linked together in a chain. In contrast to centralized systems, where transactions are validated by a single organization, in a blockchain, multiple entities participate in validating transactions. The operations are only recorded in the blocks when there is a consensus among the blockchain community [1].

In the context of blockchain:

- Nodes : a node is a computer or device that is connected to a blockchain network. Each node maintains a copy of the blockchain ledger and participates in the validation and verification of transactions on the network. Nodes can be categorized as full nodes, which maintain a complete copy of the blockchain, or light nodes, which maintain only a partial copy of the blockchain [2,3]
- Cryptography : there are several types of cryptography used in blockchain technology, including Symmetric Key Cryptography, Asymmetric Key Cryptography, and Hash Functions. Public and private keys are a critical part of asymmetric key cryptography. In the context of blockchain, users have a public key and a private key associated with their account. Transactions are signed using the private key, which ensures that only the account holder can authorize the transaction. The public key is used to verify the signature and ensure that the transaction is valid [4,5].
- Main categories of blockchain : blockchain can be categorized into several types, including: Public: transactions are made obvious to all users. Users can approve on the consensus approval process. Private: authorized nodes only from a third party are allowed to participate in the consensus process. Hybrid: a combination of the characteristics of public and private blockchains. Part of the blockchain's data or records is public, while the rest remains secret and confidential. Consortium: selected nodes can contribute to the consensus process. Unlike a hybrid, this blockchain is decentralized, as it is managed by several organizations [6,7].

2.2. Consensus

Consensus in the blockchain is an algorithm used to ensure that all nodes agree on a common state shared across the entire network of the distributed ledger and that new transactions are recorded consistently across all copies of the ledger. It determines performance and security and it’s based on three key properties: safety, liveliness, and fault tolerance [8].

There are more than 84 Blockchain Consensus in the existing literature [9]. Some consensus algorithms are more widely used and known, while others are more experimental or specific to certain blockchains or projects. Each algorithm has its own specific advantages, disadvantages, and use cases. The choice of consensus will depend on the needs and objectives of the blockchain in question.

The most widely known consensus methods for blockchain networks are Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). Yet PoW is energy-intensive i.e. uses very high resources. In PoS, the richest is the solo consensus controller. With DPoS, only delegated have the power and control of all tokens.

Our initial idea is to work with a blockchain system whose consensus obeys two criteria:

- It requires the lowest possible amount of energy;
- The selection of the consensus group and the leader are based on the behavior of each node. Being part of the consensus group or a leader is by merit.
- Based on these two criteria, we seek further consensus that will be discussed in sub-section 2.4.

2.3. Copyright

Copyright is an intellectual property that protects its owner’s original work of authorship as soon as the work is fixed in a tangible medium of expression, the work can be any type of digital content, including articles, books, images, poems, videos, software, and computer programs. Copyright does not protect the concept, idea, principle, and method of content creation, rather, it protects how these things are expressed [10,11].

The protection applies from the moment of putting an original work of authorship in a tangible form under a sufficiently permanent or stable organization such that the work can be reproduced, perceived, and publicly accessed for more than a transitory period of time [12].

Blockchain technology can help protect copyright in the digital age by providing secure and transparent registration and ownership. There is a potential relationship of blockchain with copyright, including:

A. Copyright Register on the Blockchain

- The registration process involves bundling ownership information into blocks that are time-stamped and linked to the prior block with a hash value [13,14];
- Data on the blockchain are stored chronologically and are visible to all participants, creating a high level of transparency. By using digital signatures and private-public key cryptography, users do not have to reveal their true identities when they store information on the blockchain or are involved in transactions [13];
- A blockchain copyright register can provide full and reliable ownership information to rights holders and users. The registration process can be completed within seconds or minutes, and subsequent transfers of rights can also be saved on the blockchain register [15].

B. Transfer of Rights Through Smart Contracts

- Smart contracts are digital contracts that automatically execute the agreement terms written in code lines. These contracts are stored on a blockchain network [14];
- To transfer rights through smart contracts, the parties involved would need to define the terms of the transfer in the code of the contract, such as the specific work being transferred, the duration of the transfer, and the compensation involved [14].

According to a study by the World Intellectual Property Organization (WIPO), blockchain technology has the potential to transform the way that copyright works are created, distributed, and monetized. The study notes that blockchain-based copyright systems can provide greater transparency and efficiency, reduce transaction costs, and facilitate the licensing and enforcement of copyright [16].

2.4. Related Work

A. Overview

In [17] Song et al. have proposed a new blockchain consensus mechanism that is based on the contributions of its participants. This proposed mechanism, known as Proof of Contribution (PoC), evaluates the actions and behaviors of users in a blockchain-based system and quantifies them as contribution values using a specific algorithm. In their contribution algorithm, user contribution includes 3 aspects: IP right registration, IP right transaction, and Online time. The main idea behind PoC is that the more a user contributes to the network, the more likely they are to be selected as the next block creator.

