Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption

Abigael Okikijesu Bada
Computing & Informatics
Bournemouth University
Poole, UK

Amalia Damianou
Computing & Informatics
Bournemouth University
Poole, UK

Constantinos Marios Angelopoulos
Computing & Informatics
Bournemouth University
Poole, UK

Vasilios Katos
Computing & Informatics
Bournemouth University
Poole, UK

***Abstract*—Organizations all over the world are under pressure to reduce their use of non-renewable energy sources and carbon emissions into the atmosphere due to its increasing negative impact on the ongoing climate crisis. Blockchain is a disruptive technology popularised by its use in Bitcoin, which has subsequently been adopted for various use cases. However, recently Blockchain has started attracting negative attention due to its propensity for high energy consumption depending on the adopted consensus mechanism. In this work, we explore the need for green (sustainable) Blockchain by comprehensively reviewing the various existing consensus mechanisms and their energy consumption to present a framework that will contribute towards developing more sustainable and environment friendly Blockchain-enabled systems.**

***Index Terms*—Blockchain; Consensus Mechanisms; Green IT; Indicative Energy Consumption**

I. Introduction

The European Green Deal, enacted to achieve a 'climate-neutral bloc' by 2050 [1], and the recent International Telecommunication Union's global campaign to reduce ICT's carbon footprint by 45 per cent by 2030 [2], indicate an imperative need for a paradigm shift in digital transformation and energy use reconnaissance. Blockchain, which has arguably become one of the most disruptive technological solutions popularised by its use in Bitcoin cryptocurrency, is a major contributor to global carbon footprint due to its propensity for high energy consumption. Cambridge Bitcoin Electricity Consumption Index [3] estimated the Bitcoin network's annual energy at 124.60TWh, which is over 50 per cent of the current estimated global data centre electricity [4]. Also, [5] estimated Bitcoin's annual carbon footprint at 50.55 Mt CO2, an equivalent of the carbon footprint of a small country such as Hungary. Bitcoin, a peer-to-peer electronic currency developed for digital transactions without an intermediary by a decentralised database called 'a chain of blocks' [6], has gained tremendous popularity for a multitude reasons. The underpinning technology of Bitcoin, Blockchain, whose success is chiefly accrued to its intrinsic value of providing immutable, secure and authenticated transactions, has since been replicated and diversified for various use cases. The diversification was pioneered by the introduction of Ethereum, a smart contract and decentralised application platform that executes scripts and runs decentralised applications for various use cases [7]. Beyond cryptocurrencies, Blockchain solutions have been explored for many other use cases, including energy trading, Internet of Things, supply chain management and others [8] [9]. However, the infamy of Blockchain lies mainly in its high energy consumption as a result of the proof-of-work (PoW) consensus mechanism it mostly employs. The consensus mechanism is an integral facet of the Blockchain for achieving trust among nodes [10]. Although other consensus mechanisms have since been introduced to either mitigate the shortfalls of PoW or better suit some Blockchain use cases, these consensus mechanisms are both with benefits and shortfalls which invariably affect the Blockchain's efficacy and sustainability [11]. Bearing in mind the overall impact of ICT on the environment [12], it is expedient to present a lean Blockchain adoption as a deliberate effort towards the reduction of ICT's carbon footprint. Consequently, there is a need to debunk the widespread supposition of Blockchain applicability for every use case; this fundamental understanding will alleviate unnecessary wastage of resources by preventing stakeholders from venturing into ill-fated Blockchain projects. Also, because meeting the requirement of a use case and reducing the environmental impact is often a two conflicting objectives, there is a need for a framework that will help developers and stakeholders identify, fine-tune and evaluate this trade-off. Over the years, there has been an increased need for sustainable IT due to global digital transformation resulting in exponential increase of energy consumption thereby impacting carbon footprint [12]. Therefore, Green IT, or green computing - the practice or concept of using computing resources in an environmentally sustainable way while retaining or improving overall efficiency [13] - has since been introduced and adopted. To this end, Blockchain as an IT solution should also move in the same direction.

The subsequent section is as follows: Section 2 highlights related work. Section 3 gives an overview of different consensus mechanisms with a focus on their energy expenditure. Section 4 presents a decision support framework based on the specification of green Blockchain as a viable concept for

environmental sustainability. Section 5 concludes this work and gives a road map to future work.

II. Related Work

Several papers have been published over the years to either introduce, analyse or propose improvements on different consensus mechanisms for Blockchain, majority of which are PoW (and its variants) focused. Few other papers have also taken a step further to do comparative analysis of popular consensus algorithms, with emphasis on legitimate Blockchain issues such as scalability, incentivisation, security risks, etc. For instance, [14] in their work highlighted the security, scalability and power consumption of six consensus algorithms albeit vaguely (due to the limited amount of data publicly available). Due to unavailability of sufficient data, their paper presented energy consumption data of only two cryptocurrencies (Bitcoin and Ethereum) which until now use the same consensus mechanism (PoW). In more recent works, [15] and [16] show a comprehensive consensus mechanisms comparisons covering both those that are actively deployed for cryptocurrencies and those that are merely a proof of concept. The analysis detailed scalability, finality (indicates whether a transaction is reversible), accessibility and adversary tolerance of reviewed consensus mechanisms. Also, their work does not give a detailed energy expenditure of reviewed consensus mechanisms, however, they highlighted energy consumption as a major criteria that affect Blockchain consensus evaluation and provided a dichotomous (Yes/No/Fair) energy efficiency assessment. Emphasis have been laid in a few papers over the years about the importance of creating a Blockchain framework to support decision making for stakeholders [17], [18] [19]. However, none seems to be climate and environmentally focused.

