A Novel Incentive Mechanism for Blockchain-based Carbon Emission Reduction in Construction (final)

Juan Wang, Dept. of Civil Engineering, The University of Hong Kong, Hong Kong, juanwang@connect.hku.hk

Xiao Li*, Dept. of Civil Engineering, The University of Hong Kong, Hong Kong, shell.x.li@hku.hk

ABSTRACT.

In response to climate change, the construction industry is facing tremendous pressure to reduce carbon emissions and realize sustainable development. Most governments have initiated a few incentive mechanisms, such as carbon trading and green subsidies, but these mechanisms are at the industry level and depend on external supervision. Besides, the existing environment management in construction exits issues, e.g., data loss and data fraud, while blockchain technology is encouraged to be applied to address these problems. Thus, to take advantage of blockchain and motivate project members to participate in carbon reduction, this paper proposes a novel incentive mechanism for blockchain-based carbon emission reduction. Specifically, the carbon reduction credit (CR credit) is proposed to evaluate the low carbon performance of members. Then, this mechanism mainly involves two parts: (i) update CR credits through two systems: the Crowd-Wisdom System, where green innovations are assessed, and the Reporting System, where members' carbon-related misbehaviors are detected; (ii) reward the ones with higher CR credits through a new consensus mechanism of blockchain, Proof of Carbon Reduction (PoCR). In the PoCR, participants compete to be the block producer (leader) driven by profits. The leader and block verifiers are selected by an election algorithm based on Verifiable Random Function (VRF) and CR credit amounts; the one with higher CR credits is more likely to be the winner in the leader election to generate a block and get a reward. The proposed incentive mechanism is expected not only to promote mutual supervision and stimulate members' creativity in green construction but also to improve the functions of the blockchain system.

KEYWORDS

Carbon emission reduction, Blockchain, Consensus mechanism, Incentive mechanism, construction

1. INTRODUCTION

As the main source of carbon emission, the construction industry is facing increasing pressure on energy saving and emission mitigation, especially when various sustainable policies are implemented worldwide, and countries have presented a strong determination to convert to a low-carbon economy (Chen et al., 2022; Liu, 2020). Mechanisms like carbon trading, green subsidies (Gauch et al., 2022), carbon tax, etc., have been designed to encourage the industry to develop sustainably. However, these mechanisms are proposed at the industry level and depend on external supervision. To the construction company, encouraging its members to regulate their carbon-related behaviors is important for it to meet the increasingly stringent emission requirements and achieve the overall sustainable goal. However, building a supervision team or relying on a third party for supervision may be costly and inefficient. Also, members may respond passively and tend to escape regulation rather than behave better if there is not enough incentive. Thus, designing a mechanism to inspire members' enthusiasm to reduce carbon emissions and promote mutual supervision is important.

Besides, the existing environment management in the construction industry faces challenges, including low digitalization, data loss, data fraud, loose information exchange, etc. Blockchain is then introduced to address these issues due to its properties of distribution, immutability, and reliability (Li et al., 2019). As a potential technology under Industry 4.0, blockchain is also widely used in supply chain management (Tezel et al.,2020; Li et al., 2022), payment (Sonmez et al., 2022), and safety monitoring in construction. For environment management, Zhong et al. (2022) proposed a blockchain-based framework for on-site construction environmental monitoring. Rodrigo (2020) discussed the potential application of blockchain technology for embodied carbon estimating in the construction supply chain. However, in these studies, the blockchain just plays an auxiliary role as a distributed database to store uploaded data. Although the data kept in the blockchain is helpful for decision-making and carbon emission analysis, the blockchain itself in these models can not impact members' behavior directly or incentivize members to reduce carbon emissions dynamically.

To address this limit, consensus mechanism designing may provide a potential. The consensus protocol is an important part of the blockchain, which determines participants to reach a consensus and coordinate in a distributed and decentralized setting, influencing the efficiency and sustainability of the blockchain (Ismil et al., 2019; Kau et al., 2021; Figueiredo et al., 2023). Designing consensus mechanisms for specific scenarios has been used to incentivize members' behavior and support decision-making (Yang et al., 2019). For example, Luo and Zhou (2021) designed a Proof of Participation (PoP) consensus mechanism with incentives for tourists to explore more attractions. Liu et al. (2019) proposed a Proof of Benefit (PoB) consensus mechanism to manage energy transactions for vehicles (EV), in which participants solve the overall benefit problem to compete to be the block generator. However, there is still a lack of discussions in the construction field, and it is valuable and meaningful to design consensus mechanisms to incentivize members to participate in carbon mitigation.

Hence, this paper developed a new consensus mechanism of blockchain, Proof of Carbon Reduction (PoCR), and based on it, a novel incentive mechanism for blockchain-based carbon emission reduction is proposed, aiming to not only improve the data quality and data reliability but also promote construction members' participation in carbon mitigation. Specifically, the carbon-reduction credit (CR credit) is proposed to evaluate low-carbon actions and honest behaviors and is updated mainly through two systems: (i) the Crowd-Wisdom System, where one can submit ideas/schemes in green innovations and gain a CR credit increase, and (ii) the Reporting System in which the reporter who reports misbehaviors will get a CR credit reward while the reported groups will face a CR credit decrease. In the PoCR, participants in each round compete to become the leader who generates the block, and the winner in the competition will get a reward. The leader and block verifiers are selected by an election algorithm based on Verifiable Random Function (VRF) and CR credit amounts, where the one with higher CR credits has a higher probability of being chosen as a block producer. Thus, participants are encouraged to gain more CR credits in the construction process.

doi:XXX-X-XXXX-XXXX-X/XX

To the best of the authors' knowledge, it is the first paper that considers carbon reduction factors in the design of the consensus mechanism in blockchain, and thus, blockchain here not only works as an immutable and reliable ledger but also provides a dynamic incentive for curbing carbon emission.

The contributions can be listed as follows:

(1) A novel incentive mechanism for blockchain-based carbon emission reduction is proposed. It provides a financial return for the one who performs well in low carbon in the construction process, that is, has more carbon reduction credits (CR credits), thereby encouraging members to participate in green innovations and regulate carbon-related behaviors. Also, it ensures the functions and security of the blockchain system, and thus, the authenticity and immutability of data are guaranteed.