In their article [18] Aluko and Kolonin propose a reputation-based consensus mechanism for blockchain-based systems. Proof of Reputation (PoR) is a consensus mechanism that evaluates the behavior of nodes based on their reputation scores to determine their influence on the network. It is a reputation-based system that rewards participants based on their positive contributions and punishes them for negative behaviors. In this way, nodes with higher reputation score weight in the decision-making process, creating a more trustworthy and efficient blockchain network. The consensus group consists of selected members from the network nodes based on their reputation values. The leader is selected from the consensus group in each round using a random function.

In [19] the authors propose a decentralized copyright system to ensure cross-border protection of digital content and address challenges in international copyright management. The approach uses the Proof of Authority (PoA) consensus algorithm for block creation. The system design of this approach consists of a copyright federation, member countries (referred to as authorities), and users who receive tokens. The authorities maintain a consortium blockchain using the PoA consensus mechanism.

B. Consensus Mechanisms Discussion

Proof of reputation, proof of contribution, and proof of authority are suitable for blockchain-based copyright systems because they consume less energy compared to proof of work and are more effective in terms of initial fairness compared to proof of stake. Also, they are not only cryptocurrency-oriented like other consensus mechanisms. Still, they present some drawbacks:

- In proof of contribution [17], a node can contribute significantly, but its intention may be malicious, so it can never be sanctioned. Also, it can lead to centralization if rewards favor a particular group and discourage participation from individuals or entities with limited resources;
- In the proof of reputation-related work [18], one critique is that relying solely on reputation values for selecting the consensus group may not provide sufficient security. This consensus is Susceptible to Sybil attacks. It could be beneficial to include official entities or additional mechanisms to enhance security measures within the system;
- In proof of authority [19], entities have been identified statically. On one hand, it is beneficial, because it prevents Sybil attacks. But on the other hand, PoA is used in private or consortium blockchains where the network participants are known and trusted.

We consider that the most suitable consensus mechanism for a blockchain-based copyright system should fulfill the following criteria:

- Suitable for public blockchain: The consensus mechanism should apply to a public blockchain, which is accessible to a wide range of participants (nodes);
- Does not require expensive hardware: It should not rely on costly hardware requirements, ensuring accessibility and inclusivity. Since it's difficult for a lambda person to invest in equipment;
- Considers both stake and activity on the network: The consensus mechanism should take into account both the stake (credibility that a participant holds in the network) and activity (participation) of nodes on the network;
- Fast transaction times and low energy consumption: Transaction times should be fast, and the energy consumption should be low, promoting efficiency;
- Can prevent 51% attacks: Where a single entity or group gains majority control over the network.
- Can prevent Sybil attacks: Where a malicious entity creates multiple fake identities to gain control or manipulate the system.

After evaluating all the consensus mechanisms mentioned above and others not yet used for copyright protection, we decided to propose a new consensus mechanism called «**Proof of Notoriety».** Which combines the advantages of two consensus mechanisms: Proof of Reputation and Proof of Authority.

3. Proposed Approach

In this section, we present our proposed approach for protecting copyright on the blockchain. We discuss the design of our system, which utilizes our consensus mechanism the Proof of Notoriety for ensuring secure and decentralized transactions.

3.1. Consensus Proposed Approach

Proof of Notoriety is a consensus mechanism, which combines the advantages of both Proof of Reputation and Proof of Authority consensus mechanisms.

We chose to incorporate Proof of Reputation because it rewards participants with a good reputation who have demonstrated hard work on the blockchain network, making them deserving of their place in the consensus without requiring a large number of high resources. In our approach, we propose a new method to calculate the reputation value of each node.

In addition, we propose the use of the authority principle as a security measure. The involvement of official entities or organizations significantly enhances the level of security within the consensus mechanism.

A. Notoriety System Design

In our proposed system, the notoriety of a node will be based 90% on the reputation score and 10% on its status as an official authority. The calculation of a node's notoriety can be represented by the following equation:

$$notoriety(i) = (0.9 * rep(i)) + (0.1 * authority(i)) \quad (1)$$

notoriety(i) is the notoriety value of node *i*.
rep(i) is the reputation score of node *i*.
authority(i) is a value indicating whether node *i* is an authority or not.

Each node within the network has a weight value that reflects a greater influence on the consensus process. For example, in a consensus voting process, a node with a higher weight has a greater impact than a node with a low weight value. Weight value *w* is calculated as follows:

$$w(i) = \frac{notoriety(i)}{\sum_{j=0}^{N} notoriety(j)} \qquad i, j \in S \quad (2)$$

w(i): weight value of node *i*.
notoriety(j): notoriety value of node *j*.
S: network.
N: total number of network nodes.

It is important to note that the choice of utilizing 90% and 10% as parameters is a subjective decision and does not adhere to any specific mathematical formula.

The reputation score and authority status of a node are defined in the following sub-sections.

B. Reputation Score

The reputation score will be based on the participant's track record, which includes the following factors:

- First: The number of blocks a node has successfully validated;
- Second: The number of copyright data created and registered;
- Third: The number of times it has participated in consensus.