III. Overview of Consensus Mechanisms

Consensus mechanisms may considerably affect the performance and energy consumption of a Blockchain network. As Blockchain is a decentralised ledger that does not need a central authority to manage it, a consensus mechanism is used to determine the validity of a new transaction before adding a new block to the chain. The adopted mechanism determines crucial elements such as data consistency, consensus finality, speed, network scalability and sturdiness to arbitrarily-behaving (i.e., Byzantine) nodes [20]. The consensus mechanism assumes that most nodes are honest to run and maintain the system. Generally, the approval of more than 50 per cent of the network members is needed to write data in blocks; however, data can be compromised if dishonest nodes control a more significant percentage or possess a more substantial computing power [21]. Furthermore, consensus mechanisms offer rewards for users to engage in a network, such as the proof of work consensus used in Bitcoin, where miners (network nodes) earn a reward (coins) for processing transactions and generating blocks [22].

A. Consensus Mechanisms

Proof of Work (PoW) PoW, introduced in [6], was developed to alleviate double-spending in the network. A proof of work demands that nodes that verify transactions (known as miners) must perform a complex computation to assert the validity of entities in the network. In Bitcoin, mining nodes compete to validate transactions by solving a cryptographic challenge to build a valid block. When a solution is found, the winning node proposes a new block of transactions to be added to the chain [23]. PoW is done on the premise that the network can remain consistent only if the cumulative computing power of honest nodes is greater than the attacker's computing power. [24]. However, PoW mechanism consumes enormous amount of energy, e.g., Bitcoin's PoW mechanism estimated energy consumption is 1129.89 kWh per transaction which is the equivalent of the power consumption of an average U.S household over 38.73 days [5]. However, the computationally intensive mining and competition leading to high energy and resource consumption are the same reasons that render PoW secure.

Proof of Stake (PoS) PoS was introduced as an alternative to PoW to reduce energy consumption. The voting weight is related to the assets (owned units of the cryptocurrency, which are finite and visible, and thus verifiable within the Blockchain network) rather than the resource computing power [25]. In proof of stake, transaction validators are chosen semi-randomly through a two-part process. Every validator must 'invest' currencies (a piece of stake) in the network. This amount is locked in the system to be used as a guarantee for the new block. The chances of a validator being selected depend on the number of currencies invested. If this amount is significant, they have more chances to be chosen [26]. When a validator is selected, the validator must check all the transactions of the block and validate them to ascertain they are not fraudulent. When this process ends, the validator adds the block to the Blockchain. The rewards of this node for validating the block is the fees that are associated with each transaction. PoS does not consume as much energy as PoW because of the absence of miners who compete to solve mathematical puzzles [24]. However, unlike PoW, the cost of an attack on PoS is lower, i.e., PoS run the risk of an attack because it will only take a certain amount of coin (stake) for an attacker to dominate the network and introduce a fake block to the chain. Presently, the Ethereum Blockchain, which initially adopted a variant of PoW, is planning to convert to PoS [27].

Delegated Proof of Stake(DPoS) DPoS works similarly to PoS, giving priority to the nodes with more stake on the network. However, the significant difference between PoS and DPoS is that while validators in PoS are randomly chosen based on their stake, validators in DPoS are elected by other nodes on the network to validate and append new blocks (Bamakan et al. 2020). The limitation on the number of validators makes the network more centralised. This mechanism further reduces the computing resources expended by PoS. Also, the smaller number of nodes in the consensus process reduces the

transaction time of generating blocks to 3s rather than 64s in PoS. In this vote-based PoS mechanism, elected nodes are the core (nodes) of the entire system [28]. In contrast to PoW and PoS, DPoS is more energy efficient. However, because of the logical disparity between DPoS and PoS, it is impossible to compare the efficiency of the two systems in a substantive way. The consensus process fails to prevent unethical block node from being elected, and holding the right to generate blocks over a long period can lead to security risk. Nevertheless, the rest of the network nodes can vote out dishonest nodes and elect new representatives [28]. The only major energy demand of DPoS comes from a few elected block validators. EOS, which is currently the most popular Blockchain to adopt DPoS, give the estimation of the energy consumption to be 1.8kW per block and annual energy of 0.0012TWh [29].

Proof of Luck (PoL) PoL was proposed to leverage trusted execution environments (TEEs) to build a consensus mechanism that randomises validators' selection. According to [30], this mechanism aims to achieve a low-latency transaction validation while using minimal energy and computing power. Each block is assigned a 'luck' value within the system, which is a random number between zero and one. That is, higher numbers are luckier while lower numbers are unlucky. It is assumed that validators who verify transaction in the network will prefer appending their blocks to the chain with the highest luck value calculated by adding up the corresponding luck values in each block. Also, a delay is imposed before the corresponding mining is completed on the mined block's random block value. The delay optimises the communication within the network so that the miner that first solves the puzzle with higher luck will broadcast to the network. This proposition's limitation is that it is still a proof of concept that has not been deployed to test factors such as energy expenditure and transaction speed against other consensus mechanisms [14].

Proof of Elapsed-Time (PoET) Proof of Elapsed Time is a consensus mechanism introduced for private (permissioned) Blockchain networks. PoET was developed by Intel in tandem with their Software Guard Extension (SGX)3 technologies and deployed in the open-source Hyperledger Sawtooth Blockchain platform. PoET is a form of PoW consensus that attempts to eliminate the inefficient energy consumption of PoW by removing the need for the mining process; instead, it implements a randomised timer system that assigns a random waiting period to each node inside the network [31]. The node with the shorter waiting period becomes the miner. When the miner with the shorter waiting time generates the block, the other nodes must verify it before the system accepts it. For a new block to be created, it is necessary to verify two requirements. First is to ensure the randomisation of the waiting period assignment. The second one is the genuineness of the waiting period timeout [32]. PoET is a potential option for business use cases where transfers are not all financial. Also, unlike other protocols such as Bitcoin, PoET is extremely parameterisable. Finally, one of PoET's main advantages is that it consumes significantly less energy over consensus mechanism like PoW [31].

