Knowledge-Based Systems 269 (2023) 110501

Contents lists available at ScienceDirect

Knowledge-Based Systems

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

SIAEF/PoE: Accountability of Earnestness for encoding subjective information in Blockchain

Hang Thanh Bui [a,*], Omar K. Hussain [a], Daniel Prior [a], Farookh K. Hussain [b], Morteza Saberi [b]

[a] School of Business, University of New South Wales, Canberra, 2612, ACT, Australia
[b] School of Computer Science, University of Technology Sydney, Sydney, 2007, NSW, Australia

ARTICLE INFO

Article history:
Received 13 December 2022
Received in revised form 28 February 2023
Accepted 20 March 2023
Available online 25 March 2023

Keywords:
Blockchain
Subjective information
Consensus mechanism
Earnestness
Proactive supply chain risk management
Fraudulent behaviour

ABSTRACT

Blockchain technology has the potential to be applied widely in supply chain operations. One such area is proactive supply chain risk management (SCRM). In this area, existing researchers have highlighted the fraudulent behaviour of supply chain partners who do not disclose information on the risks that impact their operations. Blockchain can address this problem by encoding each partner's commitment to SCRM and achieve consensus. However, before this can be achieved, a key challenge to address is the inability of existing consensus mechanisms such as Proof of Work (PoW), Proof of Authority (PoA) and Proof of Stake (PoS) to deal with information that does not have a digital footprint. In this paper, we address this gap by proposing the Proof by Earnestness (PoE) consensus mechanism which accounts for the authenticity, legitimacy and trustworthiness of information that does not have a digital footprint. We also propose the Subjective Information Authenticity Earnestness Framework (SIAEF) as the overarching framework that assists PoE in achieving its aim. We test the applicability of SIAEF and PoE in a real-world blockchain environment by deploying it as a decentralized application (Dapp) and applying it in BscScan Testnet which is an official test blockchain network.

1. Introduction

Blockchain technology has burgeoned as a result of the booming value of cryptocurrency capitalization [1]. It enables financial transactions to be carried out without the regulation of a bank or a third party. Aspects such as privacy, trust, security and transparency of a transaction are ensured by the immutability characteristics of blockchain. These features have resulted in blockchain being used in many other domains, such as supply chains [2,3]. As reported by Lahkani et al. [4], the efficiency of the supply chain network has improved by 74%–75% with the adoption of blockchain technology. In addition to providing transparency and traceability [5], blockchains enable the supply chain partners to access a single source of truth that has a lower administrative cost than existing disparate platforms [6]. This assists them in addressing critical supply chain issues such as trust mechanisms, fraud, authenticity, and information transmission among supply chain partners [6,7].

Blockchain guarantees the immutability of a piece of information by recording it in a block. While this does not prevent entities from viewing this information (depending upon their access), it prevents them from modifying or deleting it [7]. However, this information can be updated with the modified information recorded in a new block connected to a previous block by a serial number called a hash. Over time, these linked chains of blocks enable blockchain to provide a unique and single source of truth. Before recording any information in a block, the blockchain achieves consensus among entities using different algorithms such as Proof of Work (PoW) [8], Proof of Stake (PoS) [9], Proof of Authenticity (PoA) [10], and Delegated Proof of State (DPoS) [11]. In PoW, entities are either classified as miners or verifiers. As shown in Fig. 1, to record a piece of information (or a transaction or a certificate), miners solve a complex problem associated with it. When the verifiers verify the problem's solution, consensus is achieved, and the information is recorded in a block [12]. In PoS, selected entities are classified as validators responsible for forging the next block with the information that needs to be recorded [13]. When the validators attest to the information, consensus is achieved and the information is recorded as a block. In DPoS, the entities vote for multiple representatives to act on their behalf. When used with quantum technologies, this enhances the throughput of the blockchain and minimizes latency in

* Corresponding author.
E-mail addresses: hangthanhbui@unsw.edu.au (H.T. Bui), o.hussain@adfa.edu.au (O.K. Hussain), d.prior@adfa.edu.au (D. Prior), farookh.hussain@uts.edu.au (F.K. Hussain), morteza.saberi@uts.edu.au (M. Saberi).

https://doi.org/10.1016/j.knosys.2023.110501

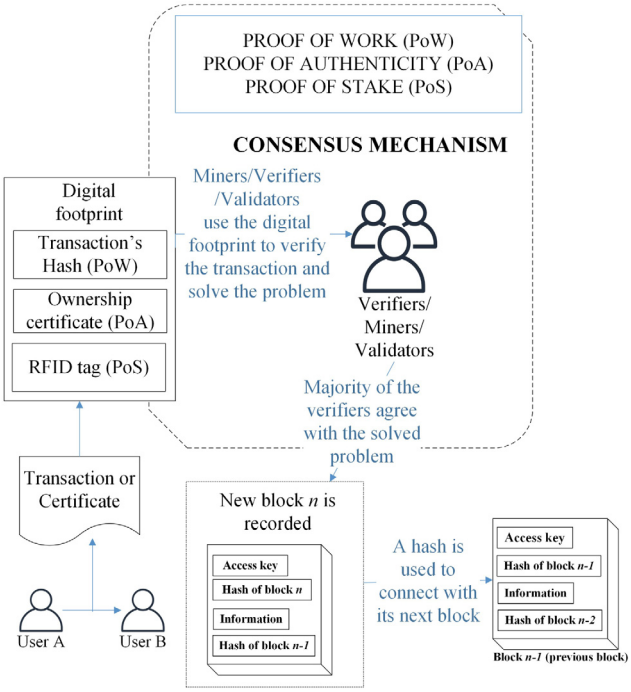

Fig. 1. The working of consensus mechanisms in blockchain.

comparison with PoW, PoS or PoA [11]. Recently, quantum cryptography [11] and post-quantum cryptography [14] have been used to build a quantum blockchain to safeguard information and withstand certain types of quantum attacks.

The type of consensus algorithm chosen depends on the nature of the transaction. But as shown in Fig. 1, irrespective of the algorithm used, a pre-requisite step for either miners or verifiers to confirm before gaining consensus is to validate the truthfulness of the information that is to be recorded in the block. Existing consensus algorithms implicitly focus on this step, assuming that the information to be recorded in a block is objective. By objective, we mean it has a digital footprint verifying its correctness. For example, the truthfulness of the statements *'Alex sent an amount of $10,000 to Elisa via Internet Banking'* or *'Responsible partner A confirmed that it had delivered the package to its client'* can be proven by the digital footprint associated with these transactions, such as a bank transfer receipt and digital tracking, respectively. However, such a digital footprint may not be available for other types of information, such as *'Alex claims that he personally handed Elisa an amount of $10,000'* or *'This painting is claimed to be painted by Picasso'*. We term these types of information, which do not have a digital footprint as subjective. Before such statements can be recorded in a block, an explicit process is needed that the consensus mechanisms can use to verify their truthfulness and trustworthiness. As explained in our state-of-the-art review paper [15], existing consensus algorithms such as PoW, PoS or PoA fail in this regard. This is a grey area in applying blockchains in domains such as proactive supply chain risk management (SCRM) in which different types of subjective information are present, as explained in the next subsection.

1.1. Subjective information — its presence and impact on proactive SCRM

Proactive SCRM is one of the integral steps in managing supply chain operations. It identifies the presence of different risk terms impacting an operation and facilitates the application of different management strategies to deal with them [16]. As supply chains are a consortium of geographically spread partners, they are exposed to different operational risks impacting different partners at different times. As a supply chain is only as strong as its weakest link, in a proactive SCRM, each consortium partner is responsible for managing the risk terms impacting it for the good and benefit of the whole chain [17]. Researchers have highlighted the fraudulent behaviour of supply chain partners [18] to cover their non-compliance to address the operational risk terms impacting them [19,20]. This makes the whole supply chain susceptible to failure. To address this, we propose that each partner's response to the risk terms impacting it be visible to other supply chain partners to ensure their accountability. The visibility and impact of each partner's response to the risk terms affecting it can easily be provided for those tasks that leave a digital footprint (objective information). However, it is challenging to provide the same for tasks that do not leave a digital footprint (subjective information). Examples of such instances in proactive SCRM are as follows:

- *Determining the correctness of claims leading to the commitment of a promise:* A supply chain contract is formed as a service-level agreement (SLA) between two or more partners. An SLA documents the particular services to be provided and defines the service standards the partner has agreed to commit to it over a period of time. In some cases, there will be a time lag from the start of an SLA to an action to be performed [21]. For example, let us assume that *Partner 1*, *Partner 2*, *Partner 4*, and *Partner 9* are part of a supply chain and they form an SLA on 14 April 2022. One of the SLA's clauses mentions that *Partner 1* should transport its manufactured goods to *Partner 2* on 18 May 2022. In such a case, the first transaction that creates a digital footprint is the shipment of goods by *Partner 1* on 18 May 2022. While this can be recorded on the blockchain and used for proactive SCRM by the existing PoW/PoS/PoA consensus algorithms, any information before this, such as information related to the manufacturing of the goods, may not, as it is not publicly shared with other partners. This leads to the following two possibilities. The first is that *Partner 1* does not ship the goods as promised despite subjectively assuring the other partners that it is on track to do so. To the other partners, this will be known on the day the goods are expected to be shipped (18 May 2022) and thus results in a single point of failure with the risks being propagated to the other downstream partners. The second possibility is that *Partner 1* transports the goods as promised in the SLA. From the perspective of ensuring accountability and providing visibility for proactive SCRM, blockchain fails in the first possibility as it cannot determine the correctness of the subjective assurances communicated by *Partner 1*. Therefore, it is important to validate the truthfulness and trustworthiness of *Partner 1's* subjective assurances to minimize the possibilities of fraudulent behaviours to avoid supply chain failure.
- *Making informed judgements about a partner's promise to be executed in the future:* In some cases, there will be a time lag between when the action specified in the SLA is executed by a partner and when its impact is realized by the other partners [21]. For example, *Partner 1* in the SLA promises on 19 May 2022 to deliver the goods progressively to *Partner 2* over a year, and the first batch of goods will be sent on the first Wednesday of September 2022. This clause refers to an action in the future, and existing PoW/PoS/PoA consensus algorithms can validate it on the first Wednesday of September 2022. However, from the perspective of proactive SCRM, it is important to validate the SLA on 19 May 2022 in terms

of *Partner 1's* (1) capacity and (2) its level of earnestness to commit to the contract. Without verifying *Partner 1's* ability on these points before forming a contract, there is a high possibility of this contract failing. Existing blockchain models do not assist in determining the capacity of a partner to commit to what is promised when subjective information is involved. To address this, the ability of a partner to be truthful and trustworthy when subjective information is involved must be determined and used when forming an SLA.