The reason for choosing these factors are as follows:

- Attracting nodes to validate blocks will lead to the expansion of the blockchain;
- The registration of copyright data is the first step for copyright protection;
- Participating in the consensus is essential to the security of the blockchain.

The reputation score (rep) is an element of the closed interval [0,1], where: $rep \in [0,1]$.

Reputation can be calculated using continuous values. The reputation score is visible to all members of the network, promoting transparency and accountability.

Every new node that joins the blockchain network, starts with an initial reputation score superior to zero rep > 0. We have chosen an initial reputation score to encourage new nodes that join the network. This decision is based on the fact that it is more rational for a node to start with some degree of reputation rather than starting with no reputation at all.

As the node behaves positively on the network, its reputation score will be periodically updated to reflect its improved behavior.

The reputation score is calculated as follows:

- Let the reputation score of node *i* be denoted by *rep(i)*;
- Let $f1$, $f2$ and $f3$ be the factors 1, 2, and 3 respectively, representing the number of blocks created, the number of copyright data registered, and the number of times the node has participated in consensus;
- Let α, β, and γ be the weights assigned to factors 1, 2, and 3 respectively;
- Then, the updated reputation score *rep'* can be calculated as:

$$rep(i)' = \frac{rep(i) + (\alpha * f1 + \beta * f2 + \gamma * f3)}{\sum_{j=0}^{N} rep(j)} \qquad i, j \in S \tag{3}$$

rep(j) is the reputation score of node *j*.

S: network.

This approach allows us to assign different weights to each factor and adjust them based on their relative importance in the reputation calculation. The result is a reputation score that takes into account multiple factors and is normalized by the total network reputation.

C. Authority

Authority is represented by a binary value that distinguishes between the official and the unofficial, where:

$$authority(i) = \begin{cases} 1 \\ 0 \end{cases} \tag{4}$$

The presence of 1 signifies the recognized status of an authoritative entity, while 0 denotes a non-official entity. For example, let's consider the participation of UNESCO in the blockchain network. In this case, UNESCO serves as an official authority, and therefore its authority value is designated as 1. This grants it a 10% increment in notoriety compared to non-official entities, such as regular nodes within the blockchain network.

D. Consensus Group

A consensus group is a members (nodes) that are selected by nodes within the network to perform tasks such as participation in the creation and validation of blocks. In our approach, the consensus group is selected through a voting process. Each node *i* submits a vote for a node *j* within the network to be a part of the consensus group, which is then broadcasted along with their weight *w* to the entire network.

The voting result of a member (node) is calculated as follows:

$$V(j) = \sum_{i \in S} w(i) \tag{5}$$

j: node whose voting result is being calculated.
i: node in the network that has voted for node *j*.
V(j): the voting result of node *j*.
w(i): weight of node *i*.
S: the set of nodes that voted for a particular node *j*.

After, all nodes have submitted their votes:

- We start by sorting the candidate nodes in descending order based on the vote score they have received, from the highest to the lowest;
- Then, we begin by including the candidate nodes in the consensus group, starting with the node that has received the highest score of votes, until the cumulative w of the selected nodes exceeds a predetermined threshold or reaches a desired percentage of the total w in the network;
- The selected consensus group is then broadcasted to the network for all nodes to recognize and follow their decisions.

E. Leader Election

There are many voting techniques. We chose “voting by elimination” (or “voting by rounds” or “Ranked- choice voting”) because it provides a more accurate representation of voter preferences by gradually eliminating less-supported candidates, ensuring increased fairness and legitimacy.

“Fig. 1,” shows the process of leader selection. It starts by counting the votes received by each candidate within the consensus group then it verifies if only one candidate remains with the highest vote count. If so, the leader is found. If not, the candidate with the lowest vote count is eliminated, after that triggering vote redistribution. This process is repeated until the leader is found.

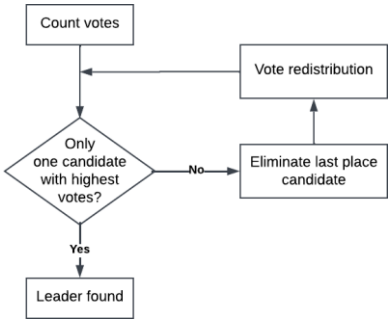

Fig.1. Leader Selection flow-chart

F. Block Publication

Once the consensus group is formed and the leader is selected from the consensus group, and once the leader has successfully created the new block, he broadcast it to the other nodes in the consensus group for validation.

The other nodes in the consensus group will then verify the validity of the new block making sure that the transactions included in it are legitimate and that the block has not been tampered with. If the block is found to be valid, it is added to the blockchain as a permanent part of the ledger.

Additionally, the reputations of the nodes within the network are updated. This is important as it ensures that nodes with good reputations are selected as part of the consensus group in future rounds, thereby maintaining the integrity of the network.

Overall, this process ensures that the blockchain remains secure and trustworthy and that all transactions are recorded in a transparent and immutable way.

