Blockchain Architecture Based on Decentralised PoW Algorithm

Cinthia P. Pascual Caceres, Jose Vicente Berna Martinez,
Francisco Maciá Pérez, Iren Lorenzo Fonseca, Maria E. Almaral Martinez
Department of Computer Science and Technology, University of Alicante,
C/ San Vicente s/n, San Vicente del Raspeig, Spain.

***Abstract*—Blockchain has gained increasing popularity across various industries due to its decentralized, stable, and secure nature. Consensus algorithms play a crucial role in maintaining the security and efficiency of Blockchain systems and selecting the right algorithm can lead to significant performance improvements. This article aims to provide a comparative review of the most used Blockchain consensus algorithms, highlighting their strengths and weaknesses. Additionally, we propose a dissociated architecture for an efficient Blockchain system that doesn't compromise on security. A comparison is made between this architecture and the reviewed algorithms, considering aspects such as algorithm performance, energy consumption, mining, decentralization level, and vulnerability to security threats. The research findings demonstrate that the proposed architecture can support complex algorithms with high security while addressing issues related to efficiency, processing performance, and energy consumption.**

***Keywords*—Blockchain technology; proof of work; consensus algorithm; proof of stake; Dissociated-PoW; security; performance**

I. Introduction

Blockchain (BC) technology offers numerous advantages that make it highly relevant and applicable in various areas of life. As a result, it has gained significant importance and presence in diverse projects. The main benefits it provides are decentralization, immutability, integrity, and reliability. These qualities guarantee a high level of information protection throughout all phases of processing and storage [1]. This technology reached its pinnacle thanks to the rise of Bitcoin, primarily attributed to its ability to establish a decentralized ledger, ensure immutable records, and provide participant anonymity. These factors played a crucial role in driving the widespread adoption and recognition of blockchain technology [2]. However, it is precisely the strength of blockchain technology that also makes it increasingly challenging to manage. In its original form, blockchain utilizes a consensus algorithm known as Proof of Work (PoW) [3], this consensus algorithm used in blockchain requires a substantial computational effort, creating a situation where only large computer producers can effectively participate. This dynamic makes it financially unprofitable for smaller infrastructures to engage in the process [4]. To address this issue, blockchain (BC) has evolved in various directions, exploring different consensus algorithms and structures that can alleviate the computational costs. In this paper, we propose a solution that harnesses the security strengths of Proof of Work (PoW) while introducing a BC architecture built on functionally specialized nodes. This approach enables the efficient implementation of PoW while minimizing the computational expenses.

To this end, Section II reviews the state of the art and the main issues related to the work, especially reviewing the different lines of work that have been adopted from the original BC. Section III proposes the new architecture, the functional characterization of the operations and the description of the nodes. In Section IV, a comparison is made with the traditional BC to show the differences and similarities of the proposed architecture and, above all, the benefits. The last section finally shows the main conclusions of the proposal with possible lines of further work.

II. Background

First, BC networks developed from the original one proposed by Satoshi [5]. Depending on the participants involved, blockchain networks can be categorized as public, private, or hybrid. Additionally, the permissions granted for write and read operations on the blockchain determine whether it is classified as permissioned or permissionless. A blockchain can combine various aspects of participation and operation permissions, resulting in a wide range of scenarios that can be applied based on the specific organization and the type of application being implemented [6]. The choice of the blockchain type depends on the intended use case and the specific requirements of the organization.

In public blockchain networks, all individuals have the freedom to read, send, or validate transactions. Furthermore, they can actively participate in the distributed consensus process. The consensus mechanism relies entirely on the merits and contributions of individual nodes within the network, without the need for any centralized authority or control. This open and inclusive approach fosters transparency, decentralization, and trust among participants in the public blockchain network [2], nodes compete to achieve consensus. Unlike in a private network, there is no access control mechanism restricting participation. Nodes have the freedom to join or leave the network without causing harm to the consensus mechanism or the generation of new blocks [7]. This decentralized nature allows for a dynamic network where nodes can freely interact and contribute to the consensus process.

In private BC networks the addition and verification of new blocks are limited to specific users authorized by the controlling entity, which can be centralized or decentralized. In such networks, unauthorized users are unable to add information to the blockchain network and may even be restricted from accessing read capabilities. Unlike public networks, private networks necessitate consensus algorithms tailored to accommodate these permission restrictions [8].

Hybrid or consortium BC networks represent a combination of both public and private networks. In these networks, participating nodes are typically invited or selected, but all transactions are publicly visible and transparent. One of the benefits of these networks is the protection they provide against 51% attacks [9]. A 51% attack refers to a scenario where a single entity or group of nodes gains control of over 50% of the network's computing power, potentially enabling them to manipulate the blockchain. In a hybrid or consortium network, the distributed nature of participation helps safeguard against such attacks, as they require majority control, which is not easily attainable in these network configurations.

In fact, each type of blockchain network requires a consensus algorithm that suits its specific needs. A consensus algorithm is a set of rules and processes that govern the operation of a distributed system. Its main purpose is to resolve data synchronisation between untrusted nodes in a decentralised environment. Consensus algorithms ensure that all participants agree on the state of the blockchain and validate transactions in a consistent and secure manner. The choice of consensus algorithm depends on factors such as the type of network, the desired level of decentralisation, scalability requirements and security considerations [10].