1.2. Contributions of this article

We explain our proposed approach by which a partner's intention and capability (henceforth termed as ***Earnestness***) to fulfil a subjective promise can be determined. Specifically, we propose **S**ubjective **I**nformation **A**uthenticity **E**arnestness **F**ramework (SIAEF) as an overarching framework that uses **P**roof **o**f **E**arnest ness (PoE) as a consensus algorithm in determining a partner's earnestness in committing to the subjective information. The partner's earnestness or trustworthiness value in committing to the subjective information it communicates can be used by the other partners when deciding if they should form an SLA with it or not when subjective information is involved. We then demonstrate how the output of SIAEF can be used by the existing consensus PoW/PoS/PoA algorithm before the information, irrespective of it not having a digital footprint, can be encoded into a smart contract and executed in blockchain for proactive SCRM. To achieve this aim, we assume that the blockchain on which PoE is applied is secure from any P2P attacks and that at least 2/3 of ranking partners can respond by following the PoE consensus mechanism. Therefore, we assume that the underlying blockchain prevents Byzantine faults and oracle problems. PoE and SIAEF in combination with PoW/PoS/PoA will assist in:

- **Accountability:** PoE and SIAEF verify and validate the truthfulness of subjective information communicated by a partner. This will also assist in determining the partner's earnestness and trustworthiness to commit to that information and encode it into a smart contract. Such earnestness of a partner is transparent to all other partners thus providing a single source of truth and preventing fraudulent behaviour.
- **Providing stability and avoiding fraudulent behaviour :** By ensuring accountability, PoE will prevent opportunistic behaviour by a partner in the selected consortia of which it is a part by measuring the partner's global legitimacy in communicating authentic subjective information. This will motivate a partner to maintain its efforts to commit to the subjective information communicated in every consortium thereby facilitating the sustainability of the distributed ledger environment.
- **Ensuring privacy and transparency:** In existing blockchain-based applications, a zero-knowledge proof is used to preserve the privacy of information without revealing its digital footprint [22]. However, this works only for objective information and fails in scenarios where subjective information is present. SIAEF addresses this and records the earnestness value of a partner at two different levels, namely (1) the permissioned level: to which only the members of the supply chain have access, and (2) the permissionless level: to which any users in SIAEF have access. The permissioned level stores detailed information about an SLA and the partner's performance in it which can be seen only by the members of the supply chain. It is similar to the concept "blockchain of blockchains" as an interoperable blockchain platform to ensure data integrity from the private to consortium level [23]. The permissionless level only stores abstract information about the partner and is visible to any users of SIAEF to determine the trustworthiness value of the partner for potential partnership selection. In this way, SIAEF ensures a high level of transparency as a nature of the blockchain-based application with a high level of privacy as the nature of a supply chain.
- **Fairness:** SIAEF ensures that a new participant joining the blockchain consortium has an equitable chance to prove its earnestness. Existing mechanisms depend on reputation-based approaches to ascertain a partner's credibility. This may negatively impact a new partner in forming SLAs with others as it does not have a past transaction history. SIAEF addresses this by determining the partner's average earnestness score to commit to the subjective information that it communicates.
- **Integrable:** SIAEF integrates PoE with other consensus mechanisms such as PoW or PoS. This ensures that an SLA that has both subjective and objective clauses can be formalized as a smart contract and executed in a blockchain-based environment.

1.3. Organization of the article

We present the working of SIAEF and PoE in 6 sections. Section 2 presents the working logic of the architecture of PoE and SIAEF. Section 3 explains how SIAEF identifies clauses from an SLA whose commitment needs to be validated by subjective information. In Section 4, we explain how the PoE consensus mechanism and SIAEF enable the legitimacy of a partner in communicating subjective information. Section 5 showcases the application of PoE and SIAEF in a real-world blockchain-based environment. Related work from the literature on PoE and SIAEF is presented in Section 6. Finally, Section 7 concludes the paper.

2. PoE and SIAEF

2.1. The working logic of PoE

As explained in Section 1, to avoid any fraudulent and non-compliant behaviour for proactive SCRM, we consider *Earnestness* as the trustworthiness of a partner that represents its intention and capability to fulfil a promise made. As mentioned in Anderson and Weitz [24], this can be measured by the partner's: *(1) track record:* its past relationship history as an indication of its capability to commit to the promises made; *(2) proactiveness:* how did the partner respond to the risk terms which were brought to its attention and which had the potential to impact its commitment to what it had promised; and *(3) communication:* the extent to which the partner kept the other partners of the supply chain informed about either its ability or inability to commit to what it had promised. For example, consider the scenario discussed in Section 1 where *Partners 1, 2, 4 and 9* form a supply chain. In the SLA formed on 19 May 2022, *Partner 1* committed to delivering the goods to *Partner 2* over a year, and the first batch of the goods was sent on the first Wednesday of September 2022. In this scenario, *Partner 1* is the *partner responsible* for committing to the promise whereas *Partners 2, 4 and 9* are the *ranking partners* who will determine *Partner 1's* earnestness score. PoE assists the ranking partners in determining the responsible partner's earnestness score using the following steps [25]:

- *Step 1: Enable the responsible partner to recommit to what they have promised*: This step starts the process of encoding subjective information from the SLA to a smart contract which can then be implemented in a blockchain. PoE

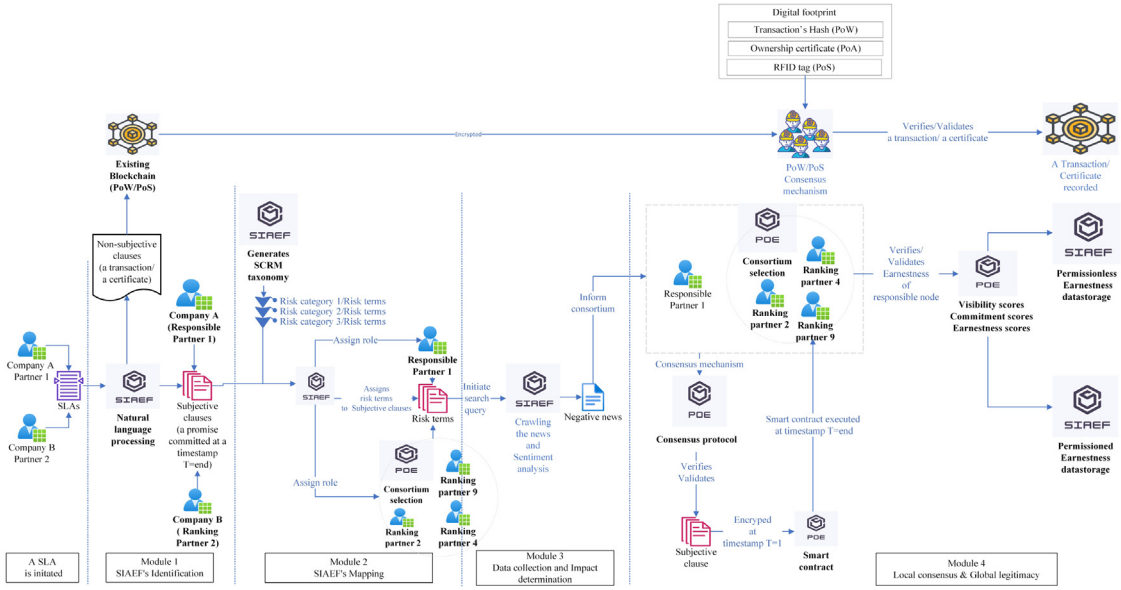

Fig. 2. Working of PoE and SIAEF to determine the earnestness of subjective information.

achieves this goal according to its operational philosophy of encouraging the responsible partner to first recommit to what has been defined as subjective information in the SLA. It does this by (a) identifying the subjective clauses from the SLA to which the responsible partner needs to commit, (b) determining the operational risk term/s which may have the potential to impact the responsible partner's commitment to what it had promised, (c) collate real-world occurrences of the identified operational risk terms and bring it to the attention of the responsible partner, and (d) note the response of the responsible partner, which can either be to recommit to what it promised earlier or change its response based on the real-world occurrences brought to its attention in (c).

- *Step 2: Determine the adherence of the responsible partner to what they have recommitted to*: This step of PoE measures the extent of the responsible partner's commitment to the promises made and computes its *earnestness score*. The earnestness score of a partner is a combination of its (1) *commitment score*, and (2) *visibility score*. The *commitment score* determines if the responsible partner committed to what it promised in the SLA. In contrast, the *visibility score* captures the extent to which the responsible partner kept the other partners of the supply chain updated about its progress in committing to the promise made in the presence of risk terms brought to its attention. From the perspective of proactive SCRM, this is important as it lets the other supply chain members determine if they will receive their resources as expected. The *earnestness score* represents the history of the responsible partner's earnestness.
- *Step 3: Achieve consensus from the ranking partners on the responsible partner's commitment to the subjective information before encoding it in a smart contract*: This step of PoE digitizes the communication between the responsible and the ranking partners in Steps 1 and 2 along with the commitment of the responsible partner to the promises made. It then achieves consensus from the ranking partners on the responsible partner's commitment to the subjective clauses. This consensus is recorded in the blockchain, which then acts as a single source of truth to represent the capability of the responsible partner to commit to its promises. The earnestness of the responsible partner in committing to subjective information can then be encoded in a smart contract and executed in a blockchain.

To achieve PoE's objective of encoding subjective information in blockchains, we propose the SIAEF, as explained in the next subsection.

2.2. SIAEF's working process

As shown in Fig. 2, SIAEF has four modules that integrate PoE in its working and determine a responsible partner's earnestness in communicating subjective information. The modules and their workings are as follows:

Module 1: Identification module analyses the SLA and identifies those clauses where a commitment has to be verified by subjective information. For example, suppose the SLA is formed on 14 April 2022 and has a clause *"Partner 1 should transport its manufactured goods to Partner 2 on 18 May 2022"*. In this case, it is identified as a subjective clause by SIAEF and moved to Module 2 for further analysis. This is because from 14 April 2022 to 18 May 2022, Partner 1 is giving a subjective commitment that it is on track to transport the goods without any digital footprint. As shown in Fig. 2, if the clause is *not* classified as a subjective clause, it will be encoded in the smart contract and executed using the existing PoW/PoS/PoA consensus algorithms.

Module 2: Mapping module achieves PoE's aim of determining the operational risk term/s which may potentially prevent the responsible partner from committing to what it had promised. It does this by first building a customized taxonomy of operational risk terms in SCRM. From this taxonomy, SIAEF, for each subjective clause, determines the risk terms which can prevent the responsible partner from committing to its promise. For example, in the above-mentioned subjective clause, SIAEF's mapping module from the generated SCRM taxonomy assigns *labour strike* as the risk term that could potentially impact the responsible partner's manufacturing and hence prevent it from being able to deliver what it had committed to. The detailed working of SIAEF's mapping module is explained in paper [25]. The identified risk term is used further in the next module.

Module 3: Data collection & impact determination module achieves PoE's aim of finding the identified risk terms by collating its real-world occurrences in the geographic region of interest. In other words, this module will gather real-time news related to the identified risk term (from SIAEF's mapping module) through an automated web crawler and bring it to the attention of the

Table 1
Notations.

