Hindawi
Security and Communication Networks
Volume 2023, Article ID 3303122, 20 pages
https://doi.org/10.1155/2023/3303122

Research Article

Blockchain-Based Cyber Threat Intelligence Sharing Using Proof-of-Quality Consensus

Dimitrios Chatziamanetoglou and Konstantinos Rantos

Department of Computer Science, International Hellenic University, Kavala, Greece

Correspondence should be addressed to Dimitrios Chatziamanetoglou; diehatz@cs.ihu.gr

Received 11 May 2022; Revised 3 September 2022; Accepted 22 September 2022; Published 13 February 2023

Academic Editor: Andrea Michienzi

Copyright © 2023 Dimitrios Chatziamanetoglou and Konstantinos Rantos. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cyber threat intelligence (CTI) is contextualised knowledge, built on information that is collected, processed, analysed, and disseminated to the right audience, in order to comprehend a malicious threat actor's motivation, goals, objectives, targets, and attack behaviours. The CTI value increases by the ability to be shared, consumed, and actioned timely, by the right stakeholders, based always on quality standards and parameters, which boost the cyber security community to understand how adversaries act and to counter the constantly emerging sophisticated cyber threats. In this article, along with the identification of research gaps, after a comparison between existing research studies in the similar scope of CTI evaluation and sharing mechanisms, we propose a blockchain-based cyber threat intelligence system architecture, which collects, evaluates, stores, and shares CTI, enabling tamper-proof data and exclusion of untrustworthy evaluation peers, while evaluating, at the same time, the quality of CTI Feeds against a defined set of quality standards. The evaluation of the data is performed utilising a reputation and trust-based mechanism for selecting validators, who further rate the CTI feeds using quality-based CTI parameters, while the consensus for preserving the fairness of the results and their final storage is performed via the recently introduced proof-of-quality (PoQ) consensus algorithm. The data, which are stored in the proposed ledger, constitute a reliable, distributed, and secure repository of CTI Feeds and contain their objective evaluation, as well as the performance of the validators who participated in each evaluation, while these data can be further used for assessing the reputation of CTI Sources. Finally, in order to assess the proposed system's reliability, integrity, and tolerance against malicious activities, the model is subject to a theoretical analysis using a probabilistic simulation, taking into account various aspects and features of the integrated mechanisms. The results show that the tolerance against malicious validators is acceptable, even when the ratio between legitimately vs. maliciously behaving validators is 1 : 50.

1. Introduction

Cyberspace landscape is constantly changing and so are the malicious threats actors, who via dynamically adopted techniques, mechanisms, and methodologies are trying to exploit known cyber security gaps or discover new ones [1]. On the contrary, organisations are increasing their attack surface in a way that can be easily attacked or damaged due to the asymmetrical nature of cyber threats and the inherent cyberspace vulnerabilities. This is the reason why it is very crucial to transform reactive behaviour to proactive, in order to counter cyberattacks more efficiently.

Furthermore, during cyberattack activities, a well-structured, trained, and effective incident response team, armed with the threat intelligence necessary to understand and analyse how threat actors behave and operate, is more than required.

Threat intelligence is not just about data, rather a finished outcome that is a result of threat intelligence cycle of data collection, processing, and analysis, which is iterative and becoming refined over time. Producing actionable and accurate cyber threat intelligence is part of a lifecycle process, referred as the intelligence cycle, comprising of 5 stages: planning and direction, collection, processing, analysis, and dissemination [2].

The latest stages of the cyber threat intelligence cycle are in the focus of this article, without decreasing the importance of the initial ones though. Cyber threat analysis deals

with the production of valuable and actionable information about standing or emerging threats, which enables the community to make accurate and timely decisions. Analysed information can enhance response and detection mechanisms and facilitate dealing with increasingly sophisticated advanced persistent threats.

The outcome of the cyber threat analysis is called cyber threat intelligence (CTI), which based on the application level, can be divided in four categories from high level to low level, as strategic, tactical, technical, and operational. Depending on the level and type of CTI, the provided information is composed of the combination of threat actors, patterns of attacks, attack methodologies, motive, threat severity, threat landscape, Techniques-Tactics-Procedures (TTP), and Indicators of Compromise (IoC). On all the aforementioned levels, CTI sharing mechanism is playing a significant role, on which governmental institutions, private sector, IT security vendors, IT industry, and security researchers are putting strong effort for reliable, timely, and accurate CTI sharing.

According to the latest cyber threat intelligence overview published by ENISA [3], CTI should follow 5 main principles: be based on reliable sources, have sufficient context from sources, be structured under a consistent data model, follow a well-defined process, and integrate automation. All those aspects should coexist in a way that quality intelligence could be delivered efficiently and effectively, securely, timely, and accurately.

Extensive existing research studies are addressing CTI data dissemination requirements, but are mainly focused on blockchain mechanisms which benefit from its key characteristics such as integrity, availability, scalability, and consensus among the stakeholders. In addition, research activities propose methods on establishing a higher level of trust, but mainly depending on the application of the blockchain technology but not derived from the data which are stored at the ledger. Furthermore, in the existing literature, quality assurance criteria for evaluating CTI data are proposed, but not clearly or directly integrated in any CTI analysis mechanism which can provide value to the CTI community.

After identification of the above research gaps, our research takes advantage of the existing work, combines the key characteristics of blockchain technology, and proposes new mechanisms for establishing trust among the CTI stakeholders, which is derived from the data stored in the ledger. Furthermore, our research proposes the integration of CTI quality criteria in CTI evaluation processes and finally introduces a new consensus algorithm for reaching agreements on the evaluation results of CTI Feeds. All evaluated CTI feeds are finally the ledger regardless of their evaluation scoring, along with evaluation data which can formulate and support reputational feedback mechanisms for future CTI Feed evaluations and evaluators selection criteria.

This article describes a decentralised solution for sharing vetted CTI information, proposing a new model called Awareness Architecture Based on Blockchain CTI Convergence $(ABC)^2$, focused on a CTI-sharing mechanism based on blockchain technology. In this scope, it focuses also on describing a new consensus mechanism, namely, proof-of-quality (PoQ), in the context of a trust-based reputation mechanism for evaluating CTI Feeds and also contextualising the overall reputation of CTI Feed Sources, based on quality parameters.

The PoQ mechanism ensures that each CTI Feed evaluation result is agreed among the selected validators/evaluators via an open dissemination and voting process. This process will lead to the update of the ledger records with the required information. Those records construct a historical immutable chain of the CTI feeds as well as a progressively updated database which constitutes the foundation for the reputational model of the proposed solution.