The original consensus algorithm used in blockchain is Proof of Work (PoW); is a decentralised consensus algorithm that requires network participants to compete to solve a computational puzzle. This puzzle-solving process helps prevent malicious actors from manipulating the system and ensures the security and integrity of the blockchain. PoW is widely used in cryptocurrency mining, where participants validate transactions and mine new tokens, as in the case of the Bitcoin network. By dedicating computational resources and solving complex puzzles, miners contribute to the consensus process and maintain the decentralised nature of the blockchain network [11]. One of the main challenges and drawbacks of PoW is the significant computational capacity required to solve the mathematical problem involved in authenticating blockchain transactions. This computational intensity leads to high energy consumption and limits the scalability of PoW-based blockchain networks. The resource-intensive nature of PoW can also make it less accessible for smaller participants or entities with limited computing power. As a result, there has been a drive to explore alternative consensus algorithms that can address these limitations, such as Proof of Stake (PoS) or delegated proof of stake (DPoS) that do not require extensive computational power. These consensus algorithms enable participants to validate transactions and secure the network based on factors like the number of tokens held or reputation, rather than raw computing power [12]. To participate in a BC network that uses PoW as a consensus mechanism, it is essential to have advanced, powerful, expensive, and energy-consuming hardware [13], thus widely so that users currently must compete against pools of mining [14]. Due to the drawbacks and limitations of the Proof of Work (PoW) consensus algorithm, the blockchain community has developed and explored various alternative consensus algorithms. These alternative algorithms aim to address issues such as high energy consumption, scalability, and accessibility. Some of the popular alternative consensus algorithms include:

Proof of Stake (PoS): in PoS participants can create new blocks and validate transactions based on the number of tokens they hold or "stake" in the network. This approach reduces energy consumption and allows for a more efficient and scalable consensus mechanism. Consensus algorithm was the next algorithm to appear. It works by encouraging users to always keep a certain number of cryptocurrencies in the wallet [15]. Keeping these cryptocurrencies locked helps participants increase their chances of being chosen, as this is one of the main criteria set for participation. Once these criteria have been established, the random node selection process begins. When the nodes are chosen and the selection process is finished, they are ready to validate transactions or create new blocks. It is more environmentally friendly than PoW as it does not require large amounts of computational power to operate [16] The security of the network is much higher as it solves or hinders certain known attack schemes, such as the 51% attack, overall, PoS offers benefits such as energy efficiency, increased network security, and improved scalability. It is an alternative consensus algorithm that has gained popularity in blockchain networks seeking to address the limitations of PoW.

Delegated Proof of Stake (DPoS): it is a consensus algorithm commonly used in blockchain networks. It is designed to address some of the limitations of traditional Proof of Stake (PoS) algorithms and aims to achieve faster transaction processing and increased scalability [4]. Referring to a more decentralised form in the BC network, it also modifies the way power is used, decreasing in frequency. With this algorithm, users can give their votes on who they want to mine the next block. Thus, it offers high levels of security for use in public BCs. Besides this, its operating model guarantees high levels of scalability. To make this possible, each participant in the network chooses, by voting, several "delegates". Once chosen, they form an ensemble that offers Byzantine Fault Tolerance (BFT) [17].

Delegated Byzantine Fault Tolerance (dBFT): consensus algorithm's main objective consists in giving the right to all stakeholders to be an active member through the voting procedure to solve the problems in the blockchain in a democratic and fair way. It is an algorithm that combines the characteristic of the DPoS algorithm, but unlike the DPoS algorithm, delegate nodes are elected to validate the new block, and where at least 2/3 must approve it [18]. In this way, the network can make decisions even if one third of the nodes are harmful or corrupted [19].

The Proof of Activity (PoA): relies on a set of approved validators who are known and trusted. Validators take turns creating new blocks, and consensus is achieved based on their identity and reputation. It is a combination of PoW and PoS [20]. Initially the system works in PoW where miners try to solve a mathematical equation using high computational capabilities. Once a new block is generated, the system switches to PoS, a group of validators is chosen at the start, and they will oversee verifying or signing the new block. Validators are elected and sign the new block. More coins a validator possesses, more likely to be elected and sign [21]. A 51% chance of an attack is also avoided in this algorithm.

Proof of Burn (PoB): consensus algorithm works in such a way that miners must send cryptocurrencies to a public and verifiable address, from which they will not retrieve them again, burning them. In other words, miners must make a kind of investment and the higher the number of cryptocurrencies burned, the more mining the miner achieves [22]. Its main benefit is that, with a higher percentage of long-term investors, price stability may increase. Also, PoB assists in determining the distribution of cryptocurrencies in a fair and decentralised manner. Reduction in the number of resources needed to achieve consensus compared to PoW is considerable and it also has resistance to double spending attack.

Proof of Capacity (PoC): consensus algorithm enables network mining devices to use their available hard disk space to decide entitlements when mining and validating transactions [23]. Differentiating this with the use of the computational power of the PoW mining device or the miner's participation in PoS cryptocurrencies. As a benefit, any hard drive can be used, including those with Android-based operating systems. Mining data can be easily erased, and the drive can be reused for any other data storage purpose. Compared to PoW [24], this improves the resource consumption for consensus by up to 30 times less.

The Proof of Elapsed Time (PoET): is a consensus algorithm that aims to achieve decentralized consensus while minimizing energy consumption. PoET was introduced by Intel as a consensus algorithm for use in private and permissioned blockchain networks.

In PoET, participants in the network compete to become the leader or validator of the next block. However, instead of relying on computational power or staking, PoET uses a random lottery-based approach. Each participant in the network waits for a randomly generated timer to expire [25]. The participant whose timer expires first becomes the leader and gets the right to create the next block.

To prevent participants from manipulating the system by manipulating timers, PoET uses a trusted execution environment (TEE). The TEE provides a secure and tamper-resistant environment for generating the random timers. This ensures fairness and prevents participants from predicting or influencing the timer outcomes.