Notation	Description
x	A service-level agreement (SLA) x signed between two partners
X	Total number of SLAs that responsible partner A has been formed in SIAEF
Cl_j	Clause j in SLA x
Sc_j	Subjective clause number j
Responsible partnerA	Is a partner in SIAEF and is defined as a responsible partner for a subjective clause j
Ranking partner$_i$	Is a partner in SIAEF and is defined as a ranking partner to assess the earnestness of the responsible partner.
R_j^A	Risk terms found by SIAEF's Module 2 related to responsible partner A and subjective clause j
Negative News$_j^A$	News with negative impact found by SIAEF's Module 3 on subjective clause j
$flag_j^A$	A flag label of the subjective clause j related to responsible partner
greenflag	Assigned to the subjective clause for which SIAEF found the presence of risk terms that may prevent the responsible partner from committing to a subjective clause. The responsible partner agrees to change the subjective clause and achieves consensus on its new subjective clause.
yellowflag	Assigned to the subjective clause for which SIAEF's Module 3 found news articles relevant to its identified risk term but the responsible partner does not want to change its initial SLA commitment and is still positive about meeting it.
blueflag	Assigned to the subjective clause for which SIAEF's Module 2 did not find any relevant risk terms or for which SIAEF's Module 3 did not find any news articles relevant to its identified risk term.
$\overline{Vi_j^{A,x}}$	The average visibility score of responsible partner A, SLA x, subjective clause j
$Vi_{i,j}^{A,x}$	Visibility score of responsible partner A, SLA x, clause j given by partner i
$\overline{Com_j^{A,x}}$	The average commitment score of responsible partner A, SLA x, subjective clause j
$Com_{i,j}^{A,x}$	The commitment of responsible partner A, SLA x, subjective clause j given by ranking partner i
$Vi_j^{A,x}$	Visibility score of responsible partner A, SLA x, subjective clause j
$Com_j^{A,x}$	Commitment score of responsible partner A, SLA x, subjective clause j
$E_j^{A,x}$	Earnestness score of responsible partner A, SLA x and subjective clause j
E^{A}	Total earnestness score of responsible partner A of X SLAs
E'^{A}	Average earnestness score of responsible partner A per each subject
E_{i,j,T_0}^{x}	Earnestness score of partner i SLA x, clause j at initial time T_0
E'^{x}_{i,j,T_0}	Average earnestness score of partner i, SLA x clause j at initial time T_0
T_1	Time stamp when the subjective clause is encoded in the smart contract
T_0	Time stamp when SLA is initiated
M	Total number of subjective clauses in X SLAs
I	Total number of partners in SIAEF

responsible partner. Continuing with the above example, after the labour strike is identified as a risk factor to the subjective clause, SIAEF forms a query [*Labourstrike* + *Partner* 1] to collate real-time news articles which include this risk term. It also determines the sentiment of the news articles related to the risk term and considers it as their impact. This analysis is used further in Module 4.

Module 4: Local consensus and global legitimacy module achieves two of PoE's aims, namely (a) based on the real-world articles brought to its attention, to ask the responsible partner to either recommit to what it promised earlier or change its response and (b) to determine the responsible partner's adherence to what it had recommitted to. Aim (a) is achieved by showing the shortlisted news articles from Module 3 to the responsible partner with an option for it to either recommit to its promise made in the SLA or change it. This response is encoded in the smart contract after consensus from the ranking partners. After the execution of the subjective clause, PoE's aim (b) is achieved by the ranking partners who determine the responsible partner's earnestness in committing to the subjective information it had promised. Continuing with the example, SIAEF, using the information determined for *labour strike* in Module 3, asks *Partner 1* to either recommit to its promise made in the SLA or change it. The response from Partner 1 is encoded in the smart contract after achieving consensus from the ranking partners. After the timestamp of the subjective clause's execution (18 May 2022), the ranking partners (*Partner 2, 4 and 9*) will submit responses to rank the responsible partner on its (1) *commitment score*; and (2) *visibility score*; which is used to determine its *earnestness score*. Such communication generated by PoE between the responsible and the ranking partners in achieving aims (a) and (b) will be digitized and stored in the blockchain to ensure the highest level of visibility and traceability. PoW/PoS/PoA can then use this digitized information as the digital footprint of *Partner 1*'s *visibility*, *commitment* and *earnestness scores*, which can then be recorded in an immutable block in the blockchain as shown in Fig. 2. These values can be accessed by different partners as *Partner 1's* earnestness in committing to subjective information and using it when forming an SLA with it which involve subjective clauses.

Fig. 2 shows how PoE and SIAEF assist in generating a digital footprint of subjective information, which PoW/PoS/PoA can then use to encode it in the blockchain. The working of SIAEF's Module 2 and Module 3 has been explained in the paper [25]. This paper focuses on how those modules integrate with Module 1 and Module 4 of the SIAEF. The working of SIAEF's Module 1 (identification module) and Module 4 (local consensus and global legitimacy module) are demonstrated in Sections 3 and 4, respectively. From the perspective of PoE's applicability, we show SIAEF as a decentralized application (Dapp) in Section 5. And the notation used in the paper is summarized in Table 1.

3. SIAEF's identification module

SIAEF's Identification module divides each clause of an SLA into two parts, namely the *conditional* and *actionable* parts. The conditional part of the clauses lists the obligations to be met to validate the agreement. The actionable part of the clauses lists the actions to implement once the conditions are met. This module focuses on the actionable part of the clauses as it represents the commitment required from the responsible partner. As the SLA's clauses are in an unstructured form, the identification module applies rule-based classification with the application of NLP to automate the process of subjective clause identification. The series of steps in this automated process is as follows:

- *Clause Pre-processing:* StandfordNLP package with attribute 'Pipeline' is used to pre-process the SLA's clauses. As shown in Algorithm 1, the first step is to clean each clause to remove the Unicode characters (line 10), then split the text

into a list of words (tokenization - line 11), lemmatize each word to remove any inflectional form to be a lemma (line 12) and attach PoS (part-of-speech) tagging to each word to indicate whether it is a noun or verb (line 13). This is then used in the next steps.

- *Determine if the clause has a measurable value to assess its completeness:* This step determines if the clause has a metric (for example, time or date) for its completeness (lines 5 and 15). If it has, then it will be considered further or else it will be omitted from further analysis.
- *Determine which actionable clauses are non-verifiable:* This step determines which actionable clauses cannot be verified directly by the PoW/PoS/PoA for their commitment and thus need verification from external sources. This is done by checking if they have a model verb or future tense present in the clause (lines 6 and 16). This means that the clause cannot be verified by existing information and thus cannot be considered by PoW/PoS/PoA. These need to be considered and verified by PoE.
- *Determine if the conditional part of the clause needs to be verified for commitment by subjective sources*: In this step, the StandfordNLP package in Python is utilized to first check if the clause has any conditional terms such as ['if', 'unless', 'until', 'upon'] (lines 7, 17–19) or connection words, such as ['as', 'as soon as', 'in the event'] (lines 8,25–27). If so, then the clause's commitment can be verified with objective sources. Such parts of the clauses will be omitted from further analysis by PoE, and they will be sent to PoW/PoS/PoA for further processing. The remaining clauses are those where the commitment needs to be verified by subjective sources, a task in which PoE will assist. Therefore, with this determination, if a clause contains commitments that need to be verified by both objective and subjective information, the objective part of the clause will be sent to PoW/PoS/PoA for encoding in the smart contract, and the subjective part will be analysed further with PoE.
- *Determine the responsible partner and the commitment to be made in the actionable part of the clause:* This step determines the specific commitment that needs to be made in the subjective clause (lines 20 and 28). Furthermore, if subjective clauses contain a list of nouns (defined in line 4), they will be determined as the owner of the action who will be responsible to conduct the commitment identified, such as *Partner 1* (lines 21–23, 29–31).

To determine the accuracy of SIAEF's identification module in correctly identifying subjective clauses from an SLA, we use the cross-validation method where we compare the results given by the SIAEF's identification module (as subjective clauses of an SLA) with the ones that were classified manually by the two experts. In the manual process, each clause was given a value of either 1 or 0 by each expert. A score of 1 suggests that the experts considered the clause to be a subjective one whereas a score of 0 suggests otherwise. If both the experts ranked the clause as 1, only then is it considered a subjective clause. Table 2(a) represents the scoring statistics by the experts on a database of 82 clauses. To evaluate the level of agreement between the two experts, Cohen's Kappa coefficient (k) [26] is computed as shown in Table 2(b).

For cross-validation, we tested SIAEF'S identification module's automated output with that of the manual process. We did this by categorizing the automated output as follows:

- True Positive (TP) $\rightarrow$ means that the clause identified by SIAEF as a subjective clause is consistent with that of the manual process undertaken by the experts;

Table 2
The experts' level of agreement in assessing the subjective clauses.

(a) Scoring statistics

Scoring metrics	Clauses
Both experts score 1	15
Both experts score 0	67
Expert 1 scores 1 Expert 2 scores 0	0
Expert 1 scores 0 Expert 2 scores 1	0

(b) The degree of agreement

Level of agreement	Coefficient
Probability of agreement (p_o)	1
Probability of random agreement (p_e)	0.74
Cohen's Kappa coefficient (k)	1

Table 3
Performance metrics of SIAEF's automated identification.

Factor	Number	Metric	Metric's Score
TP	15	a	0.99
TN	66	p	0.94
FP	1	r	1
FN	0	$F1$	0.97

- True Negative (TN) $\rightarrow$ means that the clause is not identified by SIAEF as a subjective clause which is consistent with that of the manual process undertaken by the experts;
- False Positive (FP) $\rightarrow$ means that the clause is identified by SIAEF as a subjective clause which is incorrect as it was not identified as one in the manual process undertaken by the experts;
- False Negative (FN) $\rightarrow$ means that the clause is not identified by SIAEF as a subjective clause which is incorrect as it was identified as one in the manual process undertaken by the experts.

On the classified results, we computed the *accuracy* (a), *precision* (p) and *recall* (r) metrics as shown in Table 3. It can be seen that the a of the automated process is 99% while the p is 94%. Only one out of the 82 clauses classified by SIAEF's identification module was inconsistent with that of the experts. The (r) of the model is 100%, meaning that all subjective clauses are identified by SIAEF's identification module. Therefore, the $F1$ score is high at 97%. These results show that the SIAEF's identification module is a good classifier to identify the subjective clauses in the SLA. This information is used in SIAEF's Modules 2 and 3 before achieving consensus in Module 4, as explained in the next section.

4. SIAEF'S local consensus and global legitimacy module

As discussed earlier, this module of SIAEF uses PoE to achieve the ranking partners' consensus on the responsible partner's commitment to the subjective clause. Such consensus verifies the extent of the subjective clause's commitment by the responsible partner and digitizes it into a smart contract. This process consists of many steps as follows:

4.1. Step 1: Selection of ranking partners and PoE consensus protocol

To initiate the consensus process, we select the ranking partners and define the consensus protocol as follows:

- **Selection of ranking partners**: As defined in Algorithm 2 (lines 1 and 2), if a partner is part of the supply chain and is not a responsible partner for that clause, then it is eligible to be selected as a ranking partner. In scenarios

Algorithm 1: SIAEF subjective identification

Require: *standfordnlp*('*en*'), Cl_j
Ensure: Sc_j
1: $Sc_j \leftarrow False$
2: $cws1 \leftarrow$ list of connection words
3: $vb \leftarrow$ ['*VBZ*','*VBN*']
4: $nn \leftarrow$ ['*NN*','*NNS*','*NNPS*','*NNP*']
5: $mdvb \leftarrow$ list of model verbs
6: $nr \leftarrow$ list dates, numbers, currency
7: $cd1 \leftarrow$ ['if', 'unless', 'until', 'upon']
8: $cd2 \leftarrow$ ['as', 'in', 'as soon as', 'in the event']
9: **for** i in range(0,*len*(*Cl*)) **do**
10: $cleanCl_j \leftarrow$ cleantext(Cl_j)
11: $tokenCl_j \leftarrow$ tokenize(Cl_j)
12: $lemCl_j \leftarrow$ lemmatize(Cl_j)
13: $lemCl_j.pos \leftarrow$ pos($lemCl_j$)
14: $Sc_j \leftarrow$ "False"
15: **if** $lemCl_j.words$ in nr **then**
16: **if** $lemCl_j.pos$ in vb and $mdvb$ **then**
17: **if** $lemCl_j.words$ in $cd1$ **then**
18: remove chunk of word after $lemCl_j.words$ in $cd1 \rightarrow$ PoW/PoS/PoA
19: $Sc_j \leftarrow$ "True"
20: **return** commitment $\leftarrow Sc_j$
21: **if** $lemCl_j.pos$ in nn **then**
22: *responsiblepartner* $\leftarrow$ True
23: **return** *responsiblepartner*
24: **end if**
25: **else if** $lemCl_j.pos$ in $cd2$ **then**
26: remove chunk of words after $lemCl_j.words$ in $cd1 \rightarrow$ PoW/PoS/PoA
27: $Sc_j \leftarrow$ True
28: **return** commitment $\leftarrow Sc_j$
29: **if** $lemCl_j.pos$ in nn **then**
30: *responsiblepartner* $\leftarrow$ True
31: **return** *responsiblepartner*
32: **end if**
33: **end if**
34: **end if**
35: **end if**
36: **end for**

when the supply chain has limited partners, it will need external partners who are not a part of the supply chain to be the ranking partners. In such cases, those partners who have a positive *total earnestness score* (E^i) and a positive *average earnestness score* (E'^i) are eligible to be selected as ranking partners. The higher the E'^i, the higher the possibility of that partner being selected as a ranking partner. The selected ranking partners will establish a consortium to verify and validate the responsible partner's commitment to the subjective clause as promised.