The aim of this article is dual. The first one deals with the evaluation of the quality of CTI Feeds, considering quality-driven CTI-sharing challenges. This evaluation is based on the ratings provided by a set of a selected pool of validators, based on reputational-focused selection criteria. A secondary objective of this article is to put context on the reputation of the CTI Feed sources, based on the evaluation of their own published feeds. The reputation of the validators has a critical role on the fulfilment of those objectives, since it is one of the decisive elements among the performance and reputation metrics which will be presented later on.

The article is structured as follows. Section 2 presents the key considerations of our research, related background work as well as the motivations and challenges that triggered the proposal of a blockchain-based CTI-sharing scheme. Section 3 presents the architecture of the proposed model and analyses the various components that comprise it. Section 4 presents a conditional theoretical simulation of the model's tolerance against malicious injections, while the final sections summarise the paper's proposals and depict our future work objectives.

2. Background and Related Works

Ideally, cyber threat intelligence reports contain combined, processed, and analysed information that helps security professionals to make informed decisions regarding security controls to protect the organisations from cyber threats. Efficient and informed decision-making is based on actionable and contextualised threat intelligence data feeds, timely shared in an optimised and trusted environment [4], and easily understood by the people in charge, fulfilling also quality standards to provide actual benefit.

The latest SANS Cyber Threat Intelligence Survey of 2021 [2] reports that the majority of CTI is collected and shared via means which do not include automation or optimisation mechanisms such as e-mail exchange, presentations and briefings, spreadsheets, and reports in digital format, while the rest of the collection and sharing methods are based on either vendor/in-house or open-source systems. Even though there is no direct reference to the tools and mechanisms which support the CTI collection/sharing, there is a strong indication that blockchain technology is not used on production.

2.1. Key Considerations. The main key topics which drive our research, proposing a new CTI sharing model, are as follows:

(a) Availability, in terms of the ability of the audience and stakeholders to access the environment which collects, stores, evaluate, and shares CTI data

(b) Reliability and quality, with regard to the quality criteria and level of standardisation

(c) Reputation, regarding the historical aggregation of data which can enable trust among the stakeholders as a whole and also for each one of them

(d) Integrity, concerning the prevention and tolerance for unauthorised changes

(e) Consensus, in terms of which methodology or algorithm is used to reach final agreement for updating the ledger

(f) Openness and fairness, as to allow the access and participation of an open audience to consume services, but still under certain processes for fair access control when contribution for evaluations required

(g) Scalability, in respect of supporting increasing number of transactions

(h) Tolerance against malicious activities

2.2. Existing Research Studies. Two different research areas will be taken into consideration, since both of them combined address the key considerations mentioned before. The first one is the work related to CTI sharing using blockchain technology, while the second one deals with blockchain-based models for establishing trust.

2.2.1. Research for Blockchain-Based CTI Sharing and CTI Feed Evaluation. He et al. [5] address the need of using blockchain technology, proposing a theoretical rating mechanism based on an agnostic data model, abstract credibility factors, and consensus algorithm. Gong and Lee [6] propose a blockchain-based CTI sharing framework with a prevention mechanism against Sybil attacks, referring to an abstract mining-related consensus algorithm, for collection of threat intelligence by smart contracts and storage of meta-information in blockchain, ensuring validation and traceability to the data source. Mendez Mena and Yang [7] research is based on the Ethereum platform, applying the proof-of-authority consensus algorithm, using a distributed data collection method with an abstract data model and a permissioned based network, from an ISP point of view. Cha et al. [8] propose a model which mitigates problems such as data collection efficiency and scalability, using an abstract data model and blockchain technology to efficiently process big data, working with multiple feeds to verify the reliability of the data shared during data collection and providing security and privacy in a distributed way. Riesco et al. [9] propose a CTI blockchain-sharing framework using the STIX data model as a reference as well as W3C semantic web standards to enable a workspace of knowledge related to behavioural threat intelligence patterning to characterise tactics, techniques, and procedures, while they propose an Ethereum Blockchain Smart contract Marketplace to better motivate the sharing of that knowledge between all parties involved as well as creating a standard CTI token as a digital asset with a promising value in the market. Homan et al. [10] propose a blockchain network model that facilitates the secure dissemination of CTI data using a testbed based on Hyperledger Fabric and the STIX 2.0 protocol, validating the efficacy of the segmentation, implemented using smart contracts and Fabric channels, focusing on the potential to overcome the trust barriers and data privacy issues inherent in this domain.

2.2.2. Research for Blockchain-Based Trust Establishment and CTI Evaluation. Meier et al. [11] propose FeedRank, an advanced and tamper-resistant ranking metric for CTI Feeds that does not require a ground truth, which bears similarities with collective intelligence approaches of PageRank. Wu et al. [12] propose a threat intelligence quality assessment framework enabling the establishment of trust through verifying the integrity of the information and the development of a reputation system that will allow peers to rate CTI sharing transactions based on the quality, using an abstract consensus algorithm and data model. Shala et al. [13] propose a new trust consensus protocol, consisting of three parts for evaluating the trust score of a peer: Service Trust Evaluation evaluates the services the peer is providing; Behaviour Trust Evaluation evaluates the behaviour of a peer based on the integrity of a service; Task Trust Evaluation evaluates the activities as a Test Agent or other tasks done in the machine-to-machine community. Kamvar et al. [14] and Gao et al. [15] propose a new reputation management algorithm for P2P networks, attempting to identify malicious peers that provide inauthentic files to the system, which is superior to attempting to identify inauthentic files themselves, since malicious peers can easily generate a virtually unlimited number of inauthentic files if they are not banned from participating in the network. Wang et al. [16, 17] designed a trust scheme for consensus protocol for IIoT, to provide a new module of reputation so that each participant can share a global view of reputation in the building consensus process by showing the potential of repute for managing trust in a consensus protocol. In the repute module, satisfactory behaviour is encouraged and bad behaviour is punished. Lee et al. [18] proposed a blockchain-based reputation management for manufacturers and customer interaction, including increased reliability by malicious evaluator identification. Oualhaj et al. [19] propose a blockchain-based decentralised trust management model for IoT system, which allows all IoT devices participate in the update of trust values in a decentralised way and to detect the node with malicious behaviour that provides wrong trust values. Oliveira et al. [20] proposed a Blockchain Reputation-Based Consensus via a mechanism based on majority voting that enables a group of miners through a judge based system that monitors and signs a reputation score for every miner's action. Feng et al. [21] propose Proof-of-Negotiation

(PoN) consensus algorithm, including random-honest miners' selection, parallel multiblocks' creation, and distributed blocks storage introducing trust management to evaluate the trustworthiness of miners with negotiation rules.