Proof of Activity (PoAc) Proof of Activity is a combination of PoW and PoS consensus mechanisms [33]. The protocol starts as PoW, whereby the network miners try to find a solution to challenging mathematical puzzles to win the new block's generation and validation. However, the new block does not contain transactions. The new block that the miner generates has only the block header, which includes the hash value of the previous block, the miner public address, the block's index in the b and the nonce. When this process ends, the miner broadcasts the new empty block to the network. At this point, the PoW finishes its job, and PoS takes over [34]. A selected group of nodes (validators) is necessary to sign the new block. All the chosen stakeholders check if the block header is valid, and if it is, they sign the block with their private key and broadcast the signature to the whole network. The last stakeholder receives the block, checks its validity, signs it, and creates a wrapped block, which extends the empty block header, that includes the transactions that they wish to include, the other stakeholders' signatures and their own. Then they broadcast the extended block to the network, where nodes check its validity regarding the process as mentioned above and consider it a valid block. The rewards from the transactions' verification are shared between the miners and the stakeholders [34]. Due to the adoption of PoS to complement the PoW mechanism, the energy consumption is lower than pure PoW mechanism. A well-known cryptocurrency that uses the PoAc consensus process is Decred [35].

Proof of Capacity (PoC) Proof of capacity is a consensus mechanism whereby miners plot their hard drives to take part in the mining process. Participants vote on new blocks based on their ability to assign a non-trivial volume of disc space [36]. In this algorithm, miners calculate mathematical puzzles' solutions and store them on their hard drives before the start of the mining process. The miners who solved these puzzles faster then work on the consensus process. A miner has more chances to be selected if they have the most solutions (plots) stored. The process starts with a miner creating a unique plot file. The first stage of the process is called plotting, and it uses a hashing function called Shabal. At this stage, the miner calculates the solution of Shabal and stores it in his/her hard drive. The next step is the generation of a nonce, which comes from the plot file. During the mining process, the miner will use the scoop number and the corresponding nonce to calculate the 'deadline', a time unit. They will do the same for all the nonce and will pick the minimum deadline. This deadline is the time that will pass since the last block was created until the miner is able to generate a new one. The miner with the shorter deadline is the one who can generate the new block and receive the rewards. SpaceMint is built on a non-interactive version of PoC (called proof-of-space) using the same basic model as PoW, whereby it inherits Bitcoin's incentivisation process as well as its resistance to censorship and denial-of-service attacks [37]. However, Burstcoin is the first adopter of PoC and pegs the energy consumption at 0.00024kw [38].

Byzantine Fault Tolerance (BFT) Byzantine Fault Tol-

erance refers to a distributed network's ability to behave properly, so that it finds consensus accurately and reliably even though bad actors propagate erroneous information or forget to transmit information at all. The goal is to reduce the power of malicious nodes so that the system does not crash and the honest nodes can reach a right consensus [39]. The three major approaches to this issue used in Blockchain are Practical Byzantine Fault Tolerance (PBFT), Federated Byzantine Agreement (FBA), and Delegated Byzantine Fault Tolerance (DBFT). The Ripple protocol presents a low-latency consensus algorithm that maintains robustness in the face of these Byzantine failures. The Ripple Protocol Consensus Algorithm (RPCA) is used by all nodes every few seconds to ensure the network's correctness and agreement. After a consensus is reached, the new ledger is considered "closed", and it becomes the last-closed ledger. The last-closed ledger held by all nodes in the network would be equal if the consensus algorithm is efficient and there is no fork in the network. In the time it takes for one round of consensus to end, the Ripple Protocol will process stable and accurate transactions in a matter of seconds. These transactions are provably stable up to the defined bounds, which, although not the best in the literature for Asynchronous Byzantine consensus, enable for rapid convergence and network participation versatility [40]. The energy consumption of in BFT is significantly lower than PoW because it does not entail any computational puzzle.

Practical Byzantine fault-tolerance (PBFT) Practical Byzantine Fault Tolerance (PBFT) by (Castro and Liskov 2002) is a protocol that implements consensus in a byzantine and partially synchronous environment. The protocol is organised into a series of views, each of which is orchestrated by a leader. The leader of each view orders messages and sends them to the replicas in a three-step broadcast. Replicas keep a watch on the leader for protection and aliveness, and can suggest a change of view if the leader is inaccessible or malicious. Inside the asynchronous network setting, security is assured; however, since replicas depend on timeouts to identify a defective leader, liveness is only guaranteed in a partially synchronous environment. Nonetheless, the algorithm is regarded as efficient, so far; the number of malicious nodes in the network is less than or equal to one-third of the total number of nodes in the network [41]. PBFT has a lot of benefits, but it also has a lot of drawbacks. To begin with, it operates in a fully enclosed setting, in which nodes attempting to participate or exit must bring the whole system to a halt. Secondly, though PBFT ensures aliveness and security, it takes no steps to deal with inactive or malicious replicas, which is dangerous to the system and will eventually result in a system crash. Thirdly, PBFT has no specified standard for determining when replicas are sufficiently operational, resulting in network participant's reliance on others and avoid work [42]. However, PBFT does not rely on hashing techniques like PoW, rather, it is based on trust between the network nodes, therefore it is very energy-efficient. Also, because it is centralised like DBFT, the energy consumption is estimated to be within the same range. The Hyperledger Sawtooth Blockchain supports PBFT as well as PoET [43].

Federated Byzantine Agreement (FBA) Federated Byzantine Agreement is a consensus model that employs quorum slices and quorums. Quorum slices are groups of nodes that work together to achieve a consensus. Quorums are the agreements that cannot change in the future and are the subsets of quorums slices that help nodes with the agreement process. Stellar Consensus Protocol (SCP) is an evolution of Federated Byzantine Agreement [44]. FBA employs a method that eliminates the need for a central validator list whereby each validator has a Quorum Slice, which is a group of peer validator nodes that they trust. Such quorum slices can converge in a network of validators, resulting in a Quorum where consensus can be achieved by related confidence. Rounds of voting are used to find a majority. Transactions that do not meet a certain amount are eliminated in these stages, and a new round for the remaining transactions begins. FBA requires nodes to freely access the network as validators, but in order to contribute as validating nodes in the network, peer nodes must select the nodes that it trusts in their quorum slice, inferring that although a decentralised structure is required to be secure, it is highly centralised, hence, Vulnerable to a single point of failure. However, it is energy efficient and scalable [45].