- **How is consensus on the responsible partner's commitment to the subjective clause achieved?**: When a majority (at least 2/3) of ranking partners in the consortium agree, consensus on the responsible partner's commitment to the subjective clause is achieved (lines 12–26).
- **Initialization**: After the selection of the responsible and the ranking partners for each subjective clause, PoE initiates the process by assigning a score of 0 to each responsible partner for the *visibility score* (Vi^x_{i,j,T_0}), *commitment score* (Com^x_{i,j,T_0}), and *earnestness score* (E^x_{i,j,T_0}) and *average earnestness score* (E'^x_{i,j,T_0}) (lines 5–7).

4.2. Step 2: Assigning a flag to each subjective clause based on the responsible partner's response

As discussed in Sections 2.1 and 2.2, for each subjective clause, SIAEF's Module 2 identifies the risk term/s which may have the potential to prevent the responsible partner from committing to what it had promised. Module 3 collates the real-world occurrences in the geographic region of interest for this risk term. This is then shown to the responsible partner for it to either recommit to what it had promised in the SLA or change it. The ranking partners use this analysis to determine the responsible partner's adherence to its promises and accordingly determine its *commitment* ($Com^{A,x}_{i,j}$) and *visibility* ($V^{A,x}_{i,j}$) scores. The scores used to measure the commitment and visibility of the responsible partner are explained later. To assist the ranking partners in this process, as shown in Algorithm 3, SIAEF's Module 4 assigns a flag (either blue, yellow or green) to each subjective clause, as follows:

- Blue flag: A blue flag is assigned to a subjective clause for which SIAEF's Module 2 did not find any risk terms relevant

Algorithm 2: PoE protocol

Protocol for earnestness consortium selection
To join the PoE Consortium to verify the subjective information when an SLA is formed

1: The partners in the SLA are the default responsible partner and the ranking partners for consensus

For the partners which are not the partner in the SLA
2: Partner i should have $E'^i > 0$ and $E^i > 0$ as it is verified by PoE as $Partner_i$ for $i \in I$ and $I \geq 2$

Initiate SIAEF
3: The SIAEF is active when there are at least two partners joining with an SLA x
4: Initiate SLA x at T_0
5: $Vi^x_{i,j,T_0} \leftarrow 0$, $Com^x_{i,j,T_0} \leftarrow 0$, $E^x_{i,j,T_0} \leftarrow 0$, $E'^x_{i,j,T_0} \leftarrow 0$ for $i \in I$ and $I \geq 2$
6: **for** j in range (0,len(x)) **do**
7: Identify subjective clause (Sc_j)
8: **end for**
9: z=0
10: y=0
11: **for** $i \in I$ and $I \geq 2$ and j in range (0,len(x)) **do**
12: Sc_j=False
13: **if** $Partner_i$ is verified by PoE **then**
14: $y = y + 1$
15: $Partner_i$ is selected to join the consortium consensus
16: **if** Sc_j=True **then**
17: $z = z + 1$
18: **end if**
19: **end if**
20: **end for**
21: **for** j in range (0,len(x)) **do**
22: **if** $\frac{z}{y} \geq \frac{2}{3}$ **then**
23: Sc_j=True
24: Cl_j is recorded in Smartcontract at T_1
25: **end if**
26: **end for**

to the subjective clause or SIAEF's Module 3 did not find any news articles relevant to its identified risk term. This means there is a high possibility that the responsible partner will commit to what it promised. The ranking partners will note and record this response on the blockchain (lines 12–16 of Algorithm 3).

- Yellow flag: A yellow flag is assigned to a subjective clause for which SIAEF's Module 3 found news articles relevant to its identified risk term. However, the responsible partner does not want to change its initial SLA commitment and is still positive about meeting it. In other words, the responsible partner recommits to the commitments defined in the SLA despite the information being shown. The ranking partners will achieve consensus on the responsible partner's response and record it on the blockchain (lines 3–8).
- Green flag: A green flag is assigned to a subjective clause for which SIAEF's Module 3 found news articles relevant to its identified risk term. The responsible partner wants to change its commitment in response to this. In such cases, the consensus among the ranking partners is achieved on the modified expectations before recording the modified SLA on the blockchain. This signals to the other supply chain partners the modified commitments from the responsible partner and the changes to their operations according to the modified SLAs (lines 9 to 10). After the time stamp of either the initial or the modified commitment (depending on whether the SLAs were changed or not), SIAEF's Module 4 determines if the responsible partner had committed to its expectations to assign it with a $Com_{i,j}^{A,x}$ and $V_{i,j}^{A,x}$ score. Suppose the responsible partner chooses not to modify the initial SLAs (yellow flag) and adheres to them. In this case, it should be given a higher $Com_{i,j}^{A,x}$ and $V_{i,j}^{A,x}$ values compared to what it would have been given if it had chosen to modify the initial SLAs and adhered to it (green flag). Conversely, suppose the responsible partner chooses not to modify the initial SLAs (yellow flag) and does not commit to it. In this case, it should be given a higher penalty in its $Com_{i,j}^{A,x}$ and $V_{i,j}^{A,x}$ value based on what it would have been given if it had chosen to modify the initial SLAs (green flag) and does not adhere to it. The process of determining the $Com_{i,j}^{A,x}$ and $V_{i,j}^{A,x}$ values is explained in the next subsection.

Algorithm 3: Local consensus flag algorithm

Require: R_j^A, Cl_j and $NegativeNews_j^A$
Ensure: $Vi_i^A j$, $Com_i^A j$ and $E_i^A j$

```
1: for j in range(0,M) do
2:   clause=Cl_j
3:   if R_j^A is not Null then
4:     if NegativeNews_j^A is not Null then
5:       newclause=newclause
6:       if newclause==clause then
7:         flag_j^A='yellow'
8:         clause_j=newclause
9:       else
10:        flag_j^A='green'
11:      end if
12:    else
13:      flag_j^A='blue'
14:    end if
15:  else
16:    flag_j^A=='blue'
17:  end if
18: end for
```

4.3. Step 3: Ascertaining commitment ($Com_{i,j}^{A,x}$) and visibility ($V_{i,j}^{A,x}$) scores of the responsible partner

4.3.1. Determining the ($Com_{i,j}^{A,x}$) value of the responsible partner

To determine the commitment score ($Com_{i,j}^{A,x}$) of the responsible partner, the ranking partners, after the execution of the subjective clause's time stamp, need to ascertain if the subjective clause has been met or not as promised. If it has been met, then the responsible partner will be assigned a positive ($Com_j^{A,x}$) value. On the other hand, if the commitment defined in the subjective clause has not been met, the responsible partner will be given a negative ($Com_j^{A,x}$) value. As mentioned in Algorithm 4, the intensity of the ($Com_j^{A,x}$) value which the responsible partner would be given for a subjective clause depends on the flag assigned to it, as follows:

Algorithm 4: Local commitment

Require: partner *i*, Clause *j*, Responsible partner *A*, Contract*X*
Ensure: $Com_{i,j}^{A,x}$

```
1: Com_{i,j}^{A,x} ← 0
2: Q ← 'A met its commitment'
3: for i in range(0,n) do
4:   if flag_j^A=='blue' then
5:     if Q is True then
6:       Com_{i,j}^{A,x}= Com_{i,j}^{A,x}+5
7:     else
8:       Com_{i,j}^{A,x}= Com_{i,j}^{A,x}-5
9:     end if
10:  else if flag_j^A=='yellow' then
11:    if Q is True then
12:      Com_{i,j}^{A,x}= Com_{i,j}^{A,x}+50
13:    else
14:      Com_{i,j}^{A,x} = Com_{i,j}^{A,x}-50
15:    end if
16:  else if flag_j^A=='green' then
17:    if Q is True then
18:      Com_{i,j}^{A,x}= Com_{i,j}^{A,x}+25
19:    else
20:      Com_{i,j}^{A,x}= Com_{i,j}^{A,x}-25
21:    end if
22:  end if
23: end for
24: Send Com_{i,j}^{A,x}
```

- Blue flag: If the responsible partner meets its promised commitment, it will receive a commitment score of 5. On the other hand, if the responsible partner does not achieve its commitment, it will receive a commitment score of −5 (lines 4–8).
- Green flag: If the responsible partner meets its promised commitment, it will receive a commitment score of 25 (a higher reward than the blue flag). On the other hand, if it did not commit to the subjective term, it will receive a commitment value of −25 (a higher penalty than the blue flag) (lines 16–24). In this case, the reward and penalty in the commitment value of the responsible partner are higher than the blue flag. This is because, in this case, the responsible partner changed its commitment in response to the news about its risk terms. So, if it commits to it, it will be rewarded more than the blue flag. Similarly, it will be given a higher penalty than the blue flag if it did not commit to it.
- Yellow flag: If the responsible partner meets its promised commitment, it will receive a commitment score of 50 (a

higher reward than the blue and green flags). On the other hand, if it did not commit to the subjective term, it will receive a score of −50 as its commitment score (a higher penalty compared to the blue and green flags) (lines 8 to 15). In this case, the reward and penalty in the commitment value are higher than the green flag. This is because, as opposed to the green flag, in this case, the responsible partner did not change its commitment in response to the news about its risk terms. So, if it commits to the subjective clause, it will be given a higher reward than the green flag. Similarly, if it did not commit to the subjective clause, it will be given a higher penalty than the green flag because the responsible partner had a chance to change its commitment. Still, it chose not to and did not commit to its promises.