2.3. Problem Statements and Contribution. Sharing robust, fast, reliable, verified, actionable, and immutable CTI is a constantly growing need and so is the development and utilisation of platforms which support it. Nowadays, there are many CTI Feed sources that provide CTI via a variety of platforms and standards [22]; the volume of which is growing and the data models and data types that are used and are scattered across various solutions and standards, which can impact the level of quality of the threat intelligence data [23].

According to the presented related work, existing research efforts address the blockchain-based CTI dissemination as well as trust and reputation challenges among the CTI-sharing community, but not combined under one solution. Furthermore, the quality of the CTI Feeds is not addressed in a practical way, rather as an abstract requirement without any quantifiable metrics. Due to these identified gaps, a blockchain-based platform using a reputation mechanism and a new Proof-of-Quality consensus mechanism is presented, enabling trust among the CTI sharing community and addressing the challenges of CTI sharing as well as the level of CTI data quality, combining 5 main principles: reliable sources, sufficient context, consistent data model, defined process, and automation [3].

In this article, we extend the work presented in [24] to elaborate on the system's components and analyse how the quality-driven and reputation-oriented proposed model can contribute to the CTI Feed and CTI Sources evaluation, using blockchain technology. The mechanism which underpins the consensus of the model is called proof-of-quality and it relies on the output of the CTI feed evaluation, which is based on pre-defined quality evaluation parameters, utilising also a voting mechanism for reaching final agreements.

3. CTI-Sharing Model

3.1. System Model Introduction. The proposed model is composed of a number of submechanisms (Figures 1 and 2), which select the CTI Feed validators under specific criteria, receive CTI Feeds as an input, evaluate them via an evaluation control mechanism, and finally, as an output, add a block to the ledger with the evaluated CTI Feed for distributed dissemination; once consensus is reached via the proof-of-quality consensus algorithm.

The objective is to evaluate the CTI Feeds utilising predefined quality-based criteria and parameters, and a reputation mechanism that will foster trust establishment among all participants. All CTI Feeds and their evaluation results are added to the chain together with each validator's performance, in order to maintain a historical immutable archive. These performance results will be further used for assessing the validators' and the CTI Feed Sources' reputations.

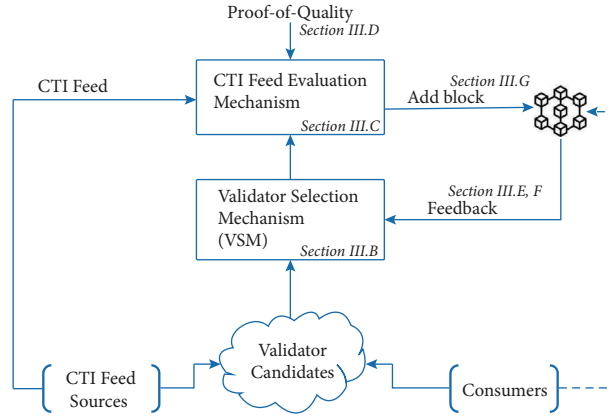

Figure 1: Model's high-level architecture.

The proposed model has 3 key roles which interact with each other as follows:

(a) CTI Feed Sources: share available CTI Feeds for evaluation as input to the proposed process, either by producing cyber threat information (e.g., Threat Actors activities and Indicators of Compromise) or sharing already received information with small-scale or no additional intelligence updates or sharing information aggregated from other data feeds, either based on internal or external collection sources

(b) Validators: the selection of validators is based on historical reputation criteria, in order to conduct the CTI Feed evaluation

(c) Consumers: they are the final users/consumers of the produced and evaluated CTI information, stored in the ledger.

Apart from the already given roles as described above, both CTI Feed sources and Consumers can be part of the evaluation process as validator candidates, being part of the validator candidate pool (2-way information flows as shown in Figure 1). The subscription process for being a validator candidate could be based on a normal subscription approach into the blockchain services, via unique identifiers and certificates, process which is not in the scope of this article.

The selection of the validators is performed by the validator selection mechanism (VSM). This mechanism filters the validator candidate pool in order to select the most performant candidates for the evaluation process, taking into consideration the validators' reputation, derived from the validators' performance already published on the blockchain. The VSM mechanism will be described in detail later on.

It needs to be highlighted that every evaluated CTI Feed is added to the blockchain, regardless of the results, allowing no room for wrong screening and in parallel fostering fairness. The decisive added value of the proposed system is that, along with the CTI Feeds, their evaluation and also the validators' performance data are added (as shown in

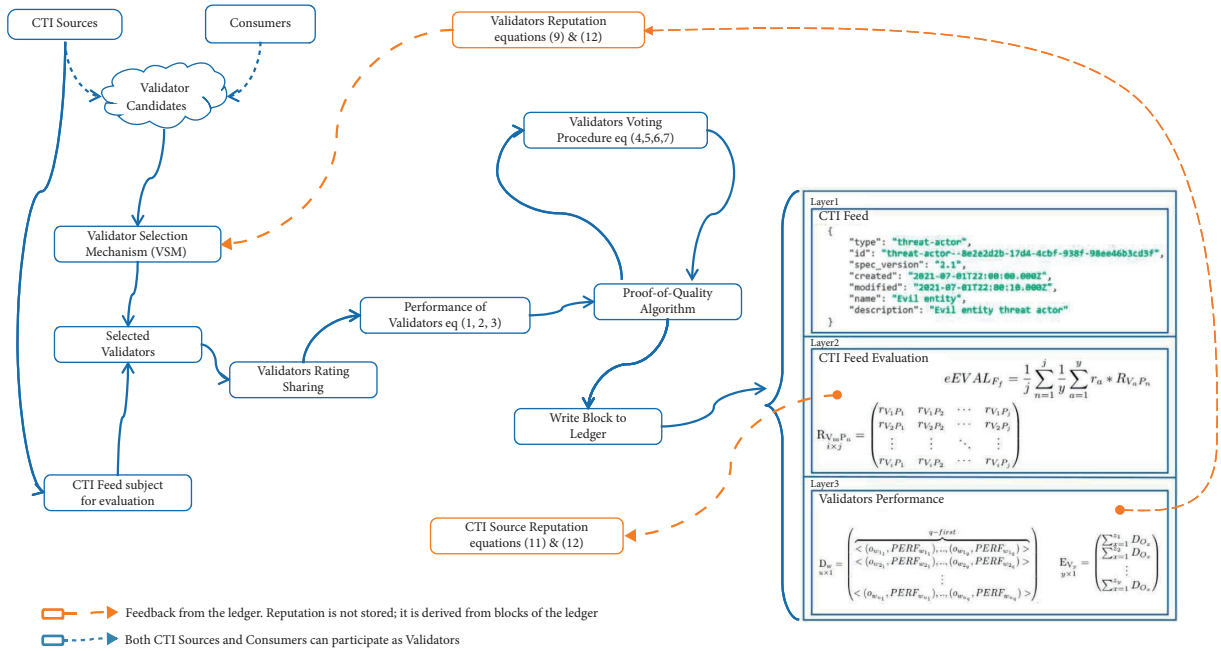

Figure 2: Block diagram of the proposed model.