Delegated Byzantine Fault Tolerance (DBFT) Delegated BFT is a consensus protocol deployed by NEO (neo-project 2021). In this protocol, NEO token holders (citizens) have the right to vote for the bookkeeping nodes (delegates), regardless of the amount of currency in their possession. GAS is the network utility token distributed passively to NEO holders to pay for transactions. Any node can become a delegate so far set requirements are met. Requirements include, a solid internet connection, 1,000 GAS and the appropriate equipment. Citizens then vote delegates. One of these delegates will be elected randomly to be the speaker. The speaker creates a new block out of the transactions that are awaiting validation. The speaker then takes the request to the delegates who will be responsible for keeping track of all transactions and logging them on the network. Delegates will listen to the citizens' demands, which are the transactions that exist in the network, they will track them in the network and add them in the ledger [14]. Although DBFT's processes is energy efficient, it is not fully decentralised. Also, delegates need to work under genuine identities to be selected, therefore, there's no privacy on the Blockchain [46] [47].

Proof of Authority (PoA) PoA is a mechanism introduced for permissioned (private) Blockchain to facilitate validators' accountability while providing data privacy and security controls lacking in PoW [48]. Here validator's identity rather than their asset is at stake (identities are known and pre-authorised), bringing about both loss of reputation and consequently expulsion from validator set in the event of misbehaviour [49]. Because permission Blockchain operates in a more trusted environment, it relies on message-based consensus schema rather than hashing procedures [50]. Therefore, it employs Byzantine Fault-Tolerant (BFT) algorithms such as the Practical Byzantine Fault-Tolerant (PBFT) [51] to ensure sufficient fault

tolerance. PoA operates differently from PBFT; it requires fewer message exchanges, thus providing better performance and toleration to faults [17]. The algorithm uses a group of nodes referred to as authorities, out of which a leader is elected to be in charge of proposing new blocks. The selection relies on mining rotation schema. Each authority is assigned with a unique ID and has access to a consensus software, which handles clients' transactions in the network. The two implementations of this algorithm are Aura and Clique. Although they work differently, the process of proposing a new block by the leader is the same [48]. The potentials of PoA as a solution for solving Byzantine consensus problem [52], has made it appealing to industries with critical security requirements. However, PoA is suitable for private Blockchain application whereby validator's identities are visible to participants and can potentially cause third-party manipulation. However, PoA is energy efficient with fast transaction time, high throughput and scalability [17] [53].

Proof of Importance (PoI) PoI is a consensus mechanism that NEM cryptocurrency [54]launched that is used to determine the nodes that are eligible to add a block to the Blockchain, a process called 'harvesting'. Nodes will receive transaction fees within a block in return for harvesting it. Accounts with a higher value score are more likely to be selected to harvest a block. To be considered for harvesting, an account must have at least 10,000 vested XEM, according to the NEM protocol [55]. Unlike similar consensus mechanisms such as proof of stake, PoI considers participant's (nodes) overall support of the Blockchain network. For instance, it can be argued that the PoS mechanism promotes coin hoarding since the validators mine the percentage of transactions proportional to their stake, encouraging nodes to save their coins instead of spending them. PoI, on the other hand, reflects on the network's total support by taking three aspects into account: vesting (the more vested coins, the higher the PoI score), transaction associates (rewards users who make transactions with other NEM accounts on the network), and the amount and scale of transactions in a given number of days (transactions above a certain set-size lead to the account's PoI score) [55] [56]. PoI is scalable and assets (stake) are less likely to be hoarded to the point of threatening the efficiency of the network [54]. However, it is vulnerable to Sybil attacks and nothing-at-stake crisis may also take place [55].

Proof of Burn (PoB) Proof-of-burn was first suggested by Iain Stewart in 2012, it is a method for the irreversible and provable destruction of cryptocurrencies. They work similarly to PoW, however, with lesser energy consumption. The main idea is that miners should "burn" some of their coins to generate a new block. This way, nodes obtain mining rights in the system. The process starts when a miner sends some coins to a verified address, referred to as 'eater address'. This act does not consume a lot of energy, only the coins that miner has sent to the eater address and ensures that the network is active. The coins that miner sent to the eater address cannot be spent. The transactions between miners and eater address can verify that coins are no longer available to be spent. When these transactions are verified, miners can receive their rewards [57]. In 2014, Slimcoin deployed this mechanism but it has since been discontinued [58]. Also, the Counterparty project adopts this mechanism [59]. For the bootstrapping of the Counterparty cryptocurrency, users burned more than 2,130.87 BTC [**?**]. There is no need to invest in powerful hardware to adopt PoB, and it promotes a long-term commitment and time horizon for a project. However, it is challenging to create and apply network effects before the Blockchain's full maturity and there is no guarantee that a user will ever recover the full value of the coin being burned [59].

Proof of Believability (PoBLV) Proof of believability is a consensus mechanism deployed by IOSToken (IOST). Here, the validators are chosen based on their previous contributions and behaviour [60]. The consensus algorithm allows high transaction throughput while ensuring nodes remain compatible, based on factors such as IOST token balance, reputation-based token balance, network inputs, and user behaviours. Proof of Believability uses an intra-shard Believability-First approach. The validators are elected based on their believability score which depends on multiple factors, like token balance, contributions to the community, reviews etc. The highest believability score has more chances of being selected into the believability league. Then, the protocol divides the nodes into groups, the believable leagues and the normal. Believable validators process transactions fast during the first phase of the protocol. Then, normal leagues verify these transactions in the second phase, providing finality and verifiability. Furthermore, believable validators are divided into smaller groups, one validator per group, where the transactions are distributed randomly to be verified. Therefore, the latency of the protocol is lower than in other protocols [61]. However, the division of validators into groups of one may cause security problems as this validator may act maliciously. For this security issue to be avoided, normal validators will sample transactions and detect discrepancies. In the case that a believable validator is detected as fraudulent, it will lose all the tokens and standing. The duped users will receive compensations for any loss [62]. PoBLV is energy efficient, scalable with fast transaction time and finality. However, there is probability of error in the network architecture and probable security issues based on single node verifier [62] [29].