G. Incentivizes

Incentivizing participants in the consensus process is an important aspect of maintaining a secure and reliable blockchain network. In our proposed approach, the reward in the form of tokens. Currently, the specific number of tokens awarded to the leader as a reward is yet to be determined. Our focus has been on developing the consensus approach, ensuring the stability and efficiency of the blockchain network.

H. Sanctions

To discourage malicious behavior and ensure the integrity of the blockchain network, a system of sanctions can be implemented to penalize nodes that violate the rules or engage in harmful activities.

There will always be temporary verifications of the copies of the blockchain on each node. If a full node has an invalid blockchain that does not respect the hashing rules or a short blockchain (as determined by comparing it with the longest chain in the network), then the node will receive:

- First Warning: The first time a node misbehaves, it receives a warning from the network. The warning is recorded and kept as part of the node's history. Assuming that the error is due to human error or latency or network problems;
- Second Warning: If a node continues to misbehave after receiving a warning, it will receive a second warning, which will decrement its reputation. And the authority becomes 0 in the case where it is official;
- Third Warning: If it receives a third warning, it will be excluded from the network.

In this work, we used the longest chain rule as an approach to testing the behavior of nodes in the blockchain network. The longest chain rule is a commonly used approach to test node behavior on a blockchain. The longest chain rule states that the valid chain with the most accumulated work (usually measured as the most blocks) is considered the correct chain.

3.2. Blockchain Architecture

The main idea of this work is to propose a new consensus algorithm for blockchain. However, it was difficult, if not impossible, to implement our algorithm on an existing platform. Since platforms impose their own consensus methods. Which is why we deciding to create a blockchain from scratch.

A. Block Structure

Our proposed approach for copyright protection is specifically designed for poem protection, which is one type of creative work that authors may want to protect.

To achieve this, we have designed a block structure that includes important data about each poem, such as the title, author, content, and date. This data is stored in a JSON format and is linked to a unique transaction ID that identifies the addition of the poem to the blockchain.

Transactions in our proposed blockchain architecture are designed to provide validation rewards to the network's validators. Each transaction includes the number of tokens, sender and recipient addresses, and a unique transaction ID.

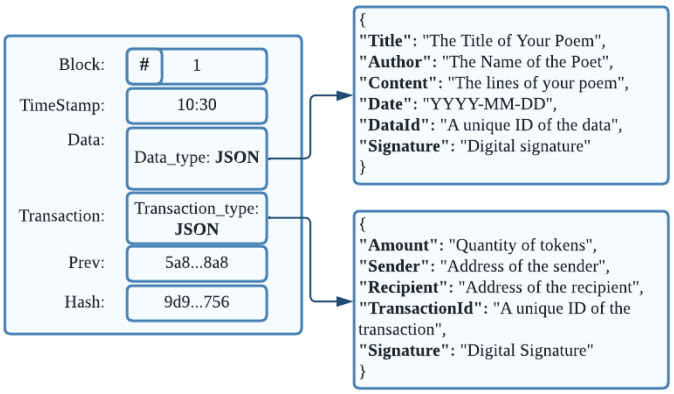

Fig.2. Block structure

B. Network Topology

The network architecture proposed for this blockchain-based copyright protection system includes both:

- Light nodes: participate in the network by verifying the status of the blockchain and maintaining a partial copy of the blockchain.
- Full nodes: maintain a complete copy of the blockchain and participate in the consensus process.

The essential condition is that the nodes participating in the consensus must be full nodes.

The blockchain network is designed as a public network, allowing anyone to participate as a node in the network.

When a new node joins the network, it should have the freedom to choose the type of node it wants to be. In our proposed blockchain network, there are no predefined criteria for joining. The design of our consensus mechanism does not consider specific criteria for new nodes before they join the network. Instead, the evaluation of a new node will occur after it joins the network. The behavior of the new node will be assessed based on our proposed consensus mechanism, which is the Proof of Notoriety.

3.3. System Model

This sub-section is providing a detailed explanation of how our blockchain functions, unveiling its key components and shedding light on its inner workings.

A. Global Blockchain Structure

To illustrate the blockchain conception, a UML class diagram is provided in "Fig. 3,":