Figure 3), data which constitute the baseline for the reputation mechanism, as for the validators' reputation used in the Validator Selection Mechanism, as well as for assessing the CTI Source reputation.

The decision on whether a CTI Feed will be eventually utilised or not is left to the discretion of each consumer, who will be able to make the decision based on the data stored in the ledger.

It should also be clarified that all roles of the model are uniquely identified once registered in the system, the public identity of which is not recognisable by the rest of the community, in order to preserve the fairness, objectivity, and impartiality of the follow-on processes. The unique identification can be generated and maintained by combining multiple identity attributes of each role (e.g., id during registration and name of the organisation/company) hashed via a hash algorithm (e.g., SHA3), producing a unique name which provides anonymity. For ease of reading, this is not applied in the present article, and all roles are presented in a way that can be easily identified.

The system's notations which define the basic structural elements of this article are listed in Table 1.

3.2. VSM: Validator Selection Mechanism. Trust is established based on available evidence of the validators' past behaviour and contribution to past evaluation metrics and data. VSM is meant to collect and analyse such evidence, resulting in a reputation score, which is further to be taken into account to decide whether a specific validator should be considered as trusted and further selected for contributing to the CTI Feed evaluation process. This past behaviour is already part of the ledger, offering reliability, transparency, and immutability.

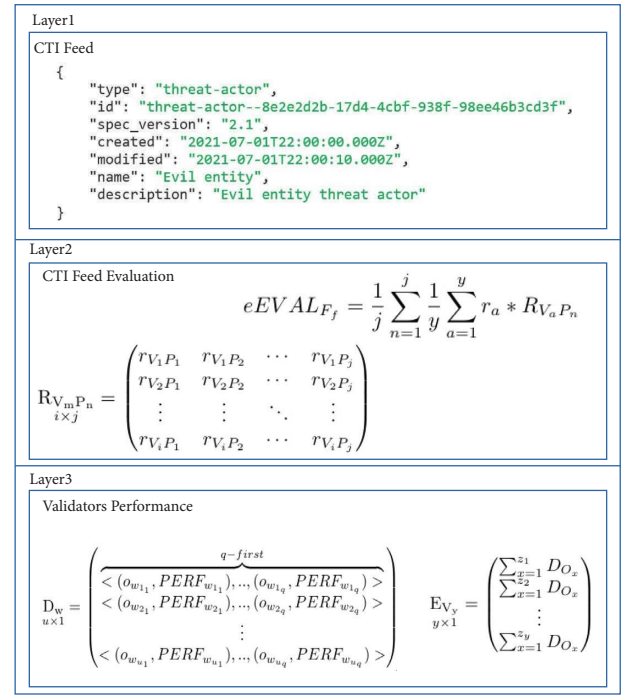

Figure 3: Block layers.

During the VSM process shown in Algorithm 1, the pool of candidate validators is subject to a clustering method using ML algorithms such as K-Means or DBSCAN [25], applying also outlier detection and removal. Validators with good previous conduct and evaluation contribution history have a higher probability of being selected based on their accumulated reputation. Validators are mainly selected out of the most reputable cluster, which is calculated taking into

Table 1: System notations.

Notations	Description
S_s	CTI feed source, $s \in [1..q]$
F_f	CTI feed, $f \in [1..k]$
V_m	Validator, $m \in [1..i]$
P_n	Quality parameter, $n \in [1..j]$
VSM	Validator selection mechanism
q – first	Max number of validators for consensus
SDM	Squared deviation from the mean
$R_{V_m P_n}$	Validator rating against quality parameters [1..100]
MRV	Mean rating value per quality parameter
PERF_{V_m}	Validator performance
$i\text{EVAL}_{F_f}$	Interim evaluation of CTI feed
$e\text{EVAL}_{F_f}$	Enriched evaluation of CTI feed
$A_{V_m B_b}$	Validator performance matrix per block
REP_{V_m}	Validator reputation
$C_{F_f B_b}$	Stored CTI feed evaluation per block
REP_{V_m}	Validator reputation
REP_{S_s}	CTI feed source reputation
O_{V_m}	Ordered list of validator performance
D_w	Matrix of O_{V_m}
A_T	Aging factor
f^t	Fading factor

account the number of evaluations per validator and their performance, out of the validator performance matrix in equation (10), while their overall reputation is shown via equation (11), as described later.

Furthermore, considering fairness, in order to increase the chance of other less reputable validators to increase their reputation, a weighted random choice mechanism can be applied, resulting the selection of validators which belong into less reputable clusters, based on an adjustable ratio (x/y), with $x > y$, for example, x% out of the most reputable cluster and y% out of less reputable clusters. This way, fairness is established, ensuring that all validator candidates have chances to be selected as validators.

The number or the percentage of the finally selected validators in comparison to the total validator candidate number can vary according to the requirements and is subject to further optimisation which is not covered in this article. The same applies to the percentage of the most reputable candidates versus the less reputable ones.

Furthermore, a feedback mechanism that utilises historical data already published on the blockchain (such as IoC, e.g., malicious IPs) provides valuable information to the VSM to further screen the validators' candidacy.

3.3. CTI Feed Evaluation and Rating Metrics. The foundation of the CTI Feed evaluation mechanism consists of the following performance metrics:

(i) CTI Feed rating

(ii) Validator performance

3.3.1. CTI Feed Rating. Each selected validator V_m, $m \in [1..i]$, rates each CTI Feed F_f, $f \in [1..k]$ (Figure 4), against all quality parameters P_n, $n \in [1..j]$, where i is the total number of selected validators, k is the number of CTI Feeds under evaluation, and j is the total number of the quality parameters, respectively. Such a set of quality parameters can be defined as in [26–28]. Although, in [26], the quality parameters are CTI Source and not CTI Feed oriented; these can be refined in order to be applicable in the context of this paper, but this scope is outside of the objectives of the present work. Examples of CTI Feed quality parameters are shown in Table 2.