(2) To better track members' behavior and update CR credits, the Crowd-Wisdom System and the Reporting system are designed. The Reporting system is designed to detect misbehavior in carbon emission through mutual supervision between different groups. This scheme is necessary, especially for behaviors that violate regulations but are difficult to detect. It is also used to detect malicious attacks on the system. The Crowd-Wisdom System is built to record members' innovations in sustainable construction.

(3) A new consensus mechanism of the blockchain is proposed, in which the block verifiers and the block producer (leader) are chosen by an election algorithm based on Verifiable Random Function (VRF) and CR credits. Under this consensus mechanism, verifiers are randomly selected proportional to their CR credit amount. Verifiers are then ranked by CR credits, and the one with the highest CR credits is chosen as the leader and gets a reward once a block is generated and verified to be valid.

The following parts are structured as follows. In section 2, related work is briefly reviewed. In section 3, the design goal, the roles this mechanism involved, and the concept of carbon credit are stated. Section 4 presents the process of the proposed mechanism. Then, a discussion is presented in terms of performance, security, and carbon reduction incentives in section 5. The conclusion and future work are presented in the last section.

2. Related works (brief)

2.1. Carbon Emissions in Construction

Most of the existing literature is about carbon accounting, using mainly three methods: input-output methods (Acquaye et al., 2010), process-based methods (Zaraza et al., 2022), and hybrid methods. Other studies include sustainable alternative materials (Kunic et al., 2021), optimization (e.g., structure design (DU et al., 2020), transportation routines, energy consumption of equipment (Masih-Tehrani et al.,2020), etc.), application of new technologies (eg. 3D concrete printing (Batikha et al., 2022). As for policies, carbon emission reduction decisions of stakeholders in the construction supply chain have been analyzed based on a game with government subsidies (Wang et al., 2022). The impact of policies such as carbon tax, construction waste sorting policy (Liu et al., 2023), and carbon trading policy (Liu & Li, 2023) have also been discussed. *However, few studies discuss how to motivate members involved in the construction process to regulate their carbon-related behaviors, and there is a lack of incentive mechanisms for carbon reduction from a company/project perspective.*

2.2. Blockchain Applications in Construction

In the construction field, the blockchain has been applied in information management (Yang et al., 2020), payment management (Elghaish et al., 2020), supply chain management (Wang et al., 2020), safety management (Li et al., 2022), etc. As for the application of blockchain in environment management, Zhong et al. (2022) built a blockchain-based framework for on-site construction environmental monitoring, in which smart contracts are used to monitor the pollutant level automatically. Wu et al. (2023) developed a blockchain non-fungible token-enabled "passport" for construction waste material cross-jurisdictional trading. In the applications above, blockchain technology is mainly used to store uploaded information, and thus, the main function of blockchain here is just to ensure the authenticity and immutability of data. Although smart contracts can improve their decision-making ability to some extent (Chen et al., 2023), the decision-making process is a response to the existing data. *The role of blockchain in these applications is still limited. Few studies discuss how to develop incentive mechanisms in blockchain.*

2.3. Consensus Mechanism

Consensus mechanisms are rules to decide whether a transaction is valid, ensuring that all participants maintain a common ledger. The existing consensus mechanisms in blockchain can mainly be categorized into three types (Oyinloye et al., 2021): (1) compute-intensive based consensus mechanisms which are energy-hungry mining algorithms (eg., Proof of Work (Nakamoto, 2018)); (2) capability-based consensus mechanism which focuses on the properties users have, like the amount of cryptocurrency, contribution, the amount of storage, etc. (e.g., Proof of Stake (King & Nadal, 2018), Proof of Space (Dziembowski et al., 2015); (3) Voting-based consensus mechanism where a leader is elected to generate a block (e.g., Practical Byzantine Fault Tolerance (Castro et al., 1999). With the development of blockchain technology, many new consensus mechanisms are proposed, developing the existing consensus protocols or designing to meet new requirements, such as Proof of Sincerity (Zaman et al., 2019), Proof of Reputation (Gai et al., 2018), Proof of Learning (Bravo-Marquez et al., 2019). *However, blockchain applications in construction mainly rely on several existing typical consensus mechanisms, which may not be suitable for specific scenarios, and the design of consensus mechanisms is hardly discussed in the construction industry.*

3. Preliminary

This section introduces the design goals, roles involved, and the concept of CR credit.

3.1. Design Goals

This mechanism is designed from the perspective of the entire project, rather than some of the stakeholders, and it is expected to achieve two objectives: (i) to encourage members to regulate their carbon-related behavior and promote sustainability in the construction process; (ii) to ensure the function and efficiency of blockchain, that is, guarantee the authenticity and immutability of data, and the efficiency in block generation (e.g., throughput, energy-efficiency, security).

Our paper tries to design a mechanism that allows the achievement of these goals simultaneously and makes them reinforce each other. It focuses on a "win-win" scenario rather than a trade-off between these goals. It is also expected to be incentive-compatible. That is, the individual's goal is consistent with the project's goal.

3.2. "Group"

A project may involve thousands of members, such as steel workers, tower crane drivers, managers, supervisors, designers, etc. Assume that members are rational and profit-driven and tend to adjust their behaviors according to their expected benefits.

For the sake of the feasibility of the proposed consensus mechanism, these members can be divided into several groups. "Group" is regarded as the representative of its members. The "Group" here is like the sector but has a smaller scale. For instance, the steelworkers can be divided into Steel One and Steel Two. Every member has and only has to belong to one Group at a time, and their profits depend on the performance of the "Group." These groups are the nodes participating in the proposed consensus mechanism, and different groups compete with each other to gain relatively more Carbon reduction credits, thereby obtaining potential rewards. For more information of Grouping policies, please see the section 5.4.