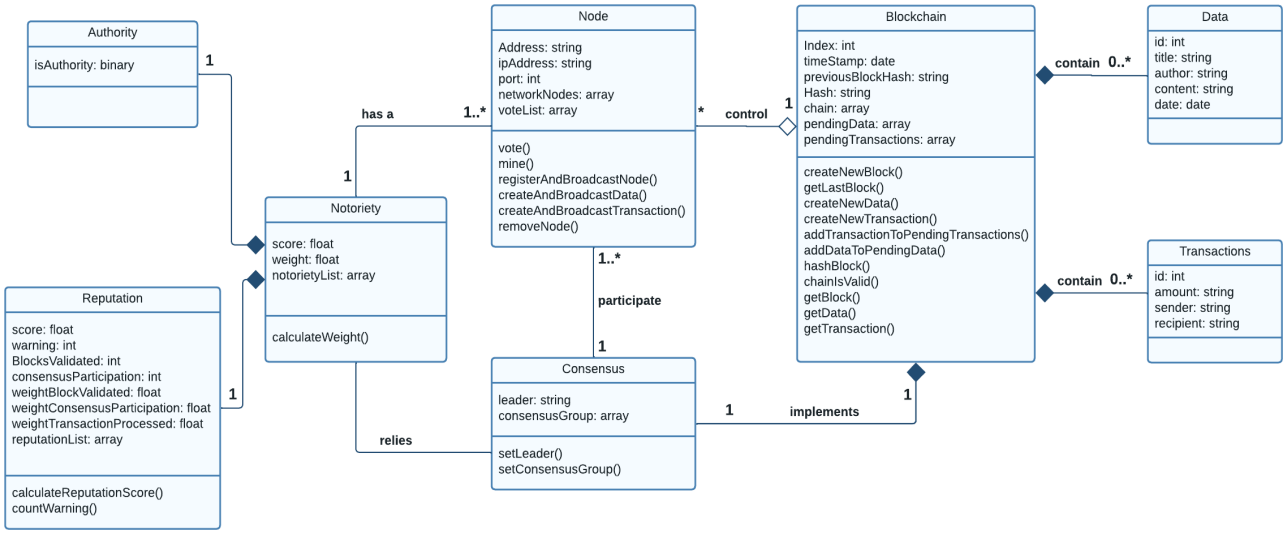

Fig.3. Blockchain class-diagram

B. Notoriety System

The notoriety system is based on 90% of a node's reputation and 10% on whether the node holds official authority status. "Fig. 4," provides an overview of the process of how the reputation score is calculated and how the authority status is determined. By considering the results of both components, we can determine the notoriety score of a network node.

When the leader creates a new block, they broadcast it to the consensus group. The consensus group then verifies the new block's legitimacy, and if it is deemed legitimate, they append it to their local blockchain. After the leader creates the new block and all of this process is done, the consensus session is reset for passing to a future consensus session and the nodes notorieties and reputations are updated.

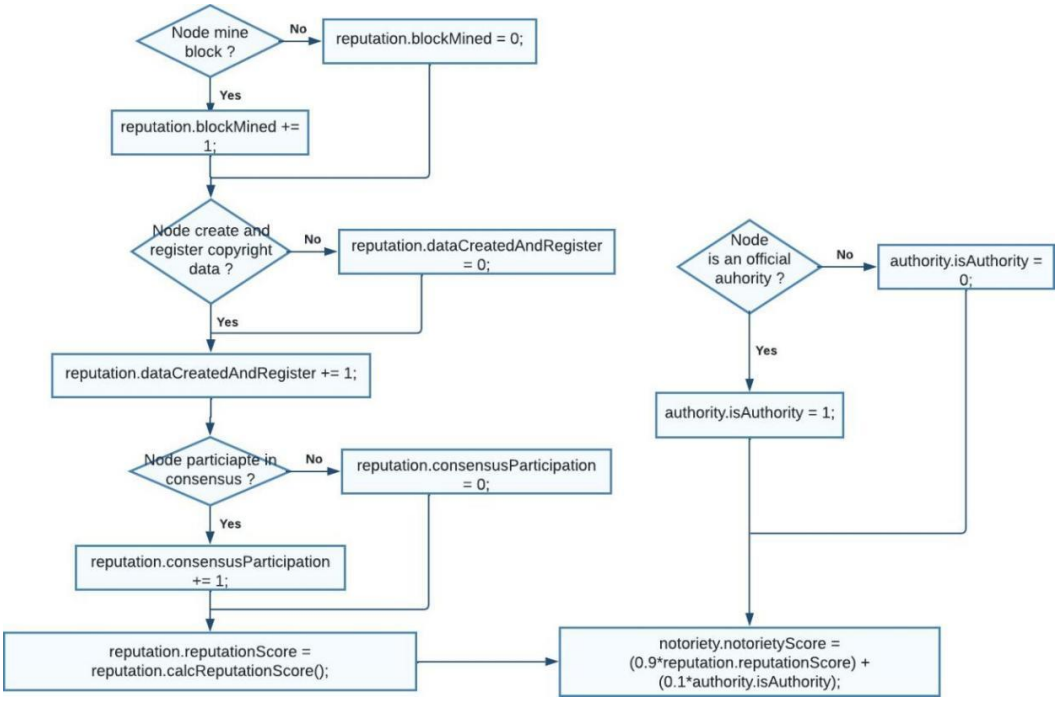

Fig.4. Notoriety flowchart

4. Experiment and Result

All the implementation work was carried out on a single computer an i5 CPU with 8GB RAM.