The rating per CTI Feed F_f is depicted as shown in the following matrix R:

$$R_{\substack{V_m P_n \\ i \times j}} = \begin{pmatrix} r_{V_1 P_1} & r_{V_1 P_2} & \cdots & r_{V_1 P_j} \\ r_{V_2 P_1} & r_{V_2 P_2} & \cdots & r_{V_2 P_j} \\ \vdots & \vdots & \ddots & \vdots \\ r_{V_i P_1} & r_{V_i P_2} & \cdots & r_{V_i P_j} \end{pmatrix}. \tag{1}$$

3.3.2. Validator Performance. This metric is measured by the deviation of each CTI Feed rating compared to the mean rating. This comparison is applied per quality parameter per each evaluation performed by all validators and is based on statistical analysis metrics, such as squared deviation from the mean (SDM). One important aspect is the applicable anomaly/outlier detection, which is already inherited in the SDM, enabling the identification and removal of misbehaving or overreacting validators from the overall calculations.

Figure 5 shows the squared deviation from the mean (SDM) of a rating $R_{V_m P_n}$ of a selected validator V_m, $m \in [1..i]$, per quality parameter P_n, $n \in [1..j]$, per CTI Feed. The closer the rating is to the mean, the better the performance of the validator will be. The SDM calculation has to take place for all the quality parameters per validator per CTI Feed evaluation separately.

Due to the immutable nature of the data on the ledger, it is proposed not to use any weighted approach on the quality parameters, which are considered equally important. In case it is required, a weight can be assigned to each quality parameter on an ad hoc basis on the already stored data, to show the relative importance of quality parameters against the others. Therefore, a weighted evaluation is still an option, based on the requirements of the methodology and context in which it is used.

The mean rating value (MRV) of all validators V_m, $m \in [1..i]$, per quality parameter P_n, $n \in [1..j]$, for a specific feed, is the following:

$$\text{MRV}_{P_n} = \frac{1}{i} \sum_{m=1}^{i} R_{V_m P_n}. \tag{2}$$

The SDM of a validator V_m per quality parameter P_n is

$$\text{SDM}_{V_m} = \left(\text{MRV}_{P_n} - R_{V_m P_n}\right)^2. \tag{3}$$

Each validator's performance is inversely proportional to the SDM metric, taking into account all the individual SDM

Data: max: Maximum number of validators to be selected
x: Percentage of most reputable validators
y: Percentage of less reputable validators
$x + y = 100$
$A_{V_m B_b}$: Validator performance matrix (equation (10))
Result: Create a pool of validators
(1) Construct a 2-dimensional plot with the average performance of each validator vs. the number of their overall validations;
(2) Identify the most performant clusters of validators;
(3) Select x% of max out of the most performant cluster/s;
(4) Select y% of max randomly out of the less performant cluster/s;
(5) Create the list of validators V_m, $m \in [1..\max]$

Algorithm 1: Pseudocode for VSM algorithm.

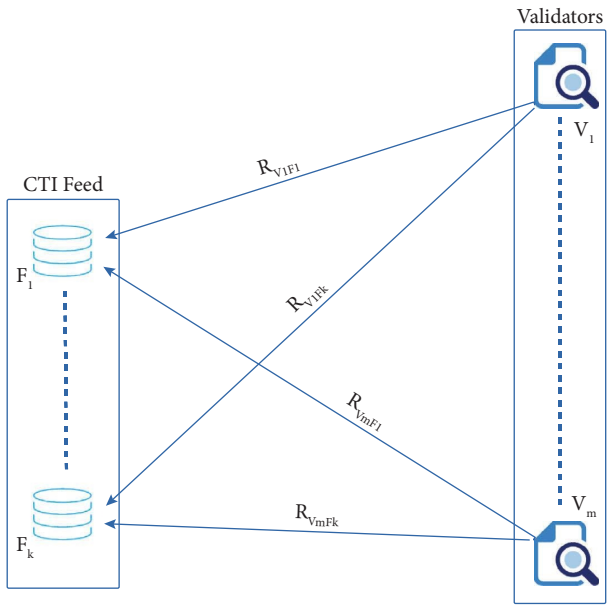

Figure 4: CTI feed rating.

Table 2: CTI quality parameters.

Parameters	Description
Extensiveness	Evaluates how many optional parameters are filled in
False positives	Determines how often feeds are invalidated
Verifiability	Expresses is a feed is linked with primary sources of information
Intelligence	Indicates how much added value a feed offers in the information by linking it to other objects
Interoperability	Measures if a CTI feed follows a specific data format to provide the data
Syntactic accuracy	Determines how compliant a feed is to the standard which is followed
Originality	Evaluates how unique the entries of each feed are
Timeliness	Analyses how soon a CTI feed is releasing information in comparison of the initial date of the malicious activity
Impact	Measures the consequences to an organisation if the information from a feed is applied
Standardisation	Measures how much of free text is used in the feed's objects

ratings per quality parameter, calculating their average SDM. The less the deviation from the MRV is, the better the performance is. The overall performance PERF of each validator V_m, $m \in [1..i]$, for all ratings $R_{V_m P_n}$ performed against every quality parameters P_n, $n \in [1..j]$, per CTI Feed F is the following:

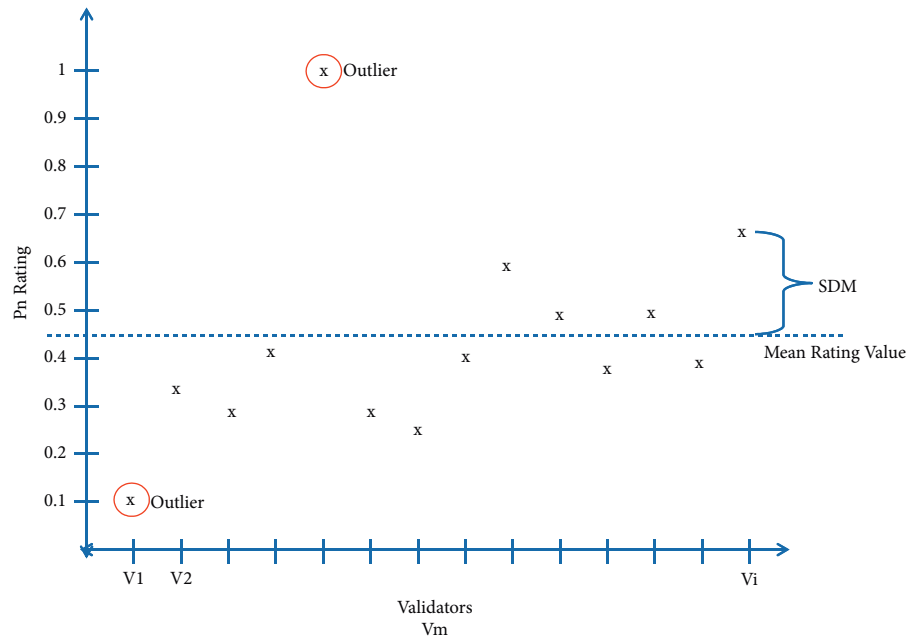

Figure 5: Squared deviation from the mean per quality parameter.

$$\mathrm{PERF}_{V_m} = \frac{1}{(1/j)\sum_{n=1}^{j}\left(MRV_{P_n} - R_{V_m P_n}\right)^2}. \quad (4)$$

This metric will be taken into account for calculating the validator reputation later on.