3.3. Carbon Reduction Credit

"Carbon emissions" is a general term or abbreviation for greenhouse gas emissions (GHGs). GHGs are defined as CO_2, N_2O, CH_4, HFC, PFC, and SF_6 in the Kyoto Protocol (Liu et al., 2020). However, as HFC, PFC, and SF_6 are rarely emitted in construction projects, the emission of CO_2, N_2O, and CH_4 is generally considered in the construction industry. Thus, the carbon-related behavior mainly refers to the behaviors related to the

doi: https://doi.org/10.47330/CBC.2023.KELI9256

above three emissions, and “low carbon” here means the level of carbon emissions is lower than the current level before any extra green measurement is implemented.

Carbon reduction credit (CR) proposed in this paper is an index that evaluates the performance of Group in low-carbon during the construction process, mainly in terms of four aspects: carbon emission, green technology, energy saving, and low-carbon management, as shown in Fig.1.

(1) Carbon emission. It mainly involves embodied emissions of material, transportation, energy consumption for processing and equipment, and disposal of construction waste. The data oracles always come from the Internet of Things (IoT) devices, such as RFID, vibration sensors, and GPS, and then the carbon emissions are calculated. To evaluate the performance in this aspect, expected/accepted intervals of emissions of key items are set. Bad violations will lead to a CR reduction.

(2) Green innovation. To improve the level of low-carbon innovation and inspire members’ enthusiasm for sustainable techniques, any new ideas for green technologies, energy optimization schemes, process reengineering, low-carbon design, mechanism design, etc., are encouraged. These innovations can be seen as improvements to the original/existing construction schemes. After being assessed, innovations are recorded and saved, which leads to a CR increase. Although these innovations may not be applied in the current project, they will provide advice for stakeholders and improve their ability to find solutions for carbon reduction in construction.

(3) Energy saving. In this aspect, the behaviors of waste of resources that are not easily detected by the system are evaluated. Misbehaviors include waste of materials, materials damage, water leakage, oil leakage, unnecessary usage of power, etc. These behaviors are mainly detected through mutual supervision. After misbehaviors are successfully reported, a CR credit reduction occurs.

(4) Low-carbon management. Management factors mainly involve elements that indirectly affect carbon emissions, such as staff training in low-carbon and environmental protection, carbon asset management, maintenance of equipment and systems, etc.

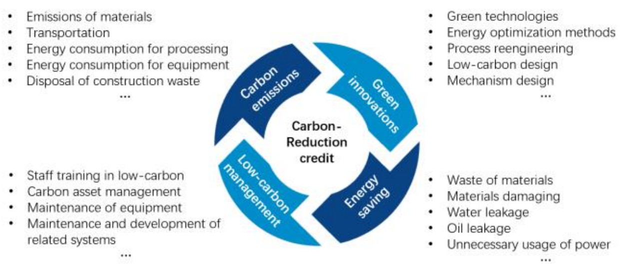

Fig. 1. Carbon-reduction credit

CR credit is based on the scoring system involving the above four parts, where every event corresponds to a certain score. This scoring system can be designed in advance by experts according to the characteristics of the project and the specific goals that companies want to achieve.

The changes in credits are traced by two systems in our proposed mechanism: the Crowd-Wisdom System and the Reporting System. For the green innovation factors, after being assessed in the Crowd-Wisdom System, innovations are recorded and saved, and this leads to a CR increase. For the other three factors, the Reporting System works: quantitative issues and qualitative issues are mainly reported by other groups and by the system, respectively; the reporter will get a credit increase while the reported groups will face a credit decrease. For more details, please see section 4.2.

The criteria for accepting/rejecting a scheme mainly includes three aspects: economic aspect, technical aspect, and environmental aspect. The first two aspects affect the adoption of the green scheme submitted, and the third aspect evaluates the potential contribution of the scheme to carbon reduction. The more cost-efficient, technically feasible, and better performance in carbon reduction the scheme is, the more CR credit increases. There is a trade-off between these three aspects, and the proportion can be set according to their importance based on the project goal during the evaluation. A scheme may be rejected for mainly three reasons: (1) too costly; (2) technically infeasible; (3) little contribution to carbon emission reduction. A successful submission in the Crowd-wisdom System leads to a CR credit increase, and the group will benefit from a high CR credit from being elected as the block generator (i.e., leader) under the POCR.

The change of CR credit follows the cause-oriented rule, that is, the one who causes the credit change is the one who bears the responsibility for this result.

4. NOVEL INCENTIVE MECHANISM FOR BLOCKCHAIN-BASED CARBON EMISSION REDUCTION

In this section, a novel incentive mechanism for blockchain-based carbon emission reduction is built.

4.1. Overall view

The proposed incentive mechanism mainly involves three parts (as shown in Fig.2): (i) The Crowd-Wisdom System and the Reporting System; (ii) Proof of Carbon Reduction consensus mechanism (PoCR); (iii) Reward allocation. The Crowd-Wisdom System and the Reporting System are used to detect and evaluate groups’ carbon-related behaviors and update their CR credits. The one with higher CR credits has an advantage in the block producer (leader) election under the PoCR. The winner who successfully generates a block will get a reward. Finally, the rewards groups will be distributed to their members.