The programming languages used to write the code are JavaScript for the backend and JSON to transfer data between the network nodes. The technologies that were used in the development of our project: Node.js and Express.js

Before starting the tests, we need to determine the values of the initial parameters: Reputation score and initial reputation value. The initial reputation value is set to 0.2 and number of nodes to 10. The reputation score is based on three factors. Each factor has a weight (α, β, and γ). We consider that f1 should be greater than f3, which is greater than f2 as well. Because f1 is the most important since it enables us to extend the blockchain by adding new blocks. f3 is higher than f2 because participation in the consensus is more important than broadcasting data.

Table 1. Weights of reputation score factors Vs consensus group and leader reputation score

α	β	γ	Consensus Group Reputation Score	Leader Reputation Score
1	1	1	1	1
0.5	0.3	0.4	0.65	1
0.05	0.03	0.04	0.240	0.256
0.005	0.003	0.004	0.204	0.206
0.0005	0.0003	0.0004	0.2003	0.2005

Based on these results, we decided to work with the values: α= 0.05, β= 0.03, and γ= 0.04. These values are chosen to speed up the test results and to notice the difference. It's preferable to use much smaller values, for a long-term blockchain, since the value of the reputation is bounded.

To evaluate the performance of our system, we conducted several tests by varying different parameters:

Firstly, we vary the difficulty which represents the number of leading zeros that must be present in the hash of a block for it to be considered valid, and calculate the block creation time with a maximum block size of 100MB. As shown in "Fig. 5," the block creation time starts increasing by incrementing the difficulty, and beyond 6 as difficulty, the time value becomes important (several hours).

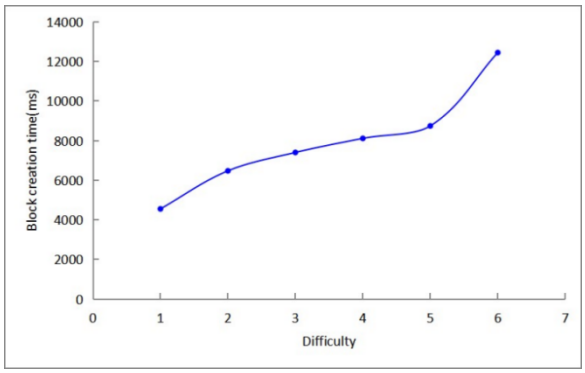

Fig.5. Block creation time as the difficulty is varied

Next, we conducted tests by varying the difficulty value to determine the optimal setting for achieving the best block creation performance. As shown in "Fig. 6," the use of the CPU increase with the increase of the difficulty. In our system we imposed a difficulty level of four zeros from the available range of difficulties (1, 2, 3, 4, 5), the reason behind this choice is:

- The difficulty level of four zeros strikes a balance between ensuring the security of the blockchain and maintaining efficient creation operations.
- Consuming less resource energy (CPU usage).

Furthermore, we varied the size of the copyright data to assess its impact on the block creation time. For the block size, we imposed a maximum size of 100MB, while the maximum size for copyright data is 10MB, the reason for choosing this size is that we are conducting tests on a single computer with 8GB RAM and an i5 CPU. "Fig. 7" show that when the copyright in a block increase, it takes more time for a new block to be produced. This is because there are more copyright data and so it takes more time for those data to be processed. Difficulty also has an impact on block creation times.

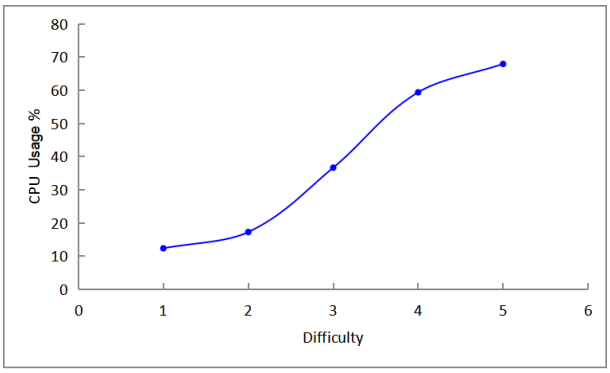

Fig.6. CPU usage as the difficulty is varied

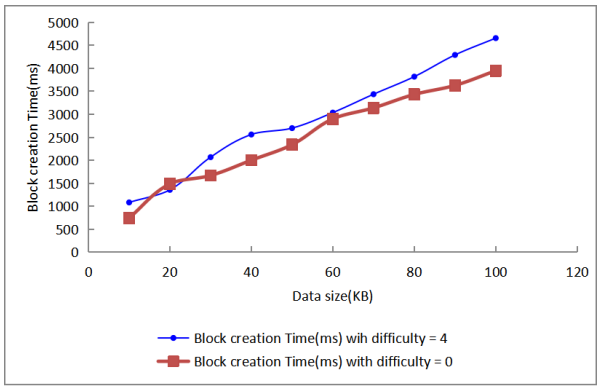

Fig.7. Average block creation time as the number of copyright data in a single block is varied

During the test, we systematically increased the size of the block data and observed the corresponding CPU usage. The results showed a clear correlation, indicating that as the data size increased, the CPU usage also increased. This can be attributed to the fact that larger data requires more computational resources for processing and validation within the blockchain network.