Proof of Devotion (PoD) Proof of Devotion selects the validators regarding the influence that they have over the network. PoD is similar to Proof of Importance, in that both use a rating system to decide who is qualified to validate and propose blocks based on a set of parameters. In PoD, an validator's eligibility is determined by its level of control, which is dependent on liquidity and dissemination. PoD is deployed by Nebulas cryptocurrency network [63], and allows the participants to generate blocks and become bookkeepers based on their influence. The process starts with participants paying a deposit to take part in the bookkeeper's selection process. This process includes virtual mining, where all the candidates try to earn their bookkeeping rights. Bookkeepers supervise the block generation process. At the end, they

gain the rewards and the transactions fees. If a bookkeeper misbehaves, they lose their deposit, which is divided and shared to the other bookkeepers [16].

Proof of Reputation (PoR) POR is a more advanced, efficient, and secure version of Proof of Authority (POA). In PoA, validators who are typically known entities are authorised to verify transactions. However, PoR relies on the reputation of participants to keep the network stable. A participant must have a high enough credibility such that attempting to be dishonest will result in significant financial and brand implications. Companies, not persons, are used as validators in POR. A dishonest participant would have a lot more to lose than only one individual as in the case of PoA. Here, they'd be losing not just their own credibility, but also the company's entire market cap and the reputations of the officers and shareholders [64] [16]. PoR is currently adopted by gochain [65]. The energy consumption is lower than PoW and it has a fast transaction time. [16].

Proof of Weight (PoWe) Proof of weight is a variation of Proof of Stake that Algorand deployed. With PoS, each participant's probability of finding the next block is determined by the number of tokens they have. However with proof of weight, weight values are assigned to participants based on the asset that each person has in their account. In typical PoS implementations, a malicious leader (who assembles a new block) will cause a fork in the network, resulting in the leader losing his money if they are detected (since two copies of the new block are signed with his key). The weights in Algorand, on the other hand, are only there to ensure that the perpetrator cannot use pseudonyms to increase their strength. As long as at least two-thirds of the total weighted fraction of participants are honest, malicious processes makes negligible effect on the network and there remains a strong resistant to double-spending attacks honest [66]. Despite the importance of evidence of weight agreement, it is challenging to motivate users of this method [16]. However, the mechanism achieves scalability by assigning each step of its protocol to a committee – a small group of members drawn at random from the total number of users. The protocol messages are observed by all other users, allowing them to learn the agreed-upon block. Agents of the committee are selected at random from all users based on their weights. As a result, it ensures that a proper percentage of committee members are. Like PoS, PoWe is energy efficient compared to PoW because and highly scalable, however, it is difficult to incentivise [66] [16].

IV. Decision Support Framework

A. Specification of a green Blockchain

Consequent to the negative impact of energy on the environment particularly in IT sphere that brought about the indoctrination of green IT as a deliberate effort for sustainability, Blockchain as an IT solution should be green. A green Blockchain in this sense denotes an environmentally sustainable Blockchain that contributes to the mitigation of global warming and the depletion of the environment. Since it has been established that inculcating greenness as a digital prerogative is a viable way of contributing to the reduction of harmful emissions into the environment [67] [68] [69], a green Blockchain should be deemed of topmost importance and ethical responsibility of stakeholders when adopting Blockchain solution especially with the existing global campaign of reducing ICT's carbon footprint by 45 per cent by 2030 [2].

To deploy a green Blockchain, the following factors ought to be considered: 1) do I need Blockchain? 2) if yes, what is the best environmentally sustainable Blockchain solution for my project? Having a clear-cut understanding of Blockchain to answer these questions will enable stakeholders choose the appropriate and sustainable solutions for their use cases and will debar them from embarking on a doomed Blockchain project, adding to the long list of failed projects as seen in [70], and wasting computing resources.

Wüst and Gervais [71], gave a road map for evaluating the suitability of a Blockchain project providing a methodology for determining the most appropriate technical approach for a project depending on the application scenario. In their procedure (flowchart), they highlighted the required trust assumptions, implementation criteria, interested parties, and technological characteristics such as throughput and latency, result of which culminates to highlighting the type of Blockchain suitable for a scenario or the incompetence of Blockchain implementation in such scenarios. For instance, they stated that, multiple writers and trust (or lack of trust) are essential determining factors for choosing the appropriate solution between Blockchain and centralised databases. That is, for a Blockchain to be an appropriate solution for a use case, there must be more than one entity that generates the transactions, and there must be some level of distrust between such entities, since Blockchain is a technology for databases with many non-trusting writers. Else, centralised database may be a more suitable option [71].

Using their in-depth framework as a benchmark, we further deep-dive and highlight the critical need for clean energy in the Blockchain ecosystem.

B. Framework

The ensuing decision support framework for consensus selection is comprised of two distinct parts. Figure 1 is the primary layer, showing the expanded Wüst and Gervais [71] decision tree. Figure 2 introduces the Indicative Energy Consumption (IECon) chart showing the link between consensus and their estimated energy consumption based on existing projects. The chart also gives examples of existing projects that adopted the highlighted consensus mechanisms.

The IECon chart aims to act as a guide for stakeholders and key decision makers to critically review their projects, its position on the IECon band, and act as a call to action to intentionally promote greenness in their Blockchain projects.

C. Evaluation

This section highlights the evaluated real world use cases of selected consensus mechanisms from the highest estimated energy consumption consensus (PoW) to the least (PoA).