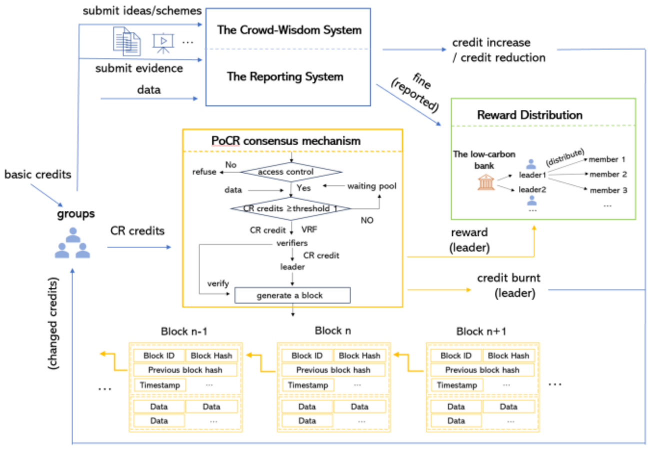

Fig.2. The framework of the proposed blockchain-based incentive mechanism

The blockchain we are involved in is a consortium blockchain; only the permitted groups can access it. At the initial stage, groups are given a fixed number (⩾threshold 1) of credits as base credits. As for the changes in CR credits, one can submit new ideas or schemes in green innovation to the Crowd-Wisdom System or report other groups’ misbehaviors in the Reporting System to gain CR credits. The one who is reported by other groups or is detected by the system due to bad violations faces a CR reduction. In the PoCR, block verifiers are randomly selected proportional to their carbon reduction credit amount based on the Verifiable Random Function (VRF), and among the selected verifiers, the one with the highest CR credit is then chosen as the leader who generates a block and get a reward. To avoid the “rich getting richer,” generating a block “burn” a certain amount of credit. Details of the Crowd-Wisdom System and the Reporting System are presented in 4.2; details of PoCR are shown in 4.3.

As mentioned above, there are three ways to cause changes in CR credits: (i) submitting ideas/schemes that contribute to green innovations in the Crowd-Wisdom System; (ii) reporting others / being reported in the Reporting System; (iii) generating a block. The current carbon reduction credit is based on the previous CR credit and the accumulated

doi: https://doi.org/10.47330/CBC.2023.KELI9256

credit changes in this period. The group $i's$ CR credits at time t can be formulated by:

$$CR_{i,t} = CR_{i,t-1} + q_{i,t}^{r,cr} + q_{i,t}^{r,r} - q_{i,t}^{f,r} - q_{i,t}^{b} \quad (t = 1,2,3 \dots)$$

$$CR_{i,0} = CR_{i,base}$$

where, $q_{i,t}^{r,cr}$ denotes the amount of the group $i's$ CR credits rewarded for contributions to green innovation through the Crowd-Wisdom System. $q_{i,t}^{r,r}$, $q_{i,t}^{f,r}$ represents the amount of the group $i's$ CR credits rewarded and CR credits fined by successfully reporting misbehaviors and being reported respectively through the Reporting System. $q_{i,t}^{b}$ is the amount of CR credits burnt at t. When $t = 0$ (initially), every group has a base CR credit $CR_{i,base}$.

Not that, to ensure fairness, CR credits can only be updated through the above ways and cannot be traded. The amount of a group's CR credits may change over time. Once its CR credits are below threshold 1, it is put in the waiting pool where nodes have no right to participate in the block generation competition and the verification process in PoCR. Once the value of CR credit is less than threshold 2, it faces a financial fine.

Each group owns two wallets: one is for CR credits (wallet 1), and another is for monetary income (wallet 2). The "Low Carbon Bank" is an account set to reward the successful block generator. The reward and its distribution will be discussed in section 4.4.

4.2. The Crowd-Wisdom System and the Reporting System

In this section, the Crowd-Wisdom System and the Reporting System are built and illustrated. Here, the "jury" plays an important role in determining the validity of submitted files and maintaining the systems. The jury can consist of senior managers and experts who have enough experience and are independent of the interests of other groups. This is a special group supported by the company and cannot participate in the competition of block generation. To prevent collusion, the members of the jury will be selected again after a period of time.

4.2.1. Crowd-Wisdom System

This system is used to stimulate the members' enthusiasm and creativity in green construction, and then more potential low-carbon schemes or tools are provided, allowing parties involved to improve their ability to handle carbon-related issues. The process of this system is as follows (shown in Fig.3):

First, the group submits its new idea/scheme in green construction to the Crowd-Wisdom System. The jury members then vote whether to accept it or reject it according to its potential contributions. If most of the members of the jury think it is of little value, then a rejection message is sent to the group. If this submitted scheme is accepted by the jury, the jury will determine the CR credit reward and broadcast the results. The scheme is kept in the system and open to the authorized members.

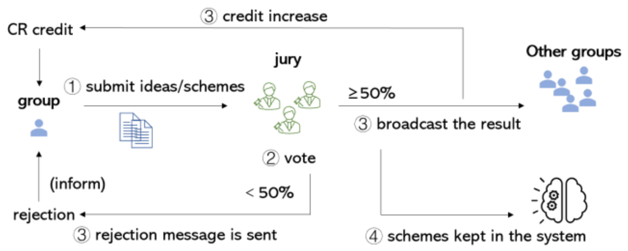

Fig. 3. Crowd-Wisdom System

4.1.2 Reporting System

To better record members' misbehaviors, a reporting system is proposed. There are commonly two types of events that are not conducive to carbon reduction: (i) qualitative events which are hard to detect by the system automatically, such as the disposal of oil; (ii) quantitative events which can be supervised by the system and be reported in time once outliers are detected. Thus, the reporting scheme involves two parts: (i) reported by other groups, and (ii) reported by the system. The former is suitable for detecting qualitative events while the latter is suitable for quantitative events. The reporting system is shown in Fig. 4.

(1) Reported by groups

Once the misbehavior of members of other groups, the reporter first submits the evidence to his group (manager), and after verification, the evidence will be uploaded to the reporting system. Then, jury members vote to accept it or reject it. If the acceptance rate is less than 50%, the reporting is then rejected. If the reporting is accepted by the jury, the group reported will get a punishment in terms of RC credit reduction (wallet 1) and financial fine (wallet 2), and the group reporting will get a reward in terms of RC credit increase (wallet 1) and monetary incentive (wallet 2). The jury charges a trial fee from the group reported (wallet 2). The result is then broadcast to other groups. The reporting evidence can be files, photos, videos, etc., and it is recorded in the system. It is the jury to make a consensus on the severity of the reported events and determine the punishment level and reward level (i.e., how much CR credits the reported nodes will decrease/increase, and how much the fine/reward).

(2) Reported by system

The system will monitor any data exceptions and malicious attacks automatically. For detecting carbon emission data, the standard levels of key data are set in the system initially according to the related policies, rules, and requirements. Once an exception occurs, the system will take measures and execute the corresponding rewarding/punishing process (CR credit decrease or increase). For detecting malicious attacks, the nodes attacked will be detected due to their abnormal behaviors, such as delays and frequent visits. The standard levels of data and the attack information can be updated, removed, and added by the jury (after a consensus is reached).