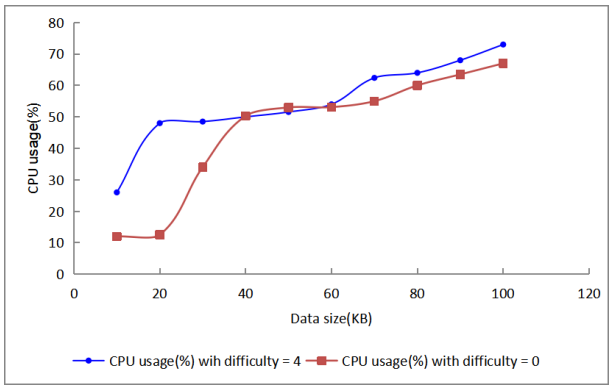

Fig.8. CPU usage as data size is varied

Also, we vary the number of nodes (we vary them between 10 and 50) to measure the time it takes for the selection of a consensus group. “Fig. 9” shows that the consensus group time increases with the increasing number of nodes. This is due to the messages being exchanged synchronously between nodes and the process described before in our approach for selecting the consensus group.

In our final test, we measured the leader selection time against the number of nodes. As shown in “Fig. 10” we observed that when the number of nodes is less than 20 nodes, the leader selection time takes about half a second. However, when the number of nodes is beyond 20, the leader selection time also increases significantly.

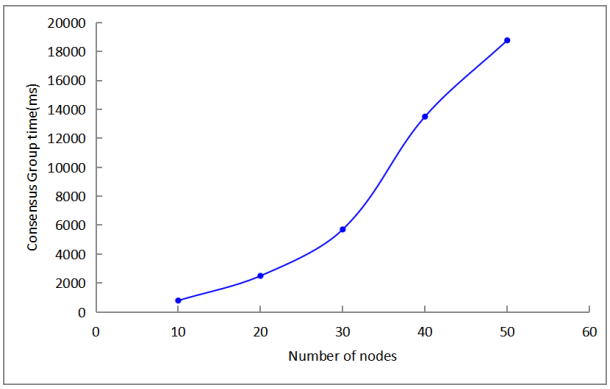

Fig.9. Consensus group time as the number of nodes is varied

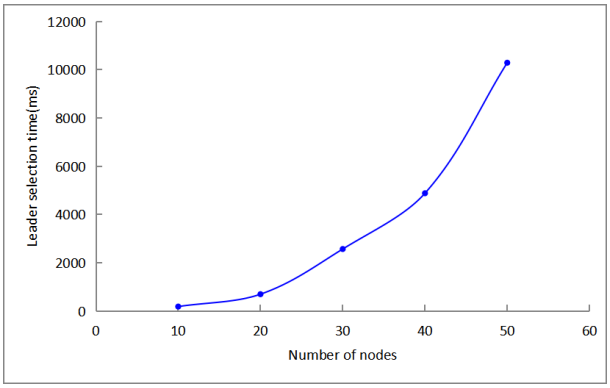

Fig.10. Leader selection time as the number of nodes is varied

For the calculation of the consensus time (from consensus group selection to the block creation), we can not provide an average time for consensus time, accounting for factors that may influence the duration of each step (variation of difficulty, number of nodes, and data size). Instead, we can consider using the following formula to calculate the consensus time:

$$CT = GT + LT + BT \tag{6}$$

where:
CT: Consensus Time.
GT: Consensus Group Time.
LT: Lead selection Time
BT: Block Creation Time.

5. Conclusions

In this work, we introduced a novel consensus mechanism called "Proof of Notoriety". It combines the advantages of both "Proof of Reputation" and "Proof of Authority" consensus algorithms and addresses the requirement for coin-independent consensus mechanisms in public blockchains.

Our consensus scheme employs a voting system where the weight of nodes plays a crucial role in determining the consensus participants. This weight is calculated by normalizing the notoriety score of each node. Furthermore, our approach incorporates a reputation system, where a node's reputation score is derived from various factors, including successfully mining blocks, active participation in the consensus process, and registering copyright data. Additionally, the authority status of a node, whether it is an official authority or not, is considered to enhance security. The reputation system and authority status are combined to calculate the notoriety score of each node. Through tests and evaluations, we have demonstrated that the proposed consensus mechanism is reasonable and energy-efficient for blockchain systems. On average, CPU usage is reduced by 8.5% when opting for proof of notoriety consensus compared to a traditional consensus such as proof of work with difficulty =4. Also, a 371.7 ms reduction in block creation time.

We note that our proposed approach can be improved by using Smart contracts that can automate the licensing process by defining the terms, conditions, and fees associated with the use of copyrighted content.

References

[1] I. Bashir, “Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained”, 2nd Edition, Packt Publishing Ltd, pp. 112-230, March 2018, ISBN-10:1788839048.

[2] D. Tapscott and A. Tapscott, “Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world”. Penguin, New York, May 2016, ISBN-10:1101980133.