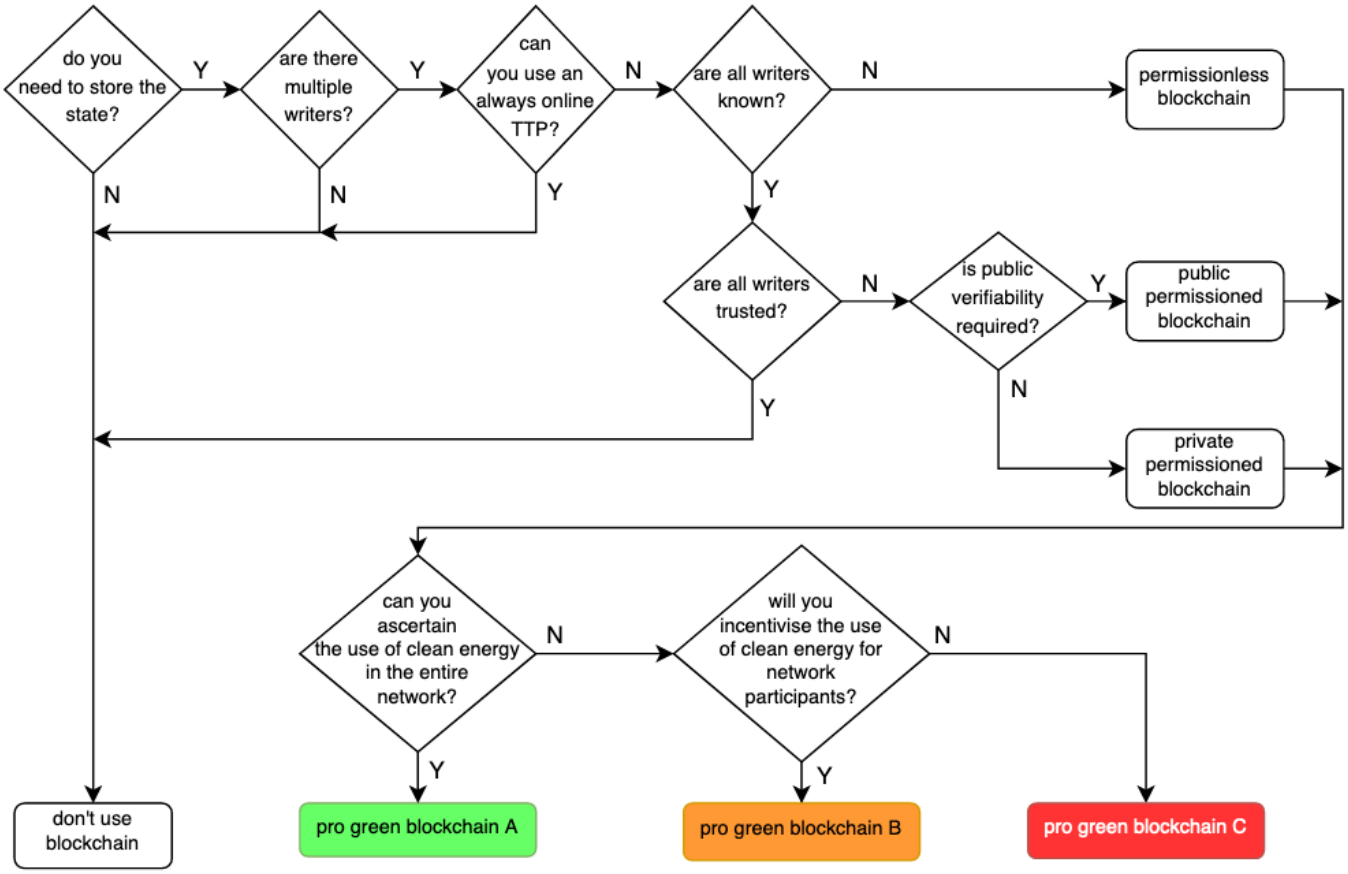

Fig. 1. The proposed framework (adapted from [71])

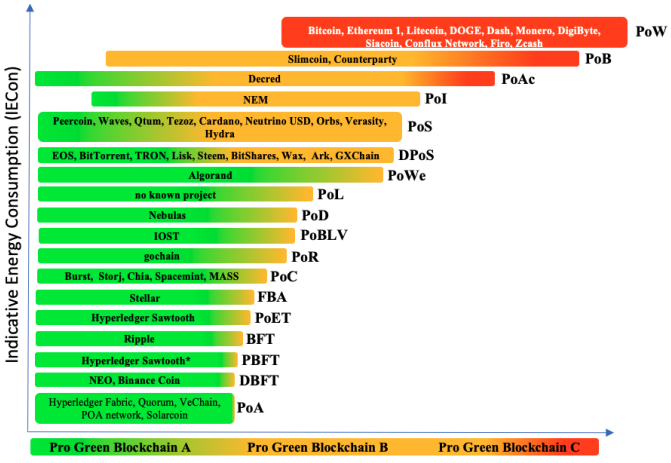

Fig. 2. IECon Chart

Use Case 1: BITCOIN (Proof-of-Work) Bitcoin was created solely as an electronic cash system that would allow anonymous transfers directly from one party to another without the need of a bank [6]. Presently, it has a market dominance of 39.30% [72]. Despite its success, the proof-of-work algorithm it uses for validating transactions consumes vast amount of energy which according to [5], is primarily sourced from fossil fuels, thus, raising awareness on the unsustainability of Bitcoin's PoW algorithm.

Having established the huge energy consumption of the proof-of-work algorithm which ranks as the highest energy consuming consensus on the IECon chart, the use of a more sustainable energy source will reduce its massive negative impact on the environment. Although this might be challenging due to the decentralised public (permissionless) element of Bitcoin, we hope that through adequate governance, miners supporting the Bitcoin network will move to a clean energy source in the near future.

Use Case 2: STELLAR (Federated Byzantine Agreement) Through the Stellar network, you can exchange any currency, be it traditional currency (fiat) or cryptocurrency. The network's token (Lumens) is used to facilitate trades on the Blockchain based ledger at a fraction of a cent and with great efficiency. The network allows individuals and institutions to create various tokens for use on the network, which has inspired some to use the network for sustainability initiatives such as investing in renewable energy [73]. The Stellar network Consensus Protocol (SCP) depends on authentication of transactions occurring via a set of trustworthy nodes instead of running through the whole network. Therefore authentication

cycle is shorter and much faster, keeping costs low and energy use to a minimum.

FBA ranks much lower on our IECon chart given that it is does not require the energy intensive 'work' of PoW for transaction authentication and because it employs a more centralised Blockchain structure, i.e., federated voting for authentication thereby promoting governance for adequate energy use.