3.4. Proof-of-Quality Consensus Mechanism. By completion of a CTI Feed evaluation/rating by all validators, the rating results of each validator are distributed to all validators via a gossip protocol [29], in order for all validators to be able to form equation (1) and further proceed with the calculation of the validator performance metrics, and further proceed with the calculation of the validator performance metrics, based on equations (2) and (4). All validators are able to have access to all ratings performed by any other validator.

The proposed PoQ mechanism ensures the distribution of the evaluation/rating results across the selected members of the process and receives feedback based on a voting procedure, the result of which determines the finalisation of the block transaction on the ledger. Only the selected validators have voting rights and those are the only ones that can monitor and verify the production of the blocks.

The consensus algorithm requires the agreement among the q – first best performant validators, where q – first is the number of the first validators of the ordered list. If i is the number of validators, then q should be much smaller than i, *i.e.*, $q \ll i$.

Each validator is expected to provide as an outcome, the production of an ordered list, from the higher performant validator to the lower one, per CTI Feed, based on the objective performance metric in equation (4). If O_{V_m} is the produced ordered list from each validator, each element pair (o_z, PERF_z), with $z \in [1..i]$ and not necessarily $z = m$, represents the validator's V_m, $m \in [1..i]$ position in the list, along with its performance PERF, as follows:

$$O_{V_m} = <\overbrace{(o_1, \mathrm{PERF}_1), (o_2, \mathrm{PERF}_2), ..}^{q\text{–first}}, (o_i, \mathrm{PERF}_i)>. \quad (5)$$

The final ordered list O_{V_m} to be sent by each validator will contain only the first q – first elements. The proposed algorithm (Algorithm 2) ensures that the validators who find themselves in the q – first best performant list and share their own produced full ordered list with the rest of the validators' community as consensus proposals. Those proposals can be considered as voting proposals, as described later on. The consensus will be reached on the agreement of the q-first best performant validators, which will be finally stored on the ledger.

Given the fact that a number of u validators ($V_u \subset V_m$, $(m \gg u \geq 1)$) will send their ordered list to the rest of the validators community, a voting mechanism is required to reach a final consensus. Furthermore, $u \geq q$, since at least q different validators are included in q – first lists of all voting proposals, but not less.

The following matrix D_w depicts the ordered list, available for voting assessment:

$$D_{\substack{w \\ u\times 1}} = \begin{pmatrix} \overbrace{\left\langle \left(o_{w_{1_1}}, \mathrm{PERF}_{w_{1_1}}\right), .., \left(o_{w_{1_q}}, \mathrm{PERF}_{w_{1_q}}\right)\right\rangle}^{q\text{–first}} \\ \left\langle \left(o_{w_{2_1}}, \mathrm{PERF}_{w_{2_1}}\right), .., \left(o_{w_{2_q}}, \mathrm{PERF}_{w_{2_q}}\right)\right\rangle \\ \vdots \\ \left\langle \left(o_{w_{u_1}}, \mathrm{PERF}_{w_{u_1}}\right), .., \left(o_{w_{u_q}}, \mathrm{PERF}_{w_{u_q}}\right)\right\rangle \end{pmatrix}. \quad (6)$$

Data: V: Validators
$R_{V_m P_n}$: Validator Rating Matrix
i: Number of selected validators
q: q-first variable
Result: Calculate W (equation (9)) and reach Consensus
(1) initialisation\;
/ * for each validator * /
(2) **for** $m \in [1..i]$**do**
(3) Outlier Detection;
(4) Calculate PERF_{V_m}; //equation (4)
(5) $V_m \longrightarrow O_{V_m}$; //create ordered list equation (5) O_{V_m}
(6) **if**self (PERF) > PERF (O_q)**then**
(7) broadcast (O_{V_m}); //to all validators
(8) **end**
(9) **end**
(10) Construct matrix D_w;//equation (6)
/ * each validator vote on D_w * /
(11) **for** $w \in [1..u]$**do**
(12) **for** $m \in [1..q]$**do**
(13) Construct matrix D_o; //equation (7)
(14) **end**
(15) **end**
(16) Construct matrix E_V; //equation (8)
(17) **do**
(18) calculate W; //equation (9)
(19) **if** *unique winner* **then**
(20) *Consensus* = *TRUE*
(21) **else**
(22) $q = q \pm 1$;
(23) **end**
(24) **While** *Consensus* = *TRUE*;

Algorithm 2: Pseudocode for proof-of-quality algorithm.

In that case, the Proof-of-Vote [30] consensus mechanism can be used, or an order ranking algorithm, such as Kemeny–Young or Borda's count [31, 32], which is a classical method of rank aggregation used in voting systems, where voters specify their preference of candidates as a priority list, which is collectively called a profile of rankings or preferences [33, 34].

In this context, Borda's count voting system mostly satisfies the proposed model's voting requirements, as it fits the q – first model that is applied. In this case, a validator who plays the role of a voting candidate is awarded score points based on the full preferences of each voter (the other validators). A candidate receives points whether being in the first-place preference of other voters or not. The main rule is that the higher the preference by the voter is, the more points the candidate collects.

It is expected that the higher the value of q is, the better the probability of reaching consensus faster is, as Borda points are distributed to more validators, and at the same time, the higher the fairness is, the higher the probability of malicious validators being selected is and vice versa. On the other side, the value of q should be kept as low as possible in order to preserve the efficiency of the system. Furthermore, if consensus is not reached, meaning that there might be a draw between 2 or more validators, the algorithm either increases progressively the value of q in order to increase the chances of establishing an agreement, or it chooses randomly one out of the validators who collected the same Borda points during the voting process.

During the voting procedure with u validators as candidates, the voting list is limited to q validators, as seen in equation (6); a first-place validator earns q Borda points, a second-place earns $q-1$ Borda points, and so on. The validator, who is ranked last among the q-first validators, earns just one Borda point.