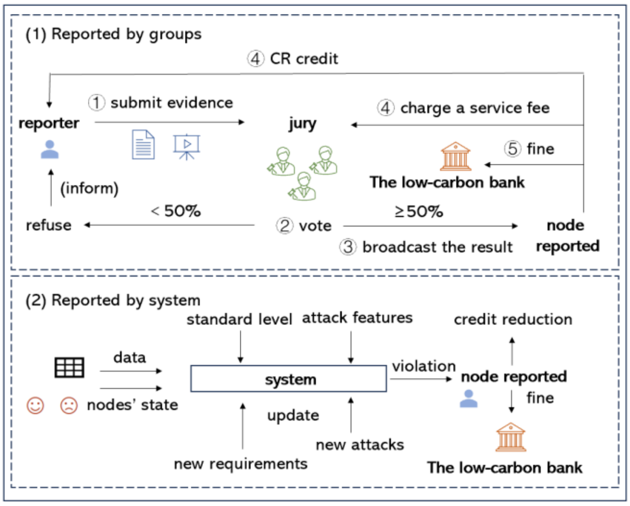

Fig. 4. The reporting system

4.3. Proof of Carbon Reduction (PoCR)

Consensus mechanisms in blockchain mainly involve three parts: (i) block proposer selection, (ii) block validation, and (iii) rewarding rule. In this paper, the leader who generates a valid block will get a reward.

In the PoCR, a group may be in the following states:

- Waiting node. The group whose CR credits are below threshold 1 is put into the waiting pool, where nodes have no right to participate in the block generation competition and the verification process.
- Candidate. The group whose CR credits are below threshold 2 is put into the candidate pool, where nodes have a chance to be selected as verifiers and the leader who produces a block.
- Verifier. Verifiers are responsible for verifying a block.
- Leader. The leader is the one with the highest CR credits among verifiers. It is expected to generate a valid block before the timeout.

doi: https://doi.org/10.47330/CBC.2023.KELI9256

The process of PoCR can be stated as (shown in Fig. 3): the groups whose credits exceed threshold 1 are put into the candidate pool first. Among the candidates, verifiers are then randomly selected proportional to their carbon reduction credit amount based on the Verifiable Random Function (VRF). The higher the CR credits, the greater the probability of being chosen. After that, rank verifiers based on their CR credit; the one with the highest CR credits is selected as the leader this round. The leader then produces a block, and others verify it. If the block is verified successfully, the groups will add this block to their blockchains; otherwise, the block is discarded. To ensure the liveness of the proposed mechanism, the prime leader (ranking second in the leader election) will generate a new block if the current block is invalid or the leader fails to produce a block before the timeout. The leader who generates a valid block successfully will get a reward (kept in wallet 2). The election of candidates and the leader is shown in section 4.3.1, and the verification process is presented in section 4.3.2.

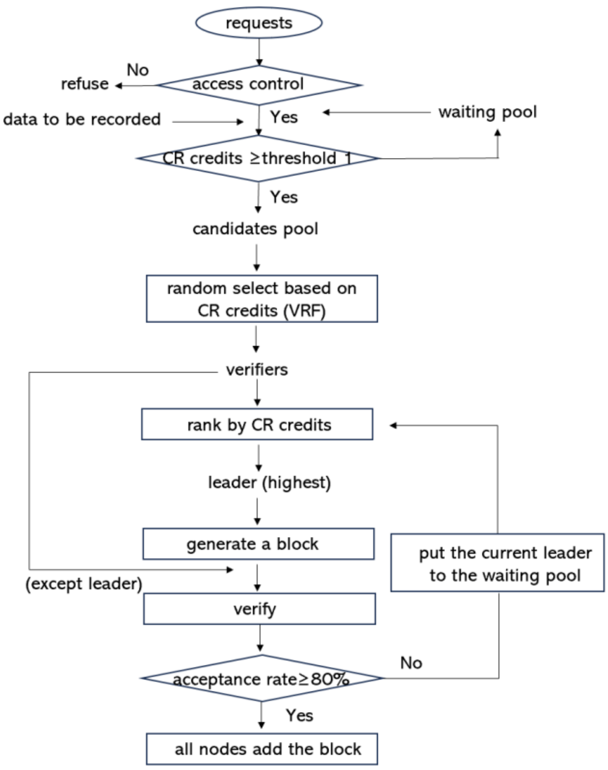

Fig. 5. PoCR process

4.3.1. Election of Verifiers and the Leader

The election process is expected to meet two goals: (1) the one with higher CR credits has a higher probability of being chosen as the leader; (2) every group has a chance to be selected. Here, randomness is considered to ensure fairness and participation. It is also important for system security; if the leader and verifiers are determined in advance, the system will more easily suffer from node attacks.

The election of verifiers is based on the Verifiable Random Function (VRF). VRF is an encryption scheme that maps inputs to verifiable pseudo-random output. Informally, on any private key sk and a seed x (a string), $VRF_{sk}(x)$ will output a hash value $v(sk, x)$ and a proof π, satisfying $v(sk, x) \in [0, 2^{hashlen-1}]$ (where $hashlen$ is the bit-length of hash). The proof π enables anyone who knows the public key pk to check that the hash indeed corresponds to x without having to know sk. It was first proposed by Micali et al. in 1999, and in 2017, Gilad et al. first applied it in the cryptocurrency, Algorand, to select committees under a distributed network. For more details on VRF, please refer to the work of the reference (Micali et al., 1999) and (Gilad et al., 2017).