[3] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”. Princeton University Press, July 2016, ISBN:9780691171692.

[4] C. Paar and J. Pelzl, “Understanding cryptography: A textbook for students and practitioners”, Springer Science & Business Media, 2010, doi: 10.1007/978-3-642-04101-3.

[5] N. Kube, “D. Drescher: Blockchain Basics: A Non-Technical Introduction in 25 Steps”, Financ Mark Portf Manag 32, pp. 329–331, August 2018, doi: 10.1007/s11408-018-0315-6.

[6] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda and S. Islam, “Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey”, in IEEE Access, vol. 10, pp. 113436-113481, January 2022, doi: 10.1109/ACCESS.2022.3216643.

[7] S. Islam, M. J. Islam, M. Hossain, S. Noor, K. -S. Kwak and S. M. R. Islam, "A Survey on Consensus Algorithms in Blockchain-Based Applications: Architecture, Taxonomy, and Operational Issues", in IEEE Access, vol. 11, pp. 39066-39082, April 2023, doi: 10.1109/ACCESS.2023.3267047.

[8] S. Aggarwala and N. Kumar, “Cryptographic consensus mechanisms☆☆Introduction to blockchain”, The Blockchain Technology for Secure and Smart Applications across Industry Verticals, vol. 121, pp. 211-226, January 2021, doi: 10.1016/bs.adcom.2020.08.011.

[9] T. Economy, “Consensus algorithms,” https://tokens-economy.gitbook.io/consensus/, Created on Sept, 2018, Accessed on March 14, 2023.

[10] F. Yang et al., “The survey on intellectual property based on blockchain technology,” in 2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS). IEEE, pp. 743–748, May 2019, doi: 10.1109/ICPHYS.2019.8780125.

[11] L. Luo, “Application of blockchain technology in intellectual property protection,” Mathematical Problems in Engineering, vol. 2022, Jun 2022, doi: 10.1155/2022/4641559.

[12] Z. A. Halloush and Q. M. Yaseen, “A blockchain model for preserving intellectual property”, In Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems (DATA '19). Association for Computing Machinery, New York, NY, USA, Article 53, pp. 1–5, December 2019, doi: 10.1145/3368691.3368744.

[13] A. Savelyev, “Copyright in the blockchains era: Promises and challenges,” Computer law & security review, vol. 34, no. 3, pp. 550–561, June 2018, doi:10.1016/j.clsr.2017.11.008.

[14] J.-L. de la Rosa et al., “On intellectual property in online open innovation for SME by means of blockchain and smart contracts”, EasyChair Preprint no. 6181, July 2021.

[15] S.Pech, “Copyright unchained: How blockchain technology can change the administration and distribution of copyright protected works”, Northwestern Journal of Technology and Intellectual Property, vol. 18, no. 1, November 2020.

[16] W. I. P. O. (WIPO), “Blockchain Whitepaper for IP Ecosystems”, Blockchain Whitepaper for IP Ecosystems (wipo.int), September 2021, Accessed on July 01, 2023.

[17] H. Song, N. Zhu, R. Xue, J. He, K. Zhang, and J. Wang, “Proof-of-contribution consensus mechanism for blockchain and its application in intellectual property protection”, Information Processing & Management, vol. 58, N° 3, p. 102507, May 2021, doi: 10.1016/j.ipm.2021.102507.

[18] O. Aluko and A. Kolonin, “Proof-of-reputation: An alternative consensus mechanism for blockchain systems”, International Journal of Network Security & Its Applications (IJNSA), Vol.13, No.4, pp. 23-40, July 2021, doi:10.5121/ijnsa.2021.13403.

[19] M. M. Islam and H. P. In, "Decentralized Global Copyright System Based on Consortium Blockchain with Proof of Authority," in IEEE Access, vol. 11, pp. 43101-43115, April 2023, doi: 10.1109/ACCESS.2023.3270627.

Authors’ Profiles

Ahmed Mounsif Kebir received his License degree in Computer Systems in the department of Computer Science from the University of Science and Technology of Oran, Mohamed Boudiaf (USTO-MB), Algeria, in July 2021. He obtained his MSc degree in Networking and Distributed Computing Systems in the department of Computer Science from U.S.T.O, Algeria in June 2023.

Asmaa Boughrara obtained from the University of Science and Technology of Oran, Mohamed Boudiaf (USTO-MB), Algeria, her License degree in computer science in 2007 and MSc degree in Computer Systems and Networks in 2009. She pursued her PhD degree in Computer Systems and Networks from USTO-MB, in 2015. In 2016, she joined the Department of Computer Science at USTO-MB and became lecture class B in 2017. Her main research areas are distributed systems, blockchain, and routing and switching.

How to cite this paper: Ahmed Mounsif Kebir, Asmaa Boughrara, "Proof of Notoriety: A Promised Consensus Mechanism for the Blockchain-based Copyright System", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.6, pp.32-44, 2024. DOI:10.5815/ijcnis.2024.06.03