4.3.2. Determining the ($V_{i,j}^{A,x}$) value of the responsible partner

As with the commitment score ($Com_{i,j}^{A,x}$) of the responsible partner, its Visibility ($V_{i,j}^{A,x}$) score is determined by the ranking partners. As discussed in Section 2.1, the ($V_{i,j}^{A,x}$) score captures the extent to which the responsible partner kept the other partners of the supply chain updated about its progress in committing to the promise made. As detailed in Algorithm 5, the ranking partners determine the ($V_{i,j}^{A,x}$) score for the responsible partner in each subjective clause for which it is responsible in a range of −12 to +12. This score is assigned by each of the ranking partners to the responsible partner in each subjective clause for which it is responsible after checking the responsible partner's performance in two different criteria and according to the flag (red, blue or green) assigned to that clause. For every criterion, the responsible partner's performance is evaluated as a 'Yes' or 'No' by the ranking partners and based on this, the following corresponding score is assigned. The criteria are as follows:

- **Criterion 1: When there are no risk terms, did the responsible partner keep the ranking partners updated about its progress in meeting its commitments? (Q1)** This criterion considers that either no risk term/s has been identified by SIAEF's Module 2 or no negative news related to the risk term/s has been identified by SIAEF's Module 3 as impacting the responsible partner's commitment to the subjective clause. As discussed in Section 4.2, the subjective clause is assigned a blue flag in such cases. Despite this, this criterion checks if the responsible partner kept the other members of the supply chain updated about its progress in relation to the positive aspects and their impact in committing to what it promised. As shown in Algorithm 5 (lines 6–8), if the responsible partner kept other supply chain partners informed, it receives a visibility score of 3. On the other hand, if the responsible partner does not keep the other supply chain partners informed, it receives a visibility score of −3 (lines 9–11).
- **Criterion 2: When risk terms are present, to what extent did the responsible partner keep the ranking partners updated about its progress in meeting its commitments?** This criterion considers that SIAEF's Module 2 has identified risk term/s and relevant negative news found by SIAEF's Module 3 as impacting the responsible partner's commitment to the subjective clause. In such cases, the subjective clause is assigned either a green or yellow flag depending on the responsible partner's response. Thus, from the perspective of SCRM, this criterion measures the extent to which the responsible partner kept the other supply chain members updated about its progress in committing to what it promised. It does this by analysing the responsible partner's performance in terms of two sub-criteria, namely:
  1. Did the responsible partner keep the other supply chain members updated on the positive and the negative (risk) factors that impact its commitment to the subjective clause? (Q2) AND
  2. In keeping the other members of the supply chain informed about the risk factors, did the responsible partner also communicate a backup plan that it intends to take if the risk factor/s identified in Module 2 is realized and impacts its ability to meet the commitment defined in the subjective clause? (Q3)

  The first sub-criteria determines if the responsible partner kept the supply chain members informed in not just the positive aspects of committing to what it promised but also how it is mitigating the impact of the identified risk term/s. The second sub-criteria determines if the responsible partner also communicated a backup plan which it will implement if the risk terms are realized. From the perspective of proactive SCRM, the performance of the responsible partner in these sub-criteria provides clarity to the other supply chain partners in achieving their goals and thus reduces the risk. As detailed in Algorithm 5, if the responsible partner satisfied only the first sub-criterion, it will receive a visibility score of 6 (lines 16–18) or 8 (lines 26–28) if the subjective clause was assigned a green or yellow flag, respectively. Similarly, if the responsible partner did not satisfy the first sub-criterion, it will receive a visibility score of −9 (lines 19–21) or −12 (lines 29–31), respectively. If the responsible partner satisfies the first and second sub-criteria, it will receive a visibility score of 9 (lines 12–15) or 12, respectively (lines 22–25).

4.3.3. Determining the earnestness and average earnestness score of the responsible partner

The *Com* and *Vi* scores of a responsible partner for a subjective clause j in an SLA x will be an average of the commitment ($\overline{Com_j^{A,x}}$) and visibility ($\overline{Vi_j^{A,x}}$) scores given by all ranking partners (Eq. (1) and (2)) respectively. The total earnestness score of a responsible partner for a subjective clause j in an SLA x is the sum of the average *Com* and *Vi* scores for that clause, as shown in Eq. (3). $E_j^{A,x}$ determined in Eq. (3) represents the total earnestness score of the responsible partner in the defined subjective clause. As explained in Sections 4.3.1 and 4.3.2, the $Com_j^{A,x}$ has a score range of [−50, 50], and the $Vi_j^{A,x}$ has a score range of [−12, 12]. Therefore, $E_j^{A,x}$, which is the sum of these metrics, has a score range of [−62, 62]. This scoring range defines a responsible partner's trustworthiness level in committing to a subjective clause. It is visualized in the SIAEF user interface (presented in Section 5). In other words, if the responsible partner is a member of different SLAs, then for each SLA, it will have a $E_j^{A,x}$ value as determined by the ranking partners. To represent the global earnestness value of the responsible partner, SIAEF uses two indicators: (1) total earnestness score (E^A) and (2) average earnestness score (E'^A). As shown in Eq. (4), E^A of a responsible partner is the sum of its earnestness scores in all X service-level agreements. Similarly, (E'^A) of a responsible partner, as shown in Eq. (5), is the average of its total earnestness score with the total subjective clauses of which it has been a part.

$$\overline{Com_j^{A,x}} = \frac{\sum_{i=1}^{n} Com_{i,j}^{A,x}}{n} \tag{1}$$

$$\overline{Vi_j^{A,x}} = \frac{\sum_{i=1}^{n} Vi_{i,j}^{A,x}}{n} \tag{2}$$

$$E_j^{A,x} = \overline{Vi_j^{A,x}} + \overline{Com_j^{A,x}} \tag{3}$$

Algorithm 5: Local SIAEF visibility scores of responsible partner A in clause j, contract X given by a ranking partner i

Require: ranking partner i, Clause j, Responsible partner A, Contract$X$
Ensure: $Vi_{i,j}^{A,x}$

$Vi_{i,j}^{A,x} \leftarrow 0$
$Q1 \leftarrow$ Responsible partner A kept ranking partner i updated on its progress
$Q2 \leftarrow$ Responsible partner A kept the other members of the supply chain updated on both the positive and the negative (risk) factors that impact its commitment to the subjective clause
$Q3 \leftarrow$ Responsible partner A communicated a back-up plan that it intends to take.
for i in range(0,n) **do**
  if $flag_j^A$=='blue' **then**
    if $Q1$ is True **then**
      $Vi_{i,j}^{A,x}$=3
    else
      $Vi_{i,j}^{A,x}$=-3
    end if
  else if $flag_j^A$=='green' **then**
    if $Q2$ is True **then**
      if $Q3$ is True **then**
        $Vi_{i,j}^{A,x}$=9
      else
        $Vi_{i,j}^{A,x}$=6
      end if
    else
      $Vi_{i,j}^{A,x}$=-9
    end if
  else if $flag_j^A$=='yellow' **then**
    if $Q2$ is True **then**
      if $Q3$ is True **then**
        $Vi_{i,j}^{A,x}$=12
      else
        $Vi_{i,j}^{A,x}$=8
      end if
    else
      $Vi_{i,j}^{A,x}$=-12
    end if
  end if
end for
Send $Vi_{i,j}^{A,x}$

$$E^A = \sum_{j=1}^{M} E_j^{A,x} \tag{4}$$

$$E'^A = \frac{E^A}{M} \tag{5}$$

These earnestness values assist the different partners in determining the trustworthiness of a responsible partner in committing to the subjective information for which it is responsible. This information can be used by the supply chain partners in forming an informed SLA with the responsible partner when subjective information is involved.

Remark 1 (*Accountability*)**.** E^A of a responsible partner in X SLAs (E^A) represents its accumulated earnestness effort across the different subjective clauses and SLAs since it joined SIAEF. The earnestness of a responsible partner in committing to the subjective information is proved by its continuous effort to maintain it over a period of time.

Remark 2 (*Fairness*)**.** E'^A represents the average earnestness score of a responsible partner for the total subjective clauses of which it has been a part. The purpose of this score is to ensure new responsible partners are not disadvantaged unfairly when new SLAs are formed in the presence of existing responsible partners. This may not be the case when only the E^A of a responsible partner is considered and if that partner has executed a higher number of SLAs or subjective clauses than a new responsible partner. Thus, the E'^A of a responsible partner per each subjective clause ensures fairness for the responsible partners forming SLAs.

4.3.4. Local and global legitimacy of the responsible partner's earnestness

Blockchains allow data to be stored data at either a public (permissionless) level or private (permissioned) level. As SCRM requires a high level of transparency and privacy, SIAEF stores the $Com_j^{A,x}$, $Vi_j^{A,x}$, E^A and E'^A of the responsible partner in two different levels as follows:

- **Local level (permissioned level)**: This level stores the detailed rankings given to the responsible partner on its commitment to the subjective clause. In other words, this level stores how each ranking partner scored the responsible partner in relation to the $Vi_{i,j}^{A,x}$ and $Com_{i,j}^{A,x}$ criteria related to the subjective clauses. These details can only be seen by the supply chain and the ranking members.
- **Global level (permissionless level)**: This level stores the cumulative scores of the responsible partner. In other words, this level stores the $Vi_j^{A,x}$, $Com_j^{A,x}$, E^A and E'^A scores. Any partner can see the scores of the responsible partner and use this to make an informed decision about forming an SLA with it.

Remark 3 (*Providing Stability and Avoiding Fraudulent Behaviour*)**.** By storing the E^A and E'^A scores of a responsible partner in a permissionless blockchain, SIAEF prevents opportunistic behaviours by that partner in a selected consortium of which it is a part. This will motivate the responsible partner to maintain its efforts to commit to the subjective information communicated in every contract for proactive SCRM.

Remark 4 (*Ensuring Privacy and Transparency*)**.** The earnestness metrics have regulated access at two levels, namely the local and global level. The data at the global level will be a trustworthy reference, albeit in abstract form, to verify and validate the reliability of a responsible partner in communicating subjective information in the supply chain. The data at the local level will also be a trustworthy reference in detailed form to check how the responsible partner performed in relation to each subjective clause and what rank the different ranking partners gave.

5. SIAEF as a decentralized application - DAPP

5.1. SIAEF/PoE development and its integration in existing block chains

To deploy SIAEF/PoE in a real-world blockchain environment, it was developed as a decentralized application (Dapp) and applied in an official test blockchain network, BSC Testnet. In this section, we demonstrate SIAEF's ability to work as a DAPP along

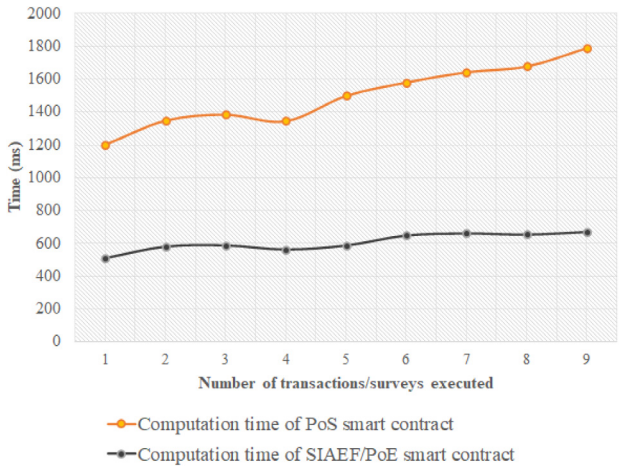

Fig. 3. Simulation on local host Ubuntu Hardhat network.

with the improvements it provides. Currently, no worldwide standard exists to validate and test the earnestness score of a responsible partner in relation to subjective information in a smart contract [27]. So, in our experiments, we base the results on the Ethereum testing standards to validate SIAEF/PoE's ability to record and determine the earnestness of a promise in relation to subjective information. As part of our validation, we evaluate SIAEF/PoE using the following criteria:

- **Integration test -** this test aims to determine the application of SIAEF/PoE in a local host.
- **System test -** this test aims to deploy SIAEF/PoE in the Testnet or development network to simulate its working in a product-like environment. This environment measures the performance of the smart contract and determines if there are any issues in SIAEF's working logic and functionalities.