The process of selecting m verifiers from n candidates proportional to their amount of CR credits is as follows. Each group i has a public/private key pair, (sk_i, pk_i). Denote the group $i's$ CR credits Q_i, and then the total CR credits of all groups is denoted by $(\Sigma_{i=1}^{n} Q_i)$. The CR credits are the weights that a group owns. Here, we regard each credit as a sub-group j; the group that owns Q_i credits then correspond to Q_i sub-groups. Let j_i represents the j^{th} unit of CR credit i owns, satisfying $j_i \in \{1,2,\dots,Q_i\}$. Set a threshold τ (which determines the expected number of groups selected), representing the number of sub-groups it wants to choose. Then, for each sub-group j, the probability of being selected is $p = \tau/\Sigma_{i=1}^{n} Q_i$. The probability that exactly k out of the Q_i are selected following the binomial distribution, formulated by $B_i(k; Q_i, p) = \binom{Q_i}{k} p^k (1-p)^k$, where $\Sigma_{k=0}^{Q_i} B_i(k; Q_i, p) = 1$. If $\frac{v(sk_i, x)}{2^{hashlen-1}}$ falls in the interval $[\Sigma_{k=0}^{j_i} B_i(k; Q_i, p), \Sigma_{k=0}^{j_i+1} B_i(k; Q_i, p))$, then the group i has exactly j_i selected sub-groups. Then, order candidates according to their value of j_i, and the top m candidates are selected as verifiers.

Then, the one with the highest CR credits among verifiers is the leader who generates a block.

For the selection of the seed of VRF, the hash of the current data is selected as the seed in this paper, denoted by $hash_{(1)}(d)$, where d is the data and $hash_{(1)}$ can be $hash256$, which could be unexpected and not be known in advance, protecting against malicious attacks.

The algorithm of the election of verifiers and the leader is shown in Table 1 and Table 2.

Table 1. The algorithm for the election of verifiers and the leader (1)

Algorithm 1 Selection by VRF
Input: τ, sk_i, Q_i, n, d
Return: $\langle v(sk_i, hash_1(d)), \pi_i, j_i \rangle$
1. $p \leftarrow \tau/\Sigma_{i=1}^{n} Q_i$
2. $j_i \leftarrow 0$
4. $\langle v(sk_i, hash_1(d)), \pi_i \rangle \leftarrow VRF_{sk_i}(hash_1(d))$
5. **While** $\frac{v(sk_i, hash_1(d))}{2^{hashlen-1}} \notin [\Sigma_{k=0}^{j_i} B(k; Q_i, p), \Sigma_{k=0}^{j_i+1} B(k; Q_i, p))$ **do**
6. $j_i + +$
7. **end**

Table 2. The algorithm for the election of verifiers and the leader (2)

Algorithm 2 Determination of verifiers and the leader
Input: $J = \{j_1, j_2, \dots j_i \dots\}$, function F: $F(j_i) = i$, $Q = \{Q_1, Q_2 \dots Q_i \dots\}$, m
Return: $Verifiers$ set: V, $leader$
1. $g \leftarrow 0$
2. $V \leftarrow [\,]$
3. $L \leftarrow [\,]$
3. $J' \leftarrow$sort (J)
4. **While** len$(V) < m$ do **do**
5. $V[g] \leftarrow F(J'[g])$
6. $L[g] \leftarrow Q[G[g]]$
7. $g + +$
8. **end**
9. $L' \leftarrow$sort (L)
10. $leader \leftarrow L'[0]$

4.3.2. Verification Process

After the block is produced, the leader will broadcast it to other nodes. Other nodes then verify the previous hash, timestamp, and random number generated by VRF, and verify the required data/transactions. After there are enough verifications (>=80%), participants add the new block to their blockchains. If the leader cannot produce a new block before the timeout or the block does not pass the verification process, the prime leader (ranked second in the leader election ranking) will be the leader who produces the new block this round. Prime leader setting can ensure the liveness of the consensus mechanism. The leader who generates a block will "burn" some carbon credits. To avoid a potential fork, nodes except the leader are not permitted to generate a block. The verification process is shown in Table 3.

Table 3 Verification process

doi: https://doi.org/10.47330/CBC.2023.KELI9256

Algorithm 3 Verification process

If $Verifyhash < previous\ block\ hash, timestamp, data, signature > is\ Ture$ **then**
  If $VerifyVRF_{pk}(\mathrm{v}(sk_i, hash_1(d), \pi, hash_1(d)) \ is\ Ture$ **then**
    If $\mathrm{v}(sk_i, hash_1(d))/2^{hashlen-1} \in [\Sigma_{k=0}^{j} B(k; Q_i, p), \Sigma_{k=0}^{j+1} B(k; Q_i, p)) \ is\ Ture$ **then**
      Return *Ture*
    end
  end
end

4.4. Reward and reward distribution

As mentioned above, groups can only get rewards from block generation. The groups with higher CR credits have more opportunities to be selected as the leader, that is, more benefits from generating blocks. The financial reward would come from the "Low Carbon Bank," which is a dedicated bonus distribution account set and maintained by project-related shareholders. This bank is expected to deposit a sufficient amount of money for rewarding block generation. A warning will be set once the deposit in "Low Carbon Bank" is below a threshold. The deposits not only come from managers but also from the reported nodes (fine). As for the reward distribution between members in the group, it can be designed by each group flexibly, such as equal distribution or distribution based on contributions. Once the money in the group's wallet 2 is transferred to its members' real-world accounts, wallet 2 is cleared (reserve a threshold of money). The reward distribution is shown in Fig. 5.

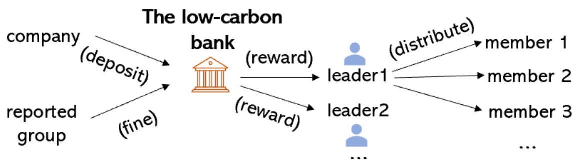

Fig. 6. The reward distribution

5. DISCUSSION

There have been some indexes proposed in previous studies to evaluate the consensus mechanisms. For instance, Xu et al. investigate the consensus mechanisms from three aspects, including the performance aspect (scalability, throughput, latency), security aspect (adversary tolerance, malicious attacks), and cost aspect (computing cost). Oyinloye et al. (2021) evaluate consensus mechanisms from the metrics of energy consumption, scalability, finality, security, and throughput. In our study, we will discuss the proposed mechanism in terms of performance (energy consumption, scalability, complexity, etc.), security, and low-carbon incentives.