The next algorithm is a new consensus mechanism using less energy and can run on low-end hardware, Proof of Assignment (PoA), developed by IOTW [26]: this algorithm can process thousands of transactions per second and has been introduced for micro mining, allowing for lightweight mining on IoT devices by eliminating the need to store and maintain the transaction ledger at the device level. Instead, the storage and maintenance of the ledger is outsourced to one or more pre-established trusted nodes in the BC network. It can run on hardware of any IoT device [27].

The Ripple Protocol Consensus Algorithm (RPCA): to maintain the veracity and consensus of the network, constantly updates its nodes; once consensus is reached, the current ledger is "closed" and becomes the last closed ledger. Assuming the success of the consensus algorithm, and that there is no fork in the network, the last closed ledger held by all nodes in the network will be identical [28]. Among its features is that the validation of transactions is immediate, reducing the time of each operation. In addition, the costs per transaction are also very low and the Ripple cryptocurrency has greater flexibility compared to other cryptocurrencies for international payments, it is oriented for monetary transactions between banks, a competitor of the SWIFT system [29].

The development of consensus algorithms aims to preserve the power and robustness of PoW while addressing its inherent challenges. However, it is essential to acknowledge that changing the consensus algorithm does not necessarily guarantee the elimination of problems, but rather introduces new considerations and trade-offs.

The proposal to shift the focus of innovation in blockchain from creating new algorithms to designing new architectures to solve existing problems is an interesting approach. By reimagining the underlying architecture, it becomes possible to optimize the performance, scalability, and energy efficiency of blockchain networks, while still leveraging existing consensus algorithms like PoW. This architecture will be called Dissociated Proof of Work (Dissociated-PoW).

III. Dissociated-PoW Architecture

The proposed Dissociated-PoW architecture aims to address the high computational cost associated with competition between mining nodes in Proof-of-Work based blockchain networks. This architecture introduces two types of functionally specialised nodes: coordinator nodes (CN) and mining nodes (MN). Each type of node and its function is described below:

- Coordinator nodes: Serving as central entities, coordinator nodes take charge of coordinating the mining process and facilitating the consensus algorithm. They play a crucial role in selecting and assigning mining tasks to the mining nodes. Furthermore, CN are responsible for overseeing the overall operation of the blockchain network and ensuring the integrity of the consensus process.
- Mining nodes: Dedicated to performing the computational work required to mine new blocks on the blockchain, mining nodes form the scheme of the Dissociated-PoW architecture. These nodes receive mining tasks from the coordinator nodes and leverage their computational resources to solve the PoW puzzle and validate transactions. MNs are pivotal in generating new blocks and maintaining the continuity of the blockchain.

This proposed architecture has the potential to enhance the efficiency and scalability of blockchain systems while preserving the fundamental principles of decentralization and trust. Further research and experimentation are needed to validate its effectiveness and practicality in real-world scenarios.

A traditional blockchain scheme exhibits the typical structure wherein all nodes participate in the mining competition, leading to high computational costs. In contrast, the proposed Dissociated-PoW scheme introduces a separation of tasks between coordinator nodes and mining nodes, resulting in a more efficient and optimized mining process.

The Dissociated-PoW architecture has the potential to mitigate the drawbacks of traditional PoW-based blockchain networks by reducing computational costs and optimising mining resource allocation. However, it is important to thoroughly analyse and evaluate the proposed architecture in terms of security, decentralisation, and performance to ensure its effectiveness in real-world scenarios.

A. *Coordinating Nodes are responsible for the following Tasks*

- Receiving and storing new information to be inserted into the blockchain.
- Managing the pending transactions PT, which form a block of information containing all the pending transactions that will be mined to generate the next block of the blockchain. PT is a block of transactions that are replicated and synchronized among all coordinating nodes.
- Deciding when to initiate the mining process by utilizing rules to trigger mining based on criteria like a timeout or reaching a maximum PT size.
- To decide who will be the MNs to mine the next PT.

B. *Mining Nodes are responsible for the following Tasks*

- Maintaining the blockchain to ensure it is accessible for any user. Each MN contains a copy of the entire blockchain.
- Mining the next block of the BC without engaging in competition. The MN receives the pending transactions PT from a CN and performs the mining process. Once the mining is completed, the new block is broadcasted to the BC.

In our proposal, it is the CN that instruct a specific MN to carry out the mining process, providing it with the necessary information to be mined, which includes the pending transactions, as illustrated in Fig. 1.

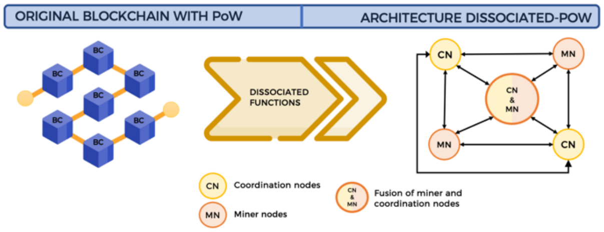
ORIGINAL BLOCKCHAIN WITH PoW
ARCHITECTURE DISSOCIATED-POW
BC
BC
BC
BC
BC
BC
BC
DISSOCIATED FUNCTIONS
CN
MN
CN & MN
MN
CN
CN
Coordination nodes
MN
Miner nodes
CN & MN
Fusion of miner and coordination nodes

Fig. 1. Converting a traditional blockchain into a dissociated blockchain.

Once mined, the new block will be distributed among the other mining nodes. This approach ensures that MN do not compete to be the first to mine; instead, it is the coordinating nodes who make the decision on which MN will perform the mining task. The selection process can be based on efficiency and effectiveness to ensure that the network utilizes the minimum computational resources.