5.1.1. Integration testing

Development environment. Integration testing provides the cost in terms of time to estimate the working of the algorithms. As there is no standard benchmark, the general rule of thumb is that the lower the computation costs, the more efficient it is. An HP EliteBook x360 830 G7 Notebook PC with Ubuntu 22.04, Intel(R) Core(TM) i7-10510U @1.80 GHz CPU and 953 GB RAM was used for testing in a local Ethereum network which is a Hardhat network. In this environment, we evaluated the working efficiency of the SIAEF algorithms by increasing the number of responses (surveys) submitted by different responsible partners. We simulated by increasing the number of surveys that increased the number of transactions executed in a standard Ethereum (PoS) smart contract. Fig. 3 shows that the computation costs to execute the SIAEF/PoE smart contract when the number of surveys was increasing is significantly less than an example of a standard token transaction between two partners using the PoS consensus mechanism. The computation time of PoS to record one token transaction costs 1080 ms but only takes 516 ms to record the ranking partners' responses using SIAEF/PoE. PoS takes 1790 ms to record a token transaction for ten transactions, whereas SIAEF/PoE in PoS takes 670 ms. So the transaction cost of SIAEF/PoE to determine the earnestness score of a responsible partner is 37% to 48% less than that of a token transaction in the existing blockchain, which uses PoS.

5.1.2. System testing

System testing is to measure or evaluate computation cost when the responsible and ranking partners deploy and execute a smart contract in a decentralized network. The computation costs include the gas used to process the transactions, which is measured as follows:

Table 4
Comparison of SIAEF/PoE gas consumption costs in two testing networks (Hardhat and BscScan).

SIAEF/PoE cost (gas consumption)	Hardhat	BscScan
Contract Deployment (contract creation)	2724778	2764999
Submit survey (contract call)	563505	612305

- **Gas used by transaction** (g_t) is the computational effort in operating a smart contract/transaction in an Ethereum blockchain;
- **Gas price** (g_p) is the price per unit of gas (g_t) which the user needs to pay to validate the transaction and record it in an Ethereum blockchain. Gas price is denoted in gwei. Gwei is a unit to measure the gas cost per cryptocurrency ether (ETH). One gwei is equal to 10^-9 ETH. As the development network is simulated, it can only estimate the gas transactions use. Gas prices are dynamic and are based on the real-time market. For the experiments we performed, we used the gas price of 03/03/2022. This is used to test the development (local host - Hardhat network) as a benchmark and compare it with the live network (implemented on 03/03/2022).
- **Transaction fee** (c_t) is also call a gas fee. This is the blockchain transaction fee that an end user pays to an Ethereum blockchain validator to immutably verify and record the transaction in a blockchain network. The transaction fee incentivizes Ethereum blockchain validators to stake their ETH and help secure the network. The transaction fee is calculated using the following formula:

$$c_t = g_t * g_p \tag{6}$$

As previously discussed, SIAEF/PoE is developed as Dapp and deployed in BSC Testnet. BSC Testnet is a peer-to-peer (block chain) network for developers to test the operation of a Dapp and is an Ethereum network that applies PoS as its consensus mechanism and BNB is its token. SIAEF/PoE generates the earnestness scores of a responsible partner. PoS in BSC Testnet uses these scores and the digital footprint generated by the communication between the responsible and ranking partners by SIAEF/PoE to encode the responsible partner's earnestness in committing to the subjective clauses. We compare the efficiency and effectiveness of BSC Testnet against the simulated Hardhat Network as the benchmark of an Ethereum network. Table 4 compares the gas consumption when executing SIAEF/PoE smart contracts on a local computer (Hardhat Network) and a virtual device (BscScan). The results show that the gas consumption of the local device (Hardhat) and the virtual device (BscScan network) are relatively in the same range, and there is a difference of only 3% with the BscScan network. Furthermore, regarding contract calls via Submit survey, the Hardhat network and BscScan consumed relatively the same amount of gas (8% of difference). Therefore, we chose BscScan Testnet as it provides an approximate estimate of gas consumption cost before executing transactions in a live Ethereum network to integrate SIAEF/PoE.

Table 5 compares the transaction fees incurred by the validator in the testing network to execute the SIAEF/PoE smart contract at a local computer (Hardhat network) and a virtual device (BscScan). The transaction fee is calculated based on gas consumption using Eq. (6). Table 5 shows that the transaction fee from Hardhat network gas consumption is 56 times higher than BscScan. This is because the Hardhat token is ETH which is 11 times costlier than BNB used in BscScan Testnet (ETH/USD = 2953.62 and BNB/USD

Table 5
SIAEF/PoE transaction fee in USD for two different testing networks (Hardhat and BscScan).

SIAEF/PoE cost (USD)	Hardhat	BscScan
Contract Deployment (contract creation)	417.00	7.43
Submit survey (contract call)	86.24	1.65

Table 6
SIAEF/PoE costs in BscScan Testnet Network.

SIAEF/PoE costs	Deployments	Submit a response
g_t	2764999	612305
g_p (gwei)	10	10
c_t (gwei)	27649990	6123050
c_t (BNB)	0.02764999	0.00612305
c_t (USD)	7.43	1.65

= 268.72) and the average gas price in an Ethereum network on the same day, 03/03/2022, (51.82 gwei) is 5 times more than the gas price in BscScan Testnet (10 gwei). This table shows that to verify a smart contract, choosing a virtual network with a token with a small exchange rate to USD will save costs for SIAEF/PoE members in a real-time blockchain network.

Table 6 shows the cost to operate SIAEF/PoE in a Testnet live network with the real-time market price. The results show that it only costs USD 7.43 for deployment and USD 1.65 for response submission.

Time consumption. SIAEF's simulation is run with an increasing number of responses from 0 to 12. The time taken to process each response is 3 s in the BSC Testnet platform. So, with 12 responses submitted by 12 different responsible partners, the total time needed to encode these responses is 39 s. The first three seconds set up the initial smart contract before the first subjective clause is encoded. This indicates delays in encoding a subjective clause in a block as it includes strings (ranking partner's responses) and numbers (earnestness scores computed). The processing time is acceptable as the transaction fee and gas cost (explained below) in processing each response is not high.

Gas Cost. For SIAEF/PoE deployment, the gas cost is 0.00000001 BNB (10 Gwei), and the transaction fee is 0.02764999 BNB ($7.43) to deploy a SIAEF/PoE smart contract. Furthermore, for each clause whose response needs to be processed and earnestness scores recorded, the gas cost is 0.00000001 BNB (10 Gwei), and the transaction fee is 0.00612305 BNB ($1.65). This is equal to the average gas price and transaction fees per transaction in BSC Testnet. This ensures the transaction pays enough fees to encode such subjective information in a block.

Remark 5 (*Integrable*)**.** SIAEF using PoE provides a truthful digital footprint of a responsible partner's commitment to subjective information. This can then be encoded in an existing blockchain with PoW/PoS/PoA.

5.2. SIAEF's user interfaces

SIAEF's global (permissionless level) and local (permissioned level) front-end dashboards are illustrated in Figs. 4–6 and 7 respectively. Brief details and the use of each dashboard are explained below:

- *Global dashboard*: Fig. 4 showcases the overall earnestness scores of all SIAEF's users. Any partner can use this dashboard to see a responsible partner's (1) E^A, (2) E'^A, (3) completion rate by SLA, (4) completion trend by SLA (which is the ratio of completed SLAs over the number SLAs executed by the responsible partner). It should be noted that from the perspective of a responsible partner, SIAEF considers an SLA as completed when all of the subjective clauses for which it was responsible are fulfilled (5) Completion rate by clauses (the ratio of completed subjective clauses over the number of subjective clauses executed across the different SLAs). The global dashboard informs SIAEF's partners (looking for potential partners with whom to form an SLA) with a transparent representation of the available responsible partners' earnestness overview as a single source of truth. This dashboard will also ensure fairness to new users of the framework. As shown in Fig. 4, Company D is a new user with a total earnestness score of 443, which is less than company E, which has a total earnestness score of 649. Despite this, it can be seen that Company D has a higher completion rate by SLA and subjective clauses. This illustrates that even though Company D is a new user, it has consistently performed better (thus exhibiting an upward trend) than Company E (thus exhibiting a downward trend).

Fig. 4. SIAEF's global dashboard.

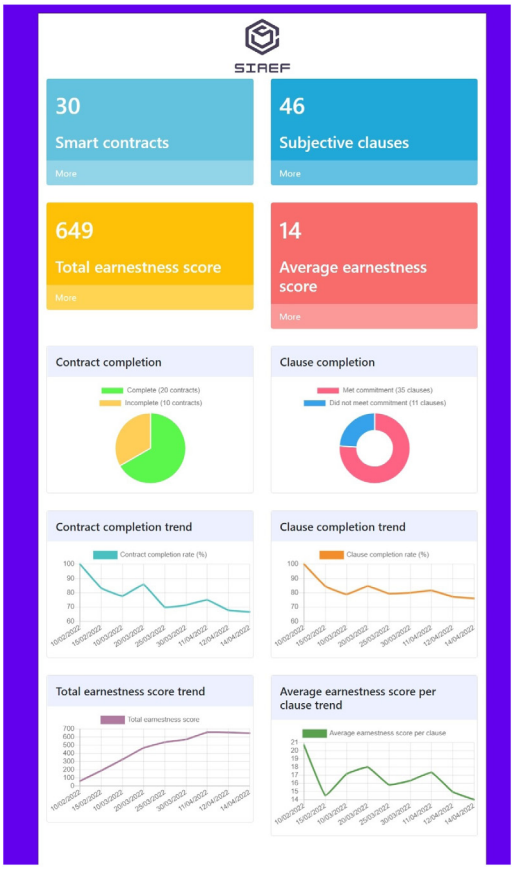

Fig. 5. SIAEF's Partner's detailed dashboard.

Fig. 6. Partner's history of committing to the subjective clauses.

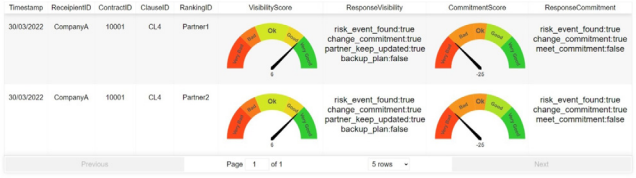

Fig. 7. SIAEF's local dashboard.

Thus, the global SIAEF dashboard provides equal opportunities to new users and encourages existing users to maintain their earnestness's stability in not only one contract but across the different contracts of which it is a part.

- *Partner's detailed dashboard*: For a partner, Fig. 5 provides a detailed track record of its earnestness to fulfil the promises made. As with the SIAEF's global dashboard, this information is accessible and visible to any partner in SIAEF. This dashboard shows the (1) X, (2) M, (3) E^A, (4) E'^A, and (5) contract and clause completion pie charts that show the number of completed/uncompleted contracts; and the number of completed/uncompleted subjective clauses. This dashboard also shows the time series trend of contract completion, clause completion, total trustworthiness score and average trustworthiness score per clause completed.
- *Partner's history of committing to the subjective clauses*: A SIAEF's partner may want to see a prospective responsible partner's detailed history in relation to their commitment to subjective clauses before forming an SLA with it. Fig. 6 shows a responsible partner's average visibility and commitment scores for each subjective clause. It also shows the responsible partner's total earnestness score as 'Very bad', 'Bad', 'Ok', 'Good' or 'Very Good' over the score range of [−62, 62], as explained in Section 4.3.3. The range ['Very bad', 'Bad', 'Ok', 'Good', 'Very Good'] is customized and depends on the need of SIAEF/PoE members. It was designed for visualization only.
- *Local dashboard*: This is SIAEF's permissioned dashboard at the local level. As discussed in Section 4.3.4, for a specific SLA, SIAEF only allows either the ranking or the supply chain partners to see the ranking given to the responsible partner. These are shown at the local level under the columns 'ResponseVisibility' and 'ResponseCommitment' of Fig. 6. These columns show the scores the ranking partners gave in the range of [−50, 50] for commitment and [−12, 12] for visibility, as explained in Section 4.3. Keeping this information permissioned ensures the highest level of transparency in showing a responsible partner's earnestness while at the same time respecting its privacy.