Besides, grouping policies will be further discussed in this section.

5.1 Performance

As for energy consumption, this proposed consensus mechanism is energy-efficient due to the low computing power required, which is different from PoW, where miners consume computing resources to solve math problems. As for scalability, this proposed mechanism is lightweight, and the size of verifiers can be controlled by a parameter set, that is, the overhead of communication between nodes is controlled. Also, the size of a group can be adjusted according to the number of members involved in the project. Thus, it shows a good performance of scalability, i.e., no matter how many groups and how many members participate.

5.2 Security

Security reflects the ability to resist attacks. Common attacks like Sybil attack, 51% attack, double spending attack, and DoS attack. (1) For the Sybil attack, the proposed consensus mechanism is applied in a consortium blockchain, that is, only the permitted and certificated nodes have the right to access this distributed system, which adds to the cost of the attack. (2) For the 51% attack, in our proposed model, only over 80% acceptance of verifiers does the block can be valid and be added to the blockchain. Also, the leader/block generator is selected randomly, and the type of nodes will change with time due to their dynamic change of CR-credit value, which makes 51% attack or collusion almost impossible. (3) For a double spending attack, in our proposed consensus mechanism, only the leader (prime leader) has the right to produce a block, which can be effective against fork issues. (4) For a DoS attack, the reporting system in the proposed mechanism can track the status of each node, and when there is a node active abnormally, it would detect it and report it. It seems that the one who has a higher CR credit are honest nodes, since if they do malicious behaviors and are detected, their CR credits would be cut.

5.3. Low-carbon Incentive

Different from the previous consensus mechanism, the proposed consensus mechanism can incentivize members to conduct environmentally friendly behaviors. Competition is introduced, and mutual supervision is realized. The groups performing well on low-carbon events will get more rewards. Some may argue that it is unfair that carbon-related events vary with job scopes, and the groups responsible for carbon-intensive tasks may have more risk to be reported, leading to a lower CR credit. While, different events are regulated by different requirements, and only bad violations are detected. Also, from the perspective of the overall goal (reduce total carbon emissions), the groups responsible for carbon-intensive tasks contribute more to the total carbon emissions of the project, and they are expected to receive more supervision. Driven by profits, other groups tend to supervise these groups for potential reporting chances, which meet incentive compatibility.

5.4. Grouping Policy

The aim of grouping in this research is to pair members with nodes in the blockchain system so that the behavior of members can be recorded and evaluated. There are mainly two ways to group members: (1) department-focus method and (2) process-focus method. In the department-focus method, members in the group mainly belong to the same department/organization. This research mainly focuses on this grouping policy.

While in the process-focus method, members from different organizations may be involved in a group to complete a specific work package. The proposed mechanism may work slightly differently under this scenario as follows:

(1) Define work packages. This step is to define work packages based on the elemental tasks. For example, steel reinforcement binding, steel forging, and pressing belong to the work package of steel engineering. Generally, members would be assigned to work packages and take responsibility for related tasks based on their professions.
(2) Identify CR credit with work packages. The increase or decrease (change) of CR credits will be tagged/identified with the corresponding work packages. It means that the contribution of CR credit change can be tracked at a work package level.
(3) Distribute returns according to the contribution of work packages. A group's reward from generating blocks is first distributed to the complected or under-going work packages it involved according to their contribution of CR credit. Then, the distributed financial return of the work package will further be distributed to its members. The distribution process can be executed automatically by algorithms.

Hence, the process-focus grouping method will mainly focus on members' carbon behaviors in their work packages rather than their affiliations and achieve mutual supervision between collaborators.

6. CONCLUSION AND FUTURE WORK

This paper proposes a novel incentive mechanism for blockchain-based carbon emission reduction in the construction process. In the future, the scoring system of the CR credits will be more specified, and experiments in the real-life world will be conducted to validate the feasibility of the proposed mechanism.

Acknowledgment: This research was supported by grants from the Research Grants Council of the Hong Kong SAR of China, the National Natural Science Foundation of China, and the University of Hong Kong

doi: https://doi.org/10.47330/CBC.2023.KELI9256

(RGC Project No.15219422 & G-HKU502/22, NSFC Project No. 72201228, HKU Project No. 2201100548, 2023A1515011162, AR03132308).

References

ACQUAYE A., DUFFY A.P., 2010. Input-output analysis of Irish construction sector greenhouse gas emissions. Build Environ 45(3): 784-791.

BATIKHA M., JOTANGIA R., BAAJ M.Y., MOUSLEH I., 2022. 3D concrete printing for sustainable and economical construction: A comparative study. Automation in Construction 134: 104087.

BRAVO-MARQUEZ F., REEVES S., UGARTE M., 2019. Proof-of-Learning: A Blockchain Consensus Mechanism Based on Machine Learning Competitions. In Proceedings of the 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), Newark, CA, USA, 4–9.

CASTRO M., LISKOV B., 1999. Practical Byzantine fault tolerance. In Proceedings of the 3rd Symposium on Operating System Design and Implementation (OSDI), New Orleans, LA, USA, February 1999; Unisex Association: Berkeley, CA, USA: 173–186.

CHEN G.F., S.M.ASCE., LIU M., A.M.ASCE., ZHANG Y.X., WANG Z.G., HSIANG S.M., A.M.ASCE., HE C., S.M.ASCE. 2023. Using Images to Detect, Plan, Analyze, and Coordinate a Smart Contract in Construction. Journal of Management in Engineering 39(2): 04023002.

CHEN W.L, YANG S.Y., ZHANG X., JORDAN N.D., HUANG J.S., 2022. Embodied energy and carbon emissions of building materials in China. Building and Environment 207, 108434.

DU T.T., TURRIN M., JANSEN S., VAN DEN BOBBELSTEEM A., FANG J., 2020. Gaps and requirements for automatic generation of space layouts with optimised energy performance. Automation in Construction 116: 103132.

DZIEMBOWSKI S., FAUST S., KOLMOGOROV V., PIETRZAK K., 2015. Proofs of space. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; Springer: Berlin/Heidelberg, Germany: 585–605.