To prevent fraudulent transactions from being injected into the blockchain, all nodes within the network must be aware of all members' identities. This involves maintaining an up to date Blockchain node list (BCNL) for each node, containing information about the participants in the network. This measure ensures transparency and security, as all nodes have knowledge of the network's composition.

As shown in the proposed Dissociated-PoW architecture, the dissociation of mining tasks and the coordination provided by the CN contribute to a more efficient, secure, and decentralized blockchain network.

Action flows of the CN for the specified tasks:

1) Receiving a new transaction:

- A coordinating node receives a new transaction to be included in the blockchain.

2) Adding it to the pending transactions:

- The CN incorporates the new transaction into its own pending transactions PT block.

3) Disseminating the new transaction among the rest of the CN:

- The CN broadcasts the new transaction to all other coordinating nodes to ensure they are informed about the pending transaction.
- It is essential to ensure that the transactions are inserted into the PT block in the same order among all coordinating nodes during dissemination.

4) Validating the origin of the new transaction:

- Other coordinating nodes verify the origin and validity of the new transaction sent by the CN.

5) Synchronizing all the pending transactions:

- After validation, all coordinating nodes have the same block of pending transactions, ensuring synchronization.

As for mining, it is performed in the following way with a leader node among the CN:

1) Detecting the mining start condition:

- The leader CN detects the condition to initiate the mining process.

2) Notifying other CN nodes about mining:

- The leader CN notifies all other CN nodes that mining is about to proceed, prompting them to freeze the current pending transactions block and mark it as in the mining state.

3) Selecting a MN to mine the pending transactions:

- The leader CN selects a MN from the Blockchain Node List (BCNL) to mine the current pending transactions block and sends the pending transactions block to be mined.

4) Notifying completion and disseminating the new block

- Once the selected MN finishes mining, it notifies the CN that initiated the mining process and disseminates the new block to all other MNs.

5) Indicating the end of mining and validating the mined block:

- The leading CN indicates to the other CN that mining is finished and that the previous block of transactions can be finalized.
- The rest of the CN verify the correctness of the mined block and conclude the mining operation. As shown in the Fig. 2.

This process, with a designated leader node among the CN, ensures a coordinated and efficient mining process in the Dissociated-PoW architecture, promoting consistency and integrity throughout the blockchain network. As shown in Fig. 3.

Action flows to start mining:

1) The leading CN decides when to initiate the mining process.

2) The leading CN notifies the rest of the CN to begin mining and instructs them to freeze the current pending transactions (PT) block.

3) The leading CN selects a node from the network to perform the mining task and sends the PT block to that node.

4) The selected mining node informs the leading CN when it has completed the mining process and broadcasts the newly mined block to all other MN.

5) The leading CN notifies all the other CN that the previous mining process has concluded, and the mined PT can be removed.

The synchronization between Coordinator nodes in the Dissociated-PoW blockchain network follows a functional model that is similar to node coordination in a Kafka cluster [28]. A leader node is designated, and the rest of the CN become followers. Only the leader node can determine the timing of mining and which MN will be responsible for the mining task. The designation of a leader node is based on the order of entry to the BC network, and in the event of the leader node's failure, the next node in the list is designated as the new leader. Every CN has a synchronized PT block, so if any CN goes down, as long as there is at least one CN remaining in the network, the process continues uninterrupted.

Nodes may enter the BC network with the roles of MN, CN, or both. However, having both roles do not give priority to the node in being designated as a MN. The decision of exactly when to start mining follows predefined rules in the BC. Typically, mining is triggered when a certain number of pending transactions is reached or when a specific time limit between mining operations is reached if there are pending transactions. Additionally, a maximum pending transaction limit criterion is used to restrict the size of the block to be mined. Employing a time limit criterion ensures that transactions are not left waiting indefinitely to be mined. Deciding exactly when to mine simply follows predefined rules in the BC. Normally, mining is set when a certain number of pending transactions is reached or when a certain time limit between mining is reached, if there are pending transactions. A maximum PT limit criterion limits the size of the block to be mined. Using a time limit criterion allows transactions not to be left eternally waiting to be mined.

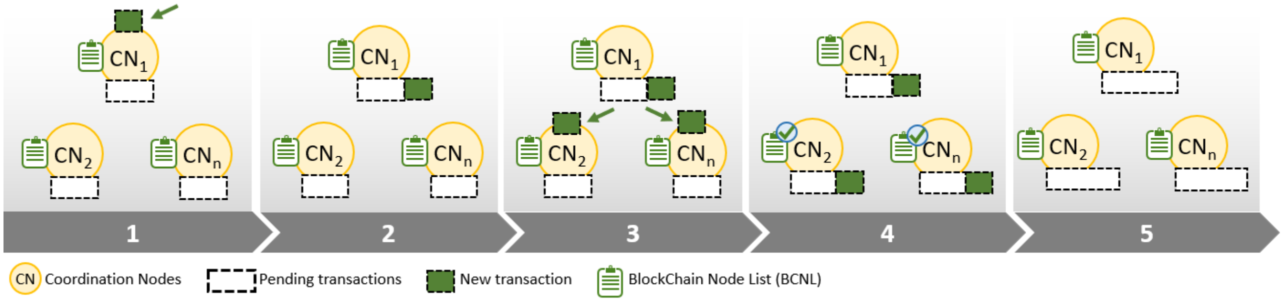

Fig. 2. Action flows of the coordination nodes for the specified tasks.