5.3. Security analysis

It is only possible for data leakage to occur in the proposed SIAEF framework during data transfers between the permissioned and permissionless levels. To ensure security and data storage at both permissioned and permissionless levels, SIAEF uses the blockchain of blockchains proposed by [23]. For example, Hyperledger Fabric is the permissioned blockchain to record the local earnestness score of the responsible partners. We use BscScan Testnet, an Ethereum network, as a permissionless blockchain in our implementation. The global earnestness score of the responsible partner is recorded at the permissionless level. Hence, within layers, data security will be maintained by Hyperledger and Ethereum. Each level contains a data communication process that transmits the genesis hash (GH), root hash (RH), local transaction signature (LTS), and block number (BN) of the previous layer to the next layer when a new block is added in the previous layer. To ensure security, all data transferred from one layer to the next layer are hashed using SHA-256. This means that a man-in-the-middle attack is not feasible within a limited time frame of 30 s, which is a reasonable transaction time. Therefore, we can confidently assert that using the concept of blockchain of blockchains will maintain the security of internal data stored in each layer [23]. Recently, quantum blockchain technology which can be used to ensure a high level of security has been proposed [28].

In addition to securing two levels of data transfers from outside attacks, the SIAEF framework also ensures security from an internal perspective to prevent fraudulent and opportunistic behaviours. As discussed in Section 1.2, fraudulent or opportunistic behaviour is common when a partner is a member of a different consortium. To demonstrate how SIAEF assists in avoiding this, we performed a rule-based behaviour simulation of five companies to compare their chances of forming a contract when their earnestness is regularly measured compared to one when their earnestness was not measured. The lavender line in Fig. 8 shows the number of SLAs that a company will form when SIAEF/PoE is not used. In this case, it can be seen that the chances of that company forming an SLA vary significantly as other companies do not know of its commitment to the subjective information it communicates. Fig. 8 shows the simulated performance of three companies, Companies B, C, and D, represented by the orange, grey, and yellow lines, respectively, whose earnestness performance is measured and monitored. These companies are simulated in such a way to ensure they have a low commitment to meeting the subjective information they communicate. In such scenarios, as observed from Fig. 8, there is a consistent decline in the number of SLAs they will form over a time period. This is because their earnestness score, as shown in Fig. 9, also declines which indicates to other companies that opportunistic and fraudulent behaviours are evident in the consortium of which it is part As a result, their SLAs continued to decrease, ceasing on 19th March, 1st April and 18th April, respectively. Companies A and E

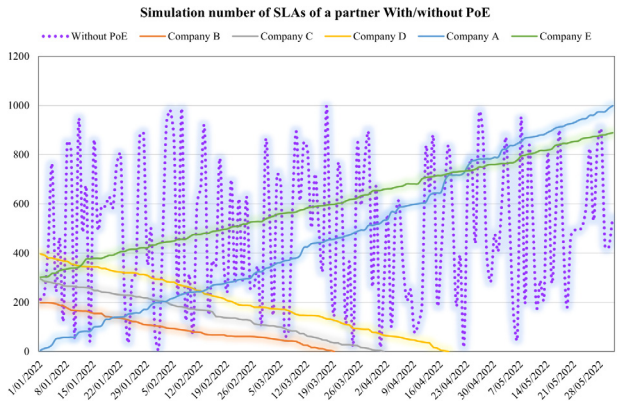

Fig. 8. Number of SLAs in 6 months with and without the assistance of SIAEF.

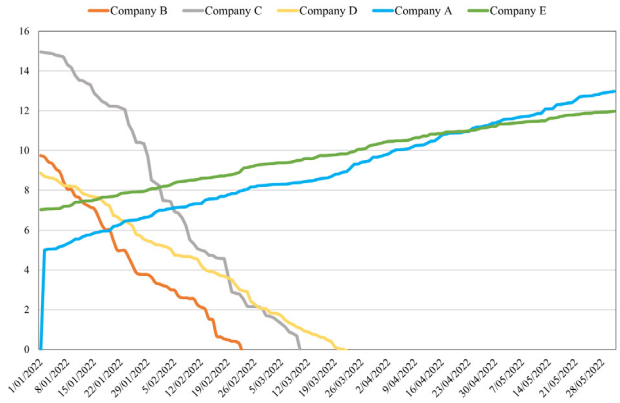

Fig. 9. Global average earnestness score of SIAEF's members.

represented by blue and green lines, respectively, are simulated to adhere to their commitment. In these scenarios, Companies A and E increase their global earnestness scores as shown in Fig. 9 and consistently increase the number of SLAs that they form with other companies as shown in Fig. 8. Therefore, SIAEF/PoE motivates members to maintain their earnestness to increase their SLAs signed over timestamps which eliminates the tendency of fraudulent behaviour in selected consortiums, thereby ensuring security from an internal perspective.

6. Related work

From 2020, existing research and empirical papers have proposed several proofs and frameworks to verify and validate the trustworthiness of a partner in blockchain. But as pointed out in our recent survey paper [15], none of this work considers subjective information in blockchain applications. Some of the most recent work on trustworthiness and reputation management in blockchain-based applications are:

Blockchain-based communication. Jiao Li et al. [29] propose a novel consensus mechanism based on multilink integrated factors. It leverages the entity's communication link number and the entity's trust degree to identify entities with high communication capacity and trust, which are then selected as a source of communication. This approach improves concurrency and communication efficiency. Entities are classified as honest, free riders or malicious nodes. They are assigned their status based on their trust degree, where honest entities have a trust degree between 0.8 and 1, the free rider has a trust degree between 0.6 and 0.8, and malicious nodes have a trust degree of less than 0.6. The score of a node determines who can forward the data and who is banned from accessing it. While the working of this approach is similar to PoE/SIAEF as it classifies the trustworthiness of the entity with the score range, it is only applicable in the context where information that the entity communicates is from an objective source. It fails in scenarios when the information that the entity communicates is from a subjective source such as promises.

Reputation-based PBFT consensus mechanism. Li et al. [28] proposed a voting-based Practical Byzantine Fault Tolerance (PBFT) consensus mechanism to deal with the fraudulent or opportunistic behaviour of a validator. To motivate the validator to be honest, PBFT uses a game theory-based incentive (GTI) method, which incentivizes validators to conform to acceptable and honest behaviour and disclose accurate information regarding transactions and blocks. It is a similar concept to blockchain-based communication consensus. However, the information it considers is only from objective sources such as transactions. This differs from SIAEF's aim, which considers information from subjective sources and aims to ascertain its trustworthiness for proactive SCRM.

Zero-knowledge proof. The zero-knowledge proof (zk-SNARK) was introduced to verify and validate a transaction without revealing the digital footprint of a transaction [30–32]. The zero-knowledge proof assumes that the transaction has a digital footprint which means that it is applicable only when objective information is present. In the presence of subjective information, it fails. PoE addresses this drawback and is able to work on information that has no digital footprint.

Blockchain in a Reputation-based model. Fortino et al. [33] propose an agent-based reputation framework with blockchain technology in the Internet of Things (IoTs). The framework distributes trust information on every IoT device with a capable software agent as a reliable agent to the blockchain. The reliable agents are grouped by their reputation capital (RC) given by other devices which have had direct interaction with this partner and based on their history of interactions. The framework is an effective model which minimizes the self-promotion or opportunistic behaviour of an agent in IoTs. However, this agent-based reputation does not consider subjective information as SIAEF does. Qi et al. [34] propose a blockchain-aided secure reputation framework. This framework assists E-commerce in preventing false feedback from the buyers to ensure the reputation of the sellers is genuine. However, the proposed framework does not consider the subjective information from the sellers. This leaves reputation-based frameworks open to the fraudulent behaviours of a partner (agents or sellers) that may cause failures.

Trustchain. Malik et al. [35] proposed a peer-to-peer network blockchain-based trust management in supply chains. The proposed model enables each partner in a supply chain to verify and validate the trustworthiness of the data, which has a digital footprint as provided by the partner. The proposed model, however, does not consider the presence of subjective information. As emphasized in Section 1.1. subjective information is prevalent in the supply chain and needs to be considered to avoid any fraudulent behaviour by the interacting partners.

Fraud-resilient blockchain-based solution. Guerar et al. [36] provide a blockchain-based application that considers fraudulent behaviour by an entity on the Ethereum blockchain. To address this, the authors record the invoice financing flow immutably and the entities' reputation on their past behaviour in terms of whether they paid on time or not. This is done using PoW/PoS/PoA to record the financing flow that an entity undertook that has a digital footprint and the invoice transactions between them. However, when subjective information is present, the platform does not assess the risk terms that could impact a commitment to subjective information. Therefore, there is a need

for a consensus mechanism (such as PoE) to record the information which does not have a digital footprint before using existing consensus mechanisms such as PoW, PoS or PoA to encode them (shown in Fig. 1).

7. Conclusion and future work

In this paper, we proposed and demonstrated how SIAEF and PoE assist in validating the authenticity of subjective information in blockchains. We applied SIAEF as a novel decentralized application (Dapp) that enables a partner's earnestness in committing to subjective information in a blockchain to be recorded. In SCRM, this ensures that responsible partners do not act fraudulently and avoid procrastination with a high level of accountability, transparency and privacy. A fallen unicorn, Theranos, has made Silicon Valley question fraudulent behaviour which involves a "big promise little proof" [37]. Had the truthfulness of Theranos's promise been assessed with a mechanism similar to SIAEF, it would not have raised $724 million of capital for a "dream" technology [38]. SIAEF provides a trustworthy platform where a partner in a supply chain can have an immutable track record of its earnestness to the promises it has made and its trustworthiness. Any partner can use this record to make informed judgements about forming an SLA with the partner in question. In our future work, we will validate the integration of PoE and SIAEF in an Amazon-managed blockchain, which enables SIAEF to build its own permissioned network with an open-source Ethereum framework. Furthermore, we will also test the application of PoE and SIAEF in other domains, such as carbon credits provenance, where subjective information with respect to the origin of a carbon credit is involved.

CRediT authorship contribution statement

Hang Thanh Bui: Conceptualization, Methodology, Data curation, Investigation, Formal analysis, Validation, Writing – original draft, Writing – review & editing. **Omar K. Hussain:** Conceptualization, Methodology, Resources, Formal analysis, Validation, Writing – original draft, Writing – review & editing. **Daniel Prior:** Conceptualization, Formal analysis , Writing – review & editing. **Farookh K. Hussain:** Conceptualization, Formal analysis, Writing – review & editing. **Morteza Saberi:** Conceptualization, Methodology, Formal analysis, Writing – review & editing.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Hang Thanh Bui reports financial support was provided by University of New South Wales Canberra for her PhD candidature.

Data availability

Data will be made available on request

References

[1] A. Gorkhali, L. Li, A. Shrestha, Blockchain: a literature review, J. Manag. Anal. 7 (3) (2020) 321–343, http://dx.doi.org/10.1080/23270012.2020.1801529.