ELGHAISH F., ABRISHAMI S., HOSSEINI M.R., 2020. Integrated project delivery with blockchain: An automated financial system. Automation in Construction 144: 103182.

FIGUEIREDO K., HAMMAD A.W.A., HADDAD A., TAM V.W.Y. 2022. Assessing the usability of blockchain for sustainability: Extending key themes to the construction industry. Journal of Cleaner Production 343, 1311047.

GA F., WANG B.; DENG W., PENG W., 2018. Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. In Database Systems for Advanced Applications; Springer International Publishing: Cham, Switzerland, 666–681.

GAUCH H.L., HAWKINS W., IBELL T., ALLWOOD J.M., DUNANT C.F., 2022. Carbon vs. cost option mapping: A tool for improving early-stage design decisions. Automation in Construction 136: 104178.

GILAD Y., HEMO R., MICALI S., VLACHOS G., 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. SOSP '17: Proceedings of the 26th Symposium on Operating Systems Principles 51-68.

ISMAIL L., MATERWALA H., 2019. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. Symmetry 11, 1198.

KING S., NADAL S., 2018. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Available online: https://decred.org/research/king2012.pdf.

KUNIC A., NABONI R, KRAMBERGER A., SCHLETTE C., 2021. Design and assembly automation of the Robotic Reversible Timber Beam. Automation in Construction 123, 103531.

LI J., GREENWOOD D., KASSEM M. 2019. Blockchain in the built environment and construction industry: A systematic review, conceptual models and practical use cases. Automation in Construction 102, 288-307.

LI X.,., LU W.S., XUE F., WU L.P.F., ZHAO R., LOU J.F., XU J.Y. 2022. Blockchain-Enabled IoT-BIM Platform for Supply Chain Management in Modular Construction. Journal of Construction Engineering and Management 148(2): 04021195.

LI X., ZENG J.H., CHEN C., CHI H.L., SHEN G.Q., 2022. Smart work package learning for decentralized fatigue. Comput-aided Civ Inf.

LIU C., CHAI K.K., ZHANG X.S., CHEN Y., 2019. Proof-of-Benefit: A Blockchain-Enabled EV Charging Scheme. In Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA.

LIU J.K., LI J.Y., 2023. Economic benefit analysis of the carbon potential of construction waste resource management based on a simulation of carbon trading policy. Environmental Science and Pollution Research 30(36): 85986-86009.

LIU J.K., LI Y.X., WANG Z.S., 2023. The potential for carbon reduction in construction waste sorting: A dynamic simulation. Energy 275:127477.

LIU, G.W., CHEN R.D., XU P.P., FU Y., MAO C., HONG J.K. 2020. Real-time carbon emission monitoring in prefabricated construction. Automation in Construction 110, 102945.

LUO L., ZHOU J., 2021. BlockTour: A blockchain-based smart tourism platform. Computer Communications 175:186-192.

MASIH-TEHRANI M., EBRAHIMI-NEJAD S., DAHMARDEH M., 2020. Combined fuel consumption and emission optimization model for heavy construction equipment. Automation in Construction 110, 103007.

MICALI S., RABIN M., VADHAN S., 1999. Verifiable random functions. 40th Annual Symposium on Foundations of Computer Science (Cat. No.99CB37039), New York, NY, USA, 120-130.

NAKAMOTO S. 2008. Bitcoin: A Peer-To-Peer Electronic Cash System. Available online: https://bitcoin.org/ bitcoin.pdf.

OYINLOYE D.P., THE J.S., JAMIL N., ALAWIDA M., 2021. Blockchain Consensus: An Overview of Alternative Protocols. Symmetry 13,1363.

RODRIGO M.N.N., PERERA S., SENARATNE S., JIN X.H. 2020. Potential Application of Blockchain Technology for Embodied Carbon Estimating in Construction Supply Chains. Buildings 10,140.

SONMEZ R., AHMADISHEYKHSARMAS S., GUNGOR A.A., 2022. BIM integrated smart contract for construction project progress payment administration. Automation in Construction 129: 104294.

TEZEL A., PAPADONIKOLAKI E., YITMEN I., HILLETOFTH P., 2020. Preparing construction supply chains for blockchain technology: An investigation of its potential and future directions. Frontiers of Engineering Management 7,547-563.

WANG W., HAO S.J., HE W., MOHAMED M.A., 2022. Carbon emission reduction decisions in construction supply chain based on differential game with government subsidies. Building and Environment 222:109149.

WANG Z.J., WANG T.Y., HU H., GONG J., REN X., XIAO Q.Y., 2020. Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. Automation in Construction 111: 103063.

WU L.P.F., LU W.S., PENG Z.Y., WEBSTER C., 2023. A blockchain non-fungible token-enabled 'passport' for construction waste material cross-jurisdictional trading. Automation in Construction 149, 104783.

XU, Y.Q., TAO, X.Y., DAS, M., KWOK H.H.L, LIU H., WANG G.B., CHENG J.C.P. 2023. Suitability analysis of consensus protocols for blockchain-based applications in the construction industry. Automation in Construction 145, 104638.

YANG J.; ONIK M.; LEE N.Y.; AHMED M.; KIM C.S. 2019. Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making. Applied Science 9, 1370.

doi: https://doi.org/10.47330/CBC.2023.KELI9256

YANG R., WAKEFIELD R., LYU S., JAYASURIYA S., HAN F.L., YI X., YANG X., AMARASINGHE G., CHEN S.P., 2020. Public and private blockchain in construction business process and information integration. Automation in Construction 118: 103276.

ZAMAN M.U., SHEN T., MIN M., 2019. Proof of Sincerity: A New Lightweight Consensus Approach for Mobile Blockchains. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14.

ZARAZA J., MCCABE B., DUHAMEL M., POSEN D., 2022. Generative design to reduce embodied GHG emissions of high-rise buildings. Autom in Construction 139.

ZHONG B.T., GUO, J.D., ZHANG L., WU H.T., LI H., WANG Y.H. 2022. A blockchain-based framework for on-site construction environmental monitoring: Proof of concept. Building and Environment 2017, 109064.