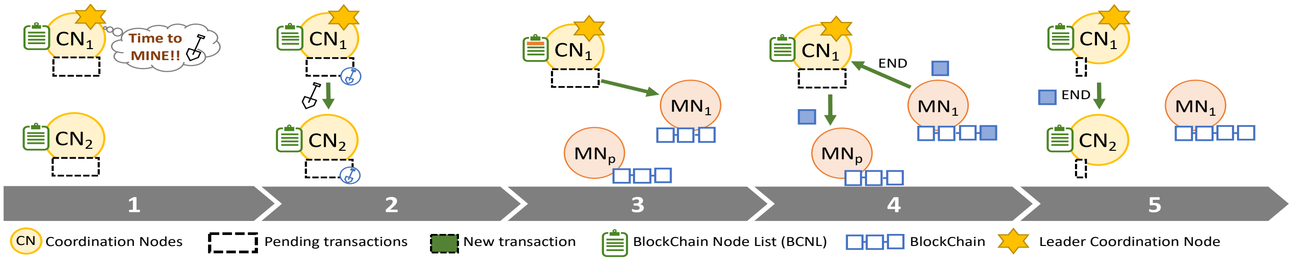

Fig. 3. Action flows to start mining nodes.

When the leading CN determines that mining is necessary, it instructs the other CN in the network to freeze the PT block, ensuring that any new incoming transactions are directed to a new temporary PT block. This way, the PT block being mined remains unchanged.

The BCNL (Blockchain Node List) is utilized to select the main CN responsible for mining the PT block. This list contains all the nodes comprising the BC network, their respective roles, the PT blocks mined by each node, and their hardware specifications. Moreover, nodes can provide information about their performance status. For instance, if a node is experiencing overload at a given time, it can indicate this in the BCNL to avoid being designated as a mining node. With access to this list, the leading CN can choose the most suitable node at that moment, taking certain constraints into consideration:

- The best-performing node will be selected from the BCNL list.
- Mining distribution will be balanced to ensure that all nodes in the list participate in the mining process.
- If no MN can be designated, the leading CN will keep the block as pending mining until a node from the list becomes available.

To participate as an MN, the BC may require a minimum level of computational resources to ensure that mining can occur in a timely manner. Additionally, even the leading BC may reject a mining request made to a node if it determines that the node will be unable to complete the mining task. In such cases, the request will be redirected to a new MN.

This approach enables the Dissociated-PoW architecture to efficiently manage mining tasks and ensure that mining is carried out optimally based on the performance capabilities of the participating nodes.

IV. Benchmarking Proposal Compared against other Algorithms

This proposal, as discussed in the previous section, offers several benefits that make the Dissociated-PoW consensus algorithm more effective than other existing algorithms, overcoming many of the disadvantages present in traditional ones. In this chapter, we will compare our Dissociated-PoW algorithm with the following consensus algorithms: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Delegated Byzantine Fault Tolerance (dBFT), Proof of Activity (PoA), Proof of Burn (PoB), Proof of Capacity (PoC), Proof of Elapsed Time (PoET), Proof of Assignment (PoA), Proof of Checkpoint (PoC), and Ripple Protocol Consensus Algorithm (RPCA).

As mentioned earlier, the main disadvantage of PoW is the substantial computational and energy requirements to solve the consensus test, with exclusive resource usage that cannot be utilized for other tasks. Additionally, the well-known 51% attack poses a significant problem, with the algorithm being dominated by large mining pools. On the contrary, our proposal ensures that only the designated mining node invests computational and energy resources, leading to substantial savings as there is no competition among nodes. By dissociating the selection of the time and mining node from the traditional competition algorithm, we also eliminate the risk of a 51% attack, ensuring that no entity dominates the PoW algorithm and avoiding the dominance of large miners.

In PoS, significant drawbacks include challenges in maintaining miner anonymity, as those who invest the most in the BC end up being the dominant miners in solving the consensus algorithm. Scalability issues and potential slow transactions also arise. In Dissociated-PoW, the CN oversees selecting the best candidate for mining, guaranteeing investor anonymity and independence from major stakeholders. As the network has specialized nodes dedicated to BC maintenance, the quality of service is assured, avoiding collapsed nodes except for the one that may be mining at any given time. However, as the BC is replicated in the rest of the nodes, its operation can be supported by a nearby node.

The DPoS algorithm is also vulnerable to centralization due to its limited number of nodes in the network, and transactions are not anonymous. In Dissociated-PoW, all transactions are anonymous, and the number of nodes is organized by the CN and MN responsible for distributing the workload.

The dBFT algorithm employs a relatively recent protocol that has not been extensively tested in large Blockchain networks, making it susceptible to centralization with a limited number of representing nodes. Similar to DPoS, transactions are not anonymized. Dissociated-PoW addresses these concerns by having a specific group of nodes that focus on coordinating work and sending pending transactions to MN to commence mining after a certain period.

Overall, Dissociated-PoW offers improved anonymity, decentralization, and scalability while mitigating the vulnerabilities present in other consensus algorithms, making it a promising choice for effective and efficient blockchain networks.

In the PoET algorithm there is no anonymity. Making it vulnerable to Sybil attacks [30], The more malicious nodes there are, the higher the likelihood that some of them will be involved in block formation. In contrast, in Dissociated-PoW, participants remain anonymous, and as the CN are responsible for overseeing mining, Sybil attacks among the MN are not possible. As for the CN, malicious actions may involve attempting to extract a fake PT packet, but this would be detected by the other CN. They could also try to slow down the BC network, but this would be detected as a failure of the leading CN, and the next CN in the list would take the lead. Additionally, they may attempt to overload an MN by sending it all mining requests, but the MN can update its status in the BCNL at any time to prevent receiving further requests.