Use Case 3: HYPERLEDGER FABRIC (Proof-of-Authority) Hyperledger Fabric is an enterprise grade Blockchain system used in creating and operating distributed ledger applications and networks by enterprises. With the Proof-of-Authority (PoA) algorithm, entities earn the right to become validators, so retaining the position that they have gained is incentivised. Through attaching a reputation to their identity, validators are incentivised to uphold transaction process, as they do not wish to have their identities attached to a negative reputation [74].

As shown on our IECon chart, the PoA algorithm is ranked to be more energy efficient in comparison to the previously discussed alternatives i.e. Proof-of-Work (PoW) and Federated Byzantine Agreement (FBA) due to its usage of minimal to non-existent computational power and also its incentivised capabilities that can be of advantage for clean energy use among participanting nodes.

V. Conclusions & Future Work

In this work, we presented a framework that will aid the decision of stakeholders in choosing the right consensus mechanism for their Blockchain project based on their energy consumption. To achieve this, a review of the areas of green IT and Blockchain was done. This led to the concept of green Blockchain as a crucial denominator for reducing global carbon footprint. We also critically reviewed 18 consensus mechanisms, highlighting their pros and cons with samples of live projects. Following, a decision supporting framework was developed by expanding the work of Wüst and Gervais, for the first phase of energy evaluation of intended projects. This was followed by developing an indicative energy consumption (IECon) chart of all reviewed consensus mechanisms, showing expected energy expenditure. Finally, we did an evaluation of three live use cases showing how their consensus mechanisms ranks on our IECon chart.

It is noteworthy that at the time of writing that there are no empirical data and published details on the energy consumption of many of the consensus mechanisms. As such the energy estimations of the reviewed consensus mechanisms are mainly based on theoretical study of the actual mechanisms and their underlying computational overheads. As a result, the Indicative Energy Consumption (IECon) chart is expected to be revised as more empirical data are produced. Future work activity will entail additional data gathering of other consensus mechanisms to expand and update the IECon chart, which will help lay down a concise pathway for wider industry adoption of green (sustainable) Blockchain.

Acknowledgment

This work has been partially supported by IDEAL-CITIES; a European Union's Horizon 2020 research and innovation staff exchange programme (RISE) under the Marie Skłodowska-Curie grant agreement No 778229.

References

[1] European-Commission. (2021) A european green deal. [Online]. Available: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en

[2] ITU. (2021) Press release. [Online]. Available: https://www.itu.int:443/en/mediacentre/Pages/PR04/2020-ICT/industry/to/reducegreenhouse/gas/emissions/by/45/percent/by/2030.aspx

[3] M. Rauchs, A. Blandin, and A. Dek, "Cambridge bitcoin electricity consumption index (cbeci)," 2020.

[4] G. Kamiya. (2020) Data centres and data transmission networks on track tracking report. [Online]. Available: https://www.iea.org/reports/data-centres-and-data-transmission-networks

[5] Digiconomist. (2021) Bitcoin energy consumption index. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption/

[6] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, 2008.

[7] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, 2014.

[8] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 5, no. 9, pp. 1–10, 2016.

[9] N. Alexopoulos, J. Daubert, M. Mühlhäuser, and S. M. Habib, "Beyond the hype: On using blockchains in trust management for authentication," in *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 2017, pp. 546–553.

[10] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information processing systems*, vol. 14, no. 1, pp. 101–128, 2018.

[11] G. Pîrlea and I. Sergey, "Mechanising blockchain consensus," in *Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs*, 2018, pp. 78–90.

[12] S. Murugesan, "Harnessing green it: Principles and practices," *IT professional*, vol. 10, no. 1, pp. 24–33, 2008.

[13] D. Wang, "Meeting green computing challenges," in *2008 10th Electronics Packaging Technology Conference*. IEEE, 2008, pp. 121–126.

[14] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 2018, pp. 1545–1550.

[15] S. M. H. Bamakan, A. Motavali, and A. B. Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Systems with Applications*, p. 113385, 2020.

[16] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43 620–43 652, 2021.

[17] T. T. A. Dinh, J. Wang, G. Chen, R. Liu, B. C. Ooi, and K.-L. Tan, "Blockbench: A framework for analyzing private blockchains," in *Proceedings of the 2017 ACM International Conference on Management of Data*, 2017, pp. 1085–1100.

[18] V. Chia, P. Hartel, Q. Hum, S. Ma, G. Piliouras, D. Reijsbergen, M. Van Staalduinen, and P. Szalachowski, "Rethinking blockchain security: Position paper," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1273–1280.

[19] S. Leonardos, D. Reijsbergen, and G. Piliouras, "Presto: A systematic framework for blockchain consensus protocols," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1028–1044, 2020.

[20] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22 328–22 370, 2019.

[21] F. Dai, Y. Shi, N. Meng, L. Wei, and Z. Ye, "From bitcoin to cybersecurity: A comparative study of blockchain application and security issues," in *2017 4th International Conference on Systems and Informatics (ICSAI)*. IEEE, 2017, pp. 975–979.

[22] K. Zīle and R. Strazdiņa, "Blockchain use cases and their feasibility," *Applied Computer Systems*, vol. 23, no. 1, pp. 12–20, 2018.

[23] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *arXiv preprint arXiv:2005.14282*, 2020.

[24] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*. IEEE, 2018, pp. 54–63.

[25] J. Sedlmeir, H. U. Buhl, G. Fridgen, and R. Keller, "Recent developments in blockchain technology and their impact on energy consumption," *arXiv preprint arXiv:2102.07886*, 2021.

[26] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[27] Ethereum-Org. (2016) Proof-of-stake (pos). [Online]. Available: https://ethereum.org

[28] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, "Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism," *IEEE Access*, vol. 7, pp. 118 541–118 555, 2019.

[29] E. Pagliari. (2019) Proof of believability: the consensus algorithm of iost. the cryptonomist. [Online]. Available: https://en.cryptonomist.ch/2019/08/11/proof-of-believability-iost/

[30] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *proceedings of the 1st Workshop on System Software for Trusted Execution*, 2016, pp. 1–6.

[31] A. Corso, "Performance analysis of proof-of-elapsed-time (poet) consensus in the sawtooth blockchain framework," 2019.