By applying this logic, the voting results, depicting earned voting points, can be depicted in the following matrix in equation (7), but this time without containing the performance information per validator PERF, which in this stage is considered as redundant.

The proposed voting mechanism results assume that agreement has been reached by accepting the voting outcome. The validator with the highest overall number of Borda points wins and then is authorised to create the

next block entry in the ledger, an entry which was validated by a distributed mechanism based on node reputation history and pre-defined quality parameters:

$$D_{\substack{o\\u\times q}} = \begin{pmatrix} \left(o_{w_{1_1}} = q\right) & \left(o_{w_{1_2}} = q-1\right) & \cdots & \left(o_{w_{1_q}} = 1\right) \\ \left(o_{w_{2_1}} = q\right) & \left(o_{w_{2_2}} = q-1\right) & \cdots & \left(o_{w_{2_q}} = 1\right) \\ \vdots & & & \\ \left(o_{w_{u_1}} = q\right) & \left(o_{w_{u_2}} = q-1\right) & \cdots & \left(o_{w_{u_q}} = 1\right) \end{pmatrix}. \quad (7)$$

Each row can now be seen as an ordered list, carrying the Borda points per validator. Each variable O_w represents a specific validator which is rated under the Borda mechanism and is unique per ordered list (each row of D_w matrix) but can exist also in the following ordered lists, since the same validator can be rated by others at the same time. Assuming that y is the number of unique validators who are subject of the voting procedure, with each $y < m$, where m is the total number of the validators Vm and z is the number of occurrence of each unique validator; the results of the voting process per validator can be derived from the following matrix:

$$E_{\substack{V_y\\y\times 1}} = \begin{pmatrix} \sum_{x=1}^{z_1} D_{O_x} \\ \sum_{x=1}^{z_2} D_{O_x} \\ \vdots \\ \sum_{x=1}^{z_y} D_{O_x} \end{pmatrix}. \quad (8)$$

Each sum of the matrix of equation (8) represents the total Borda points which are each unique validator collected during the voting process. The winner of the voting process can be derived from equation (9), the maximum value of which corresponds to the related validator:

$$W = \max E_V. \quad (9)$$

The winning validator is then authorised by the proof-of-quality consensus algorithm to write the next block on the ledger.

3.5. Dynamic Reputation Mechanism and CTI Feed and Source Evaluation. The reputation mechanism keeps track of validators' reputation and credibility while playing a key role for the validator selection mechanism (VSM), which selects the validators to perform the CTI Feed evaluation. Furthermore, it contributes to the enriched CTI Feed evaluation and the CTI Feed Source reputation, as described below.

Trust is a metric of reputation. Selected validators with consistently high values of reputation, and by extension, trustworthiness can provide more reliable and malicious-free evaluation results.

3.5.1. Validator Reputation. The stored validator performance per block is shown in the following matrix A:

$$A_{\substack{V_mB_b\\i\times p}} = \begin{pmatrix} \mathrm{PERF}_{V_1B_1} & \mathrm{PERF}_{V_1B_2} & \cdots & \mathrm{PERF}_{V_1B_p} \\ \mathrm{PERF}_{V_2B_1} & \mathrm{PERF}_{V_2B_2} & \cdots & \mathrm{PERF}_{V_2B_p} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{PERF}_{V_iB_1} & \mathrm{PERF}_{V_iB_2} & \cdots & \mathrm{PERF}_{V_iB_p} \end{pmatrix}. \quad (10)$$

As a result of the consensus mechanism, the validators have agreed on the ordered list of the best performant ones per block. Based on those results, a factor $c_z = (1/z)$, $z \in [1..u]$, can be applied, which favours the best performing validators in comparison to lower performing ones, where z is the position of a validator V_m, $m \in [1..i]$, in the agreed ordered list O. The higher in the ordered list a validator is, the higher the factor c is, and by that, the reputation of the best performing validator is increased in comparison to the rest.

The reputation REP_{V_m} of each validator V_m, $m \in [1..i]$, is linked to its own archived performance on the existing blocks B_b, $b \in [1..p]$, of the ledger, where p is the total number of blocks:

$$\mathrm{REP}_{V_m} = \frac{1}{p}\sum_{b=1}^{p} c_z A_{V_mB_b}, \quad \forall A_{V_mB_b} > 0,\ \forall m \in [1..i]. \quad (11)$$

By publishing a block, the selected validator automatically increases the overall rank of its reputation. The reputation of contributing validators to the consensus mechanism is also increased.

3.5.2. Interim CTI Feed Evaluation. Validators CTI Feed ratings are stored in the matrix of equation (1). The interim CTI Feed evaluation score is based on the average of the rating mean values which were received from each validator and for all quality parameters. Anomaly or outlier detection and removal can be already included in this procedure, to avoid skewing the results. The metric's name includes the word "interim" because this metric will be used as the base for a more enriched calculation later, including the validators reputation metric (equation (11)).

So, the interim evaluation $i\mathrm{EVAL}$ of a CTI Feed F_f, based on ratings of validators V_m, $m \in [1..i]$, per quality parameter P_n, $n \in [1..j]$, where i is the total number of selected validators and j is the total number of the quality parameters respectively, is as follows:

$$i\mathrm{EVAL}_{F_f} = \frac{1}{j}\sum_{n=1}^{j}\frac{1}{i}\sum_{m=1}^{i} R_{V_mP_n}. \quad (12)$$

3.5.3. Enriched CTI Feed Evaluation. Having calculated the reputation REP_{V_m} of the validators V_m, $m \in [1..i]$, in equation (11), we are in a position to add this metric in the interim evaluation $i\mathrm{EVAL}$ of a CTI Feed F_f which was calculated before (equation (12)). This way, we emphasise the importance of the validators' reputation to the final evaluation of the CTI Feeds. The validators that are going to

be considered are only those who managed to proceed with the voting process, as per equation (8).

In this case, we consider $r_a = \mathrm{REP}_{V_a}$ as the reputation factor of each validator V_a, $a \in [1..y]$, with $y < m$, where m is the total number of the validators Vm. The enriched evaluation $eEVAL$ of a CTI Feed F_f embedding the validator reputation is

$$e\mathrm{EVAL}_{F_f} = \frac{1}{j}\sum_{n=1}^{j}\frac{1}{y}\sum_{a=1}^{y} r_a * R_{V_a P_n}. \tag{13}$$

3.5.4. CTI Feed Source Reputation. In addition to the evaluation of the CTI Feeds, the reputation of the CTI Feed Sources can be further evaluated as a more extended approach. The CTI Feed Source reputation is linked to the archived evaluation of each own published CTI Feed, and since more CTI Feeds are added, therefore, the Feed Source reputation will be evolving.