On the other hand, Proof of Assignment (PoA) has limitations in capacity due to the processing speed and available memory of IoT devices. In Dissociated-PoW, capacity is not limited during the processing of PTs as the CNs choose the best available miner node, balancing network loads to avoid saturating a single node.

For the Proof of CheckPoint (PoC) algorithm, trust nodes external to the network are required. In Dissociated-PoW, no external nodes are needed as it only involves the coordinator and miner nodes.

In the RPCA algorithm, the network is exposed to centralization as the number of nodes representing the network is very limited, and transactions are not anonymous. In Dissociated-PoW, the CN and MN are responsible for selecting the best candidate to start mining, guaranteeing investor anonymity, and not relying on centralized entities.

Overall, Dissociated-PoW offers advantages over several existing consensus algorithms by ensuring participant anonymity, mitigating vulnerabilities to Sybil attacks, and avoiding the need for external trust nodes while maintaining high processing capacity and network decentralization.

In the next Table I, issues presented within the current algorithms can be grouped as follows:

1) Anonymity loss: This criterion evaluates whether the algorithm preserves the anonymity of nodes participating in the blockchain network. A "Yes" indicates that the algorithm does not provide strong anonymity, meaning that at some point, the identities of network nodes or owners can be identified. Dissociated-PoW receives a "No" in this category, meaning it preserves anonymity.

2) Deployment: This criterion assesses the complexity of implementing the consensus algorithm. A "Simple" deployment means that the algorithm is straightforward and easy to implement, while a "Complex" deployment suggests that it requires more effort and expertise to set up. Dissociated-PoW is considered "Simple" in this regard.

3) Non-Vulnerable to centralization: This criterion determines whether the consensus algorithm is at risk of centralization, where a small number of nodes gain excessive control over the network. A "Yes" indicates vulnerability to centralization, while a "No" means the algorithm is designed to resist centralization. Dissociated-PoW is not vulnerable to centralization.

4) Resources in network: This criterion evaluates the number of resources (such as computational power, memory, etc.) needed to maintain the blockchain network. "High" resources mean considerable requirements, while "Low" resources indicate that the algorithm can operate efficiently with minimal resources. Dissociated-PoW requires low resources.

5) Low computing load: This criterion assesses the power consumption and computing demand of the consensus algorithm. "Yes" indicates that the algorithm has low computing load, while "No" means it is computationally intensive. Dissociated-PoW has low computing load.

6) IoT device friendly: This criterion determines whether the consensus algorithm is suitable for IoT devices, which often have limited processing capabilities. "Yes" means the algorithm is compatible with IoT devices, while "No" suggests it may not be well-suited. Dissociated-PoW is friendly to IoT devices.

The comparison table shows that Dissociated-PoW performs well in terms of preserving anonymity, simplicity of deployment, non-vulnerability to centralization, efficient resource usage, low computing load, and compatibility with IoT devices. However, it's important to note that each algorithm has its strengths and weaknesses, and the best choice depends on the specific requirements and goals of the blockchain network being considered (see Table I).

TABLE I. OVERVIEW OF THE PROPERTIES OF VARIOUS CONSENSUS ALGORITHMS COMPARED TO DISSOCIATED-POW

Consensus Algorithm	**1**	**2**	**3**	**4**	**5**	**6**
Pow	Yes	Complex	No	High	No	No
Pos	Yes	Simple	No	Low	Yes	No
DPos	Yes	Simple	No	Low	Yes	No
dBFT	Yes	Simple	No	Low	Yes	No
PoA	Yes	Simple	No	Low	Yes	No
PoB	Yes	Complex	No	High	No	No
PoC	Yes	Complex	No	High	No	No
PoET	Yes	Complex	No	Low	Yes	Yes
PoA	Yes	Simple	Yes	Low	Yes	Yes
PoC	Yes	Simple	No	Low	Yes	No
RPCA	Yes	Simple	No	Low	Yes	Yes
Dissociated-Pow	No	Simple	No	Low	Yes	Yes

V. DISSOCIATED-POW PROBLEMS

Introducing a new architecture, such as Dissociated-PoW proposal, may indeed bring certain potential drawbacks. One of the concerns is the possibility of malicious coordinator nodes and mining nodes gaining access to the network, particularly in a public network where there are no access control mechanisms.

A. Mining Nodes Vulnerabilities

Potential vulnerabilities in this section will describe the possible security issues arising from malicious actions or failures in the mining nodes. Details of the CNs and MNs for the transactions that are integrated in the blockchain have been presented so far. The key to its operation is the validation of the transaction. For this reason, mining, consisting of closing the block and distributing it in the BC, must be carried out. As stated, miners communicate among themselves.

B. Eternal Mining (Lack of Computing)

Typical blockchain mining issues include the possibility of a mining node never finishing or being too late, either if the mathematical problem to be solved turns out to be very complicated or if the node does not have sufficient computational capacity at that time. To resolve this situation, CN must maintain a time limit. Once this limit is exceeded without results, the CN will withdraw the right to mine from the selected node and pass it to another CN, providing an opportunity for the block generation to occur. Alternatively, a function could be implemented where the MN is not removed from the mining right, but another new node is selected to start mining to check if it can deliver a result before the original node. This way, even if the first node fails, no computing power will have been wasted.