[32] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On security analysis of proof-of-elapsed-time (poet)," in *International Symposium on Stabilization, Safety, and Security of Distributed Systems*. Springer, 2017, pp. 282–297.

[33] S. Seth. (2021) Proof of activity. [Online]. Available: https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp

[34] I. Mizrahi and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *IACR Cryptology ePrint Archive*, 2014.

[35] Decred. (2021) Secure. adaptable. sustainable. [Online]. Available: https://decred.org/

[36] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis, "Consensus in the age of blockchains," *arXiv preprint arXiv:1711.03936*, 2017.

[37] S. Park, A. Kwon, G. Fuchsbauer, P. Gaži, J. Alwen, and K. Pietrzak, "Spacemint: A cryptocurrency based on proofs of space," in *International Conference on Financial Cryptography and Data Security*. Springer, 2018, pp. 480–499.

[38] Burstflash. (2021) The pioneer of proof-of-capacity — an eco-friendly blockchain. [Online]. Available: https://www.burst-coin.org/

[39] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," in *Concurrency: the Works of Leslie Lamport*, 2019, pp. 203–226.

[40] B. Chase and E. MacBrough, "Analysis of the xrp ledger consensus protocol," *arXiv preprint arXiv:1802.07242*, 2018.

[41] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "Sok: Sharding on blockchain," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 2019, pp. 41–61.

[42] X. Hao, L. Yu, L. Zhiqiang, L. Zhen, and G. Dawu, "Dynamic practical byzantine fault tolerance," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–8.

[43] J. Frankenfield. (2021) Hyperledger sawtooth definition. [Online]. Available: https://www.investopedia.com/terms/h/hyperledger-sawtooth.asp

[44] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Development Foundation*, vol. 32, 2015.

[45] M. Kim, Y. Kwon, and Y. Kim, "Is stellar as secure as you think?" in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 377–385.

[46] C. Comben, "Delegated byzantine fault tolerance (dbft) explained," 2019.

[47] Neo-project. (2021) Neo documentation. [Online]. Available: https://docs.neo.org/docs/enus/index.html

[48] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain," 2018.

[49] A. H. Lone and R. Naaz, "Reputation driven dynamic access control framework for iot atop poa ethereum blockchain," Cryptology ePrint Archive, Report 2020/566, 2020, https://eprint.iacr.org/2020/566.

[50] L. Tseng, "Recent results on fault-tolerant consensus in message-passing networks," in *International Colloquium on Structural Information and Communication Complexity*. Springer, 2016, pp. 92–108.

[51] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[52] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *Journal of the ACM (JACM)*, vol. 27, no. 2, pp. 228–234, 1980.

[53] Binance-Academy. (2021) Proof of authority explained. [Online]. Available: https://academy.binance.com/en/articles/proof-of-authority-explained

[54] T. NEM, "Nem technical reference," *URL https://nem.io/wpcontent/themes/nem/files/NEM_techRef. pdf*, 2018.

[55] Mycryptopedia. (2018) Proof of importance explained. [Online]. Available: https://www.mycryptopedia.com/proof-of-importance/

[56] Coingecko. (2021) Nem price, xem price index, chart, and info. [Online]. Available: https://www.coingecko.com/en/coins/nem

[57] K. Karantias, A. Kiayias, and D. Zindros, "Proof-of-burn," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 523–540.

[58] Slimcoin. (2014) The slimcoin project. [Online]. Available: https://github.com/slimcoin-project/Slimcoin

[59] J. Mattila, "The blockchain phenomenon," *Berkeley Roundtable of the International Economy*, p. 16, 2016.

[60] S. S. Hazari and Q. H. Mahmoud, "Comparative evaluation of consensus mechanisms in cryptocurrencies," *Internet Technology Letters*, vol. 2, no. 3, p. e100, 2019.

[61] V. Saini. (2021) Consensuspedia: An encyclopedia of 30+ consensus algorithms — hacker noon. [Online]. Available: https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f

[62] B. Delisle. (2018) An introduction to iostoken: A blockchain for the internet of services. [Online]. Available: https://cryptoslate.com/introduction-iostoken-blockchain-internet-services/

[63] Anon. (2018) Nebulas technical whitepaper. [Online]. Available: https://nebulas.io/docs/NebulasTechnicalWhitepaper.pdf

[64] Q. Zhuang, Y. Liu, L. Chen, and Z. Ai, "Proof of reputation: a reputation-based consensus protocol for blockchain based systems," in *Proceedings of the 2019 International Electronics Communication Conference*, 2019, pp. 131–138.

[65] GoChain. (2021) 100% ethereum compatible, 100x faster. [Online]. Available: https://gochain.io/

[66] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proceedings of the 26th Symposium on Operating Systems Principles*, 2017, pp. 51–68.

[67] Amazon. (2021) Our planet. [Online]. Available: https://www.aboutamazon.com/planet

[68] Google. (2021) Google sustainability. [Online]. Available: https://sustainability.google/progress/energy/

[69] Microsoft-Build. (2021) Deploy ethereum proof-of-authority consortium solution template on azure - azure blockchain. [Online]. Available: https://docs.microsoft.com/en-us/azure/blockchain/templates/ethereum-poa-deployment

[70] DeadCoin. (2021) 1500+ cryptocurrencies forgotten by this world (2021 updated). [Online]. Available: https://99bitcoins.com/deadcoins/

[71] K. Wüst and A. Gervais, "Do you need a blockchain?" Cryptology ePrint Archive, Report 2017/375, 2017, https://eprint.iacr.org/2017/375.

[72] Coingecko. (2021) Cryptocurrency prices and market capitalization. [Online]. Available: https://www.coingecko.com/en

[73] L. Matthews. (2021) The 15 most sustainable cryptocurrencies for 2021. [Online]. Available: https://www.leafscore.com/blog/the-9-most-sustainable-cryptocurrencies-for-2021/

[74] B. Curran. (2018) What is proof of authority consensus? staking your identity on the blockchain. [Online]. Available: https://blockonomi.com/proof-of-authority/