[2] B. Müßigmann, H. von der Gracht, E. Hartmann, Blockchain technology in logistics and supply chain management — A bibliometric literature review from 2016 to January 2020, IEEE Trans. Eng. Manage. 67 (4) (2020) 988–1007, http://dx.doi.org/10.1109/TEM.2020.2980733.

[3] R.Z. Rasi, U.S.B. Rakiman, R.Z.R.M. Radzi, N.R. Masrom, V.P.K. Sundram, A literature review on blockchain technology: Risk in supply chain management, IEEE Eng. Manag. Rev. 50 (1) (2022) 186–200, http://dx.doi.org/10.1109/EMR.2021.3133447.

[4] M.J. Lahkani, S. Wang, M. Urbański, M. Egorova, Sustainable B2B E-commerce and blockchain-based supply chain finance, Sustainability 12 (10) (2020) https://www.mdpi.com/2071-1050/12/10/3968.

[5] H. Wang, M. Zhang, H. Ying, X. Zhao, The impact of blockchain technology on consumer behavior: A multimethod study, J. Manag. Anal. 8 (3) (2021) 371–390, http://dx.doi.org/10.1080/23270012.2021.1958264.

[6] A. Gorkhali, R. Chowdhury, Blockchain and the evolving financial market: A literature review, J. Ind. Integr. Manag. 07 (01) (2022) 47–81, http://dx.doi.org/10.1142/S242486222150024X.

[7] S. Khan, R. Singh, Kirti, Critical factors for blockchain technology implementation: A supply chain perspective, J. Ind. Integr. Manag. 07 (04) (2022) 479–492, http://dx.doi.org/10.1142/S2424862221500111.

[8] R. Beer, T. Sharma, A quick look at cryptocurrency mining: Proof of work, in: 2022 2nd International Conference on Innovative Practices in Technology and Management, Vol. 2, ICIPTM, 2022, pp. 651–656.

[9] J. Yang, A. Paudel, H.B. Gooi, Compensation for power loss by a proof-of-stake consortium blockchain microgrid, IEEE Trans. Ind. Inform. 17 (5) (2021) 3253–3262.

[10] M. Qazi, D. Kulkarni, M. Nagori, Proof of authenticity-based electronic medical records storage on blockchain, in: Y.-D. Zhang, J.K. Mandal, C. So-In, N.V. Thakur (Eds.), Smart Trends in Computing and Communications, Springer Singapore, Singapore, 2020, pp. 297–306.

[11] Q. Li, J. Wu, J. Quan, J. Shi, S. Zhang, Efficient quantum blockchain with a consensus mechanism QDPoS, IEEE Trans. Inf. Forensics Secur. 17 (2022) 3264–3276.

[12] P.R. Nair, D.R. Dorai, Evaluation of performance and security of proof of work and proof of stake using blockchain, in: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV, 2021, pp. 279–283.

[13] N. Nair, A.K. Dalal, A. Chhabra, N. Giri, Edu-coin: A proof of stake implementation of a decentralized skill validation application, in: 2019 International Conference on Nascent Technologies in Engineering, ICNTE, 2019, pp. 1–4.

[14] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, Y.-X. Yang, A secure cryptocurrency scheme based on post-quantum blockchain, IEEE Access 6 (2018) 27205–27213.

[15] H.T. Bui, O.K. Hussain, M. Saberi, F. Hussain, Assessing the authenticity of subjective information in the blockchain: A survey and open issues, World Wide Web 24 (2) (2021) 483–509.

[16] V.M. Grötsch, C. Blome, M.C. Schleper, Antecedents of proactive supply chain risk management – A contingency theory perspective, Int. J. Prod. Res. 51 (10) (2013) 2842–2867, http://dx.doi.org/10.1080/00207543.2012.746796.

[17] T.-M. Choi, X. Wen, X. Sun, S.-H. Chung, The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era, Transp. Res. E 127 (2019) 178–191, https://www.sciencedirect.com/science/article/pii/S1366554519302601.

[18] MegaLag, AirTag exposes DHL fraud (no joke), 2021, https://youtu.be/EpiSzfMVPmg.

[19] M.S. Shalique, S.S. Padhi, J. Jayaram, R.K. Pati, Adoption of symbolic versus substantive sustainability practices by lower-tier suppliers: A behavioural view, Int. J. Prod. Res. (2021) 1–28, http://dx.doi.org/10.1080/00207543.2021.1939454.

[20] A. Salamai, O.K. Hussain, M. Saberi, E. Chang, F.K. Hussain, Highlighting the importance of considering the impacts of both external and internal risk factors on operational parameters to improve supply chain risk management, IEEE Access 7 (2019) 49297–49315.

[21] F. Nawaz, O. Hussain, F.K. Hussain, N.K. Janjua, M. Saberi, E. Chang, Proactive management of SLA violations by capturing relevant external events in a Cloud of Things environment, Future Gener. Comput. Syst. 95 (2019) 26–44, https://www.sciencedirect.com/science/article/pii/S0167739X18318065.

[22] D. Gabay, K. Akkaya, M. Cebe, Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs, IEEE Trans. Veh. Technol. 69 (6) (2020) 5760–5772.

[23] M.S. Rahman, M. Chamikara, I. Khalil, A. Bouras, Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city, J. Ind. Inf. Integr. 30 (2022) 100408, https://www.sciencedirect.com/science/article/pii/S2452414X22000759.

[24] E. Anderson, B. Weitz, The use of pledges to build and sustain commitment in distribution channels, J. Mar. Res. 29 (1) (1992) 18–34, http://dx.doi.org/10.1177/002224379202900103.

[25] H.T. Bui, O.K. Hussain, D. Prior, F.K. Hussain, M. Saberi, Proof by earnestness (PoE) to determine the authenticity of subjective information in blockchains - application in supply chain risk management, Knowl.-Based Syst. 250 (2022) 108972, https://www.sciencedirect.com/science/article/pii/S0950705122004713.

[26] S.M. Vieira, U. Kaymak, J.M.C. Sousa, Cohen's kappa coefficient as a performance measure for feature selection, in: International Conference on Fuzzy Systems, 2010, pp. 1–8.
[27] W. Zou, D. Lo, P.S. Kochhar, X.-B.D. Le, X. Xia, Y. Feng, Z. Chen, B. Xu, Smart contract development: Challenges and opportunities, IEEE Trans. Softw. Eng. 47 (10) (2021) 2084–2106.
[28] X. Li, Q. Liu, S. Wu, Z. Cao, Q. Bai, Game theory based compatible incentive mechanism design for non-cryptocurrency blockchain systems, J. Ind. Inf. Integr. 31 (2023) 100426, https://www.sciencedirect.com/science/article/pii/S2452414X22000930.
[29] T.L. Jiao Li, A novel multi-link integrated factor algorithm considering node trust degree for blockchain-based communication, KSII Trans. Internet Inf. Syst. 11 (8) (2017).
[30] X. Sun, F.R. Yu, P. Zhang, Z. Sun, W. Xie, X. Peng, A survey on zero-knowledge proof in blockchain, IEEE Netw. 35 (4) (2021) 198–205.
[31] Y.C. Tsai, R. Tso, Z.-Y. Liu, K. Chen, An improved non-interactive zero-knowledge range proof for decentralized applications, in: 2019 IEEE International Conference on Decentralized Applications and Infrastructures, DAPPCON, 2019, pp. 129–134.
[32] L. Cao, Z. Wan, Anonymous scheme for blockchain atomic swap based on zero-knowledge proof, in: 2020 IEEE International Conference on Artificial Intelligence and Computer Applications, ICAICA, 2020, pp. 371–374.
[33] G. Fortino, F. Messina, D. Rosaci, G.M.L. Sarné, Using blockchain in a reputation-based model for grouping agents in the internet of things, IEEE Trans. Eng. Manage. 67 (4) (2020) 1231–1243.
[34] S. Qi, Y. Li, W. Wei, Q. Li, K. Qiao, Y. Qi, Truth: A blockchain-aided secure reputation system with genuine feedbacks, IEEE Trans. Eng. Manage. (2022) 1–15.
[35] S. Malik, V. Dedeoglu, S.S. Kanhere, R. Jurdak, TrustChain: Trust management in blockchain and IoT supported supply chains, in: 2019 IEEE International Conference on Blockchain (Blockchain), 2019, pp. 184–193.
[36] M. Guerar, A. Merlo, M. Migliardi, F. Palmieri, L. Verderame, A fraud-resilient blockchain-based solution for invoice financing, IEEE Trans. Eng. Manage. 67 (4) (2020) 1086–1098, http://dx.doi.org/10.1109/TEM.2020.2971865.
[37] K. Straker, S. Peel, E. Nusem, C. Wrigley, Designing a dangerous unicorn: Lessons from the theranos case, Bus. Horiz. 64 (4) (2021) 525–536, https://www.sciencedirect.com/science/article/pii/S0007681321000185.
[38] A. Adamik, M. Nowicki, Pathologies and paradoxes of co-creation: A contribution to the discussion about corporate social responsibility in building a competitive advantage in the age of Industry 4.0, Sustainability 11 (18) (2019) https://www.mdpi.com/2071-1050/11/18/4954.

Hang Bui is a Ph.D. candidate at the University of New South Wales, Canberra. She has extensive experience in project development focusing on business modelling, supply chain management and innovation. She was featured in the newsletter for Italy's Ministry of Foreign Affairs as one of the top two excellent scholars with a successful business model in collaboration with Botta Packaging. In 2020, she was selected as one of the Top 30 Rising Stars in European packaging innovation for the 30 Under 30 Awards.

Omar K Hussain is an Associate Professor at the University of New South Wales, Canberra. His research interests are in business intelligence, cloud computing and logistics informatics. In these areas, his research work focuses on utilizing decision-making techniques for facilitating the smart achievement of business outcomes. His research work has been published in various top international journals such as Information Systems, The Computer Journal, Knowledge Based Systems, Future Generation Computer Systems, etc. He has won awards and received funding from competitive bodies such as the Australian Research Council for his research.

Daniel Prior is an Associate Professor in the School of Business at UNSW, Canberra. Daniel has worked in industry for companies such as KPMG, Acer Computer Australia and Communications Design and Management. Daniel is active on a range of corporate and not-for-profit boards, and, as a marketing strategy consultant and mentor for industry, particularly in new product development, complex systems implementations and in strategy.

Farookh Hussain is a Professor in the School of Computer Science, University of Technology Sydney. He is an Associate Member of the Advanced Analytics Institute and a Core Member of the Centre for Artificial Intelligence. His key research interests are in trust-based computing, cloud of things, blockchains and machine learning. He has published widely in these areas in top journals such as FGCS, The Computer Journal, JCSS, IEEE Transactions on Industrial Informatics, IEEE Transactions on Industrial Electronics etc.

Morteza Saberi is a Lecturer with School of Computer Science, University of Technology Sydney, Australia and has an outstanding research record and significant capabilities in the areas of business intelligence, data mining and applied machine learning. He has published more than 150 papers in reputable academic journals and conference proceedings. His Google Scholar citations and h-index are 2210 and 22 respectively. He was a Lecturer at the Department of Industrial Engineering at the University of Tafresh. He is the recipient of the 2006–2011 Best Researcher of Young Researchers Club, Islamic Azad University (Tafresh Branch) and the recipient of the National Eminent Researcher Award among Young Researchers Club, Islamic Azad University members.