C. Malicious and Vulnerable Coordinating Nodes and Miners

Malicious MN may attempt to mine fake content, i.e., transactions that were not originally processed by the CN, and try to sneak them in. After they finish mining the MNs, send the new block to the CN, whose job it is to validate that the node is correct, and therefore if they have tried to introduce transactions that were not in the original PT, they will be discarded. If it is correct, it will be distributed to other MN and CN, and in turn the CN will distribute it to nearby MN. If it is a malicious node, it is kicked out and otherwise distributed to the rest of the MN nodes in the network. Potential vulnerabilities caused by malicious actions or failures in the coordinator nodes will be described in this section.

D. Trying to Crash a Mining Node

It consists of a CN involuntarily sending mining requests to the same MNs all the time, overloading them with work. A BCNL exists, where CN may update their state to not receive requests. In Dissociated-PoW, there is a list called BCNL, where CN may update status for MN to not accept and receive any more requests, avoiding overloading MN. For an MN to receive a PT, it must receive a low mining workload.

E. Not Launching the Mining Process

As the leader CN oversees determining the start of mining, should this node fail for any reason, orphaned mining won't start. Other CN must enable a mechanism for detecting such a situation and designate new leaders independently. The role of the CN is to supervise the proper functioning of the leader node. As there are several CN, if a lag is detected, a second CN takes over leadership, notifying other CN of the incident, and the current leader is automatically substituted.

F. The CN is Malicious and Orders False Content to be Mined

Upon distribution of a new BC block, it must be validated through its BCNL by all CN to identify whether it is a bogus block or not. If it is a bogus block, it must be discarded and removed from the network.

To mitigate these potential drawbacks, it is important to implement robust security measures, access controls, and thorough vetting processes for CN and MN. Additionally, ongoing monitoring, auditing, and regular updates to the architecture can help address emerging security concerns and maintain a healthy and secure network environment.

It is essential to thoroughly analyse and address these potential drawbacks when designing and implementing a new architecture to ensure the overall security and integrity of the blockchain network.

VI. Conclusion and Future Work

This research makes several valuable contributions to the field of blockchain technology and consensus algorithms. First and foremost, it presents the Dissociated-PoW algorithm as a novel and innovative solution to address the limitations of traditional Proof of Work and other existing consensus algorithms. By functionally specializing nodes, Dissociated-PoW efficiently implements PoW while minimizing computational expenses, making it more sustainable and scalable for diverse blockchain networks.

Furthermore, the comprehensive analysis and comparison of various consensus algorithms provide valuable insights into their strengths, vulnerabilities, and suitability for different use cases. This analysis aids researchers, developers, and decision-makers in understanding the trade-offs between different consensus mechanisms, guiding them in choosing the most appropriate algorithm for their specific blockchain applications.

The proposed future work of building a robust framework that encompasses multiple consensus algorithms and emphasizes privacy safeguards across different blockchain architectures is forward-thinking and crucial for the continued advancement of blockchain technology. By addressing issues like high computational demands, network performance, and node failures, the research contributes to the development of more secure, efficient, and resilient blockchain networks.

Despite these significant contributions, the research also acknowledges certain limitations. Firstly, due to the complexity and variety of blockchain networks and consensus algorithms, conducting a detailed analysis of all possible combinations may not be feasible within the scope of this research. However, the chosen approach of comparing existing algorithms provides valuable insights and lays the foundation for future research to explore additional combinations and innovations.

Additionally, as with any research in the rapidly evolving field of blockchain technology, the proposed Dissociated-PoW algorithm and future framework may face challenges in real-world implementation. Practical testing and validation on various blockchain networks will be essential to ensure the algorithm's effectiveness and security.

Inclusive, this research makes a significant scientific contribution by proposing a novel consensus algorithm, conducting a thorough comparative analysis, and outlining a comprehensive roadmap for future work. It offers valuable insights into the state of blockchain consensus algorithms and provides a foundation for advancing the field, addressing limitations, and shaping the future of decentralized systems.

References

[1] M. N. M. Bhutta et al., “A Survey on Blockchain Technology: Evolution, Architecture and Security,” IEEE Access, vol. 9, pp. 61048–61073, 2021, doi: 10.1109/ACCESS.2021.3072849.

[2] C. S. Wright, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008, Accessed: Nov. 03, 2021. [Online]. Available: https://ssrn.com/abstract=3440802.

[3] G. Pîrlea, “Mechanising Blockchain Con-sensus,” vol. 18, 2018, doi: 10.1145/3167086.

[4] S. Aggarwal and N. Kumar, “Cryptographic consensus mechanisms,” Adv. Comput., vol. 121, pp. 211–226, Jan. 2021, doi: 10.1016/BS.ADCOM.2020.08.011.

[5] J. Sidhu, “Syscoin: A peer-to-peer electronic cash system with blockchain-based services for E-business,” 2017 26th Int. Conf. Comput. Commun. Networks, ICCCN 2017, Sep. 2017, doi: 10.1109/ICCCN.2017.8038518.

[6] B. Chase and E. MacBrough, “Analysis of the XRP Ledger Consensus Protocol,” Feb. 2018, Accessed: Nov. 03, 2021. [Online]. Available: http://arxiv.org/abs/1802.07242.

[7] G. Falazi, M. Hahn, U. Breitenbucher, F. Leymann, and V. Yussupov, “Process-based composition of permissioned and permissionless blockchain smart contracts,” Proc. - 2019 IEEE 23rd Int. Enterp. Distrib.

Object Comput. Conf. EDOC 2019, pp. 77–87, Oct. 2019, doi: 10.1109/EDOC.2019.00019.

[8] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on Private Blockchain Consensus Algorithms," Proc. 1st Int. Conf. Innov. Inf. Commun. Technol. ICIICT 2019, Apr. 2019, doi: 10.1109/ICIICT1.2019.8741353.

[9] Z. Cui et al., "A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN," IEEE Trans. Serv. Comput., vol. 13, no. 2, pp. 241–251, Mar. 2020, doi: 10.1109/TSC.2020.2964537.

[10] G.-T. Nguyen and K. Kim, "A Survey about Consensus Algorithms Used in Blockchain," 2018, doi: 10.3745/JIPS.01.0024.

[11] S. R. Niya et al., "Adaptation of Proof-of-Stake-based Blockchains for IoT Data Streams," 2019 IEEE Int. Conf. Blockchain Cryptocurrency, pp. 15–16, May 2019, doi: 10.1109 / BLOC.2019.8751260.

[12] A. Endurthi and A. Khare, "Two-Tiered Consensus Mechanism Based on Proof of Work and Proof of Stake," Proc. 2022 9th Int. Conf. Comput. Sustain. Glob. Dev. INDIACom 2022, pp. 349–353, 2022, doi: 10.23919/INDIACOM54597.2022.9763215.

[13] P. R. Nair and D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain," Proc. 3rd Int. Conf. Intell. Commun. Technol. Virtual Mob. Networks, ICICV 2021, pp. 279–283, Feb. 2021, doi: 10.1109/ICICV50876.2021.9388487.

[14] Y. F. Wen and C. Y. Huang, "Exploration of Mined Block Temporarily Holding and Enforce Fork Attacks by Selfish Mining Pool in Proof-of-Work Blockchain Systems," IEEE Access, vol. 10, pp. 61159–61174, 2022, doi: 10.1109/ACCESS.2022.3181186.

[15] W. Li, S. Andreina, J. M. Bohli, and G. Karame, "Securing Proof-of-Stake Blockchain Protocols," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10436 LNCS, pp. 297–315, Sep. 2017, doi: 10.1007/978-3-319-67816-0_17.

[16] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco, and P. Wightman, "The 51% Attack on Blockchains: A Mining Behavior Study," IEEE Access, vol. 9, pp. 140549–140564, 2021, doi: 10.1109/ACCESS.2021.3119291.

[17] Q. Hu, B. Yan, Y. Han, and J. Yu, "An Improved Delegated Proof of Stake Consensus Algorithm," Procedia Comput. Sci., vol. 187, pp. 341–346, Jan. 2021, doi: 10.1016/J.PROCS.2021.04.109.

[18] X. Qi et al., "A Byzantine Fault Tolerant Storage for Permissioned Blockchain," Proc. ACM SIGMOD Int. Conf. Manag. Data, pp. 2770–2774, 2021, doi: 10.1145/3448016.3452744.

[19] C. Zhang, C. Wu, and X. Wang, "Overview of Blockchain Consensus Mechanism CCS Concepts •Networks→ Network properties→ Network security→ Security protocols," 2020, doi: 10.1145/3404512.3404522.

[20] BentovIddo, LeeCharles, MizrahiAlex, and RosenfeldMeni, "Proof of Activity," ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, Dec. 2014, doi: 10.1145/2695533.2695545.

[21] W. Jing, "A Decentralized User Authentication Model Based on Activity Proof : Use the new user identity credential: Activity map," Proc. - 2020 Int. Conf. Commun. Inf. Syst. Comput. Eng. CISCE 2020, pp. 207–212, Jul. 2020, doi: 10.1109/CISCE50729.2020.00047.

[22] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-Burn," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 12059 LNCS, pp. 523–540, Feb. 2020, doi: 10.1007/978-3-030-51280-4_28.

[23] R. McAdam, M. McAdam, and V. Brown, "Proof of concept processes in UK university technology transfer: an absorptive capacity perspective," R&D Manag., vol. 39, no. 2, pp. 192–210, Mar. 2009, doi: 10.1111/J.1467-9310.2008.00549.X.

[24] S. Masseport, B. Darties, R. Giroudeau, and J. Lartigau, "Proof of Experience: Empowering Proof of Work protocol with miner previous work," 2020 2nd Conf. Blockchain Res. Appl. Innov. Networks Serv. BRAINS 2020, pp. 57–58, Sep. 2020, doi: 10.1109/BRAINS49436.2020.9223277.

[25] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On Security Analysis of Proof-of-Elapsed-Time (PoET)," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 10616 LNCS, pp. 282–297, Nov. 2017, doi: 10.1007/978-3-319-69084-1_19.

[26] F. Leung, T. Chan, K. R. Mehrotra, and P. Chan, "ANAPP BLOCKCHAIN TECHNOLOGIES LIMITED A Scalable Blockchain-Proof of Assignment Protocol IOTW Highly secure IoT ecosystem, enabling Instant transaction and green micro mining from any connected device-no extra hardware, no additional cost. Whitepaper," 2020.

[27] M. H. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency," Ann. Emerg. Technol. Comput., vol. 2, no. 1, pp. 1–6, Jan. 2018, doi: 10.33166/aetic.2018.01.001.

[28] V. Clincy and H. Shahriar, "Blockchain development platform comparison," Proc. - Int. Comput. Softw. Appl. Conf., vol. 1, pp. 922–923, Jul. 2019, doi: 10.1109/COMPSAC.2019.00142.

[29] D. Schwartz, N. Youngs, and A. Britto, "The Ripple Protocol Consensus Algorithm", Accessed: Feb. 24, 2022. [Online]. Available: https://arxiv.org/abs/1802.07242

[30] J. R. Douceur, "The sybil attack," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2429, pp. 251–260, 2002, doi: 10.1007/3-540-45748-8_24.