The stored CTI Feed evaluation metric per block is shown in the following matrix C:

$$C_{\substack{\mathrm{F_f B_b} \\ k\times p}} = \begin{pmatrix} e\mathrm{EVAL}_{F_1B_1} & \cdots & e\mathrm{EVAL}_{F_1B_p} \\ e\mathrm{EVAL}_{F_2B_1} & \cdots & e\mathrm{EVAL}_{F_2B_p} \\ \vdots & \ddots & \vdots \\ e\mathrm{EVAL}_{F_kB_1} & \cdots & e\mathrm{EVAL}_{F_kB_p} \end{pmatrix}. \tag{14}$$

While considering the CTI Feed Source evaluation, an additional weighted gravity factor g can be applied. By that way, the latest CTI Feed evaluation data will be taken into stronger consideration than the past ones. Cyber Threat environment is evolving by nature, while informed decisions have to be taken on time and as accurately as possible. This requirement can be underpinned to a good extent by assigning more importance to the latest intelligence CTI data, while also taking into consideration the past ones to a certain extent. So, the information stored to the latest block B_b, $b \in [1,..,p]$, will be assigned to a higher gravity/importance factor $g_b = (b/p)$, $b \in [1,..,p]$, than the previous ones.

The reputation REP_{S_s} of each CTI Feed Source S_s, $s \in [1,..,q]$, is derived from the own CTI Feed evaluation on the existing blocks B_b, $b \in [1..p]$, of the ledger:

$$\mathrm{REP}_{S_s} = \frac{1}{p}\sum_{b=1}^{p}\frac{g_p}{f}\sum_{f=1}^{k} C_{F_fB_b}, \forall C_{F_fB_b} > 0. \tag{15}$$

3.5.5. Time-Aging Factors. In addition to the factors r_m and g_b mentioned above, which describe a weighted approach based on the most recent transactions regardless of the time window between them, a time-related gravity factor can also be applied, as an time – aging or time – decay factor.

Metrics that were presented above, such as REP_V and REP_S, can be further refined or adjusted by adding a more representative trust value, which is time. Combining the most recent transactions in parallel with the time-aging factor can be used to detect and filter arbitrary behaviour changes, as more recent ledger data contributes the most; thus, an entity will be filtered out for misbehaviour.

In addition, the validators and CTI Sources would be motivated to offer more frequent and better quality data and feedback, since old entries with low-quality feedback can be forgotten and positively balanced out with more recent transactions. The time-aging mechanism can be tuned to be responsive to behaviour changes, by increasing the weight that is given to newer transactions accordingly.

Based on the above, a nonlinear aging-factor function can be applied on the metrics of REP_V and REP_S (equations (11) and (15)) in the form of a fading variable [35].

The function is shown in equation (16), where A_T is aging – factor, REP is either the reputation of a validator or a CTI Source, and f is the fading factor with an exponent t_n being the time difference between the last n ratings. In addition, time can be used also as an absolute value t, defining the time window between present and a specific time in past, including all records in the ledger that were captured during this period. In either ways, the computation of the metrics is done in a more efficient way, not having to consider all the records stored in the ledger, rather focusing on the latest defined ones, contributing to a more effective, responsive, and scalable results:

$$\begin{aligned} A_{T_n} &= f^{t_n} * \mathrm{REP}, \\ A_T &= f^{t} * \mathrm{REP}. \end{aligned} \tag{16}$$

3.5.6. Block Layers. Each block of the ledger is logically separated and divided in 3 layers, which are linked together and not meant to be stored independently (Figure 3), while they are added to the chain only when consensus is reached, via Algorithm 2.

(1) The evaluated CTI Feeds are stored on the first layer, following a particular data model, the STIX data model, as an example. For those CTI Feeds that do not follow the STIX model, a conversion mechanism could be applied so that all stored data follow the common and widely recognised data model [36, 37]. The Feed's Source information is also included in this layer as a reference point. Note that the proposed model is independent of the use of a specific data model, and STIX is only used as an example. Therefore, it can easily accommodate other equally efficient data models, such as MISP.

(2) The second logical layer stores the CTI Feed's evaluation rating results provided by the validators.

(3) The third layer stores an ordered list which contains the validators' performance, based on their ratings and the performance metrics during the CTI Feed evaluation process. The validators' reputation is not explicitly stored on the chain, while it can be calculated ad hoc based on the performance historical values stored in this layer across the ledger.

This way, the data stored in each logical block layer are immutable and distributed among the blockchain users, containing metadata, references, and relationships, useful to create a dynamic and continuously enriched environment for

(i) Reliably sharing validated CTI

(ii) Calculating the reputation of CTI Feed Sources

(iii) Setting the foundation for a critical mass of reputable validators to carry on with future CTI Feed evaluations and preserving the fairness of the system

Some of the aspects of the CTI Feeds ratings and, therefore, of the validators' performance metrics are subjectively measured, while some other are measured by applying objective criteria. For example, the quality parameters of CTI Feeds are rated by each validator on a different basis according to the discretion and perception of each validator. On the contrary, the anomaly/outlier detection and removal is a decision which is left to the consensus algorithm to be dealt with, by using globally definable metrics on a horizontal approach (cross model).

3.5.7. System FlowChart. The flowchart of the system is depicted in Figure 6 and described as follows:

Step 1: CTI Feed is made available for evaluation by a CTI Source.

Step 2: If the CTI Feed is not based on the selected data model (e.g., the STIX data model), a conversion mechanism is applied to convert the CTI Feed data to the desired model [36, 37]. The conversion mechanism is beyond the scope of this article.

Step 3: CTI Feed Sources and Consumers are roles interchangeable with the validator role, as described in Section 3 and, by that, eligible to become validators. Once the candidates are subscribed to participate as candidate validators, they are screened by the Validator Selection Mechanism (VSM), against the following criteria:

(i) Their Reputation stored in the third layer of the ledger's blocks,

(ii) IoC (e.g., malicious IPs and domain names) already stored in the first layer of the ledger's blocks. This criterion is applied to exclude the chance that a potential malicious validator is participating in the evaluation process. For example, if a validator is connected via an IP or even a resolved domain name which are registered in the blockchain as malicious ones, then those validators will be excluded from the CTI Feed evaluation process.

After the final selection of validators, they are engaged in the evaluation process, in step 4, where the CTI Feeds are available from the previous step.

Step 4: Each selected validator is rating the under evaluation CTI Feed (Figure 4), against each one of a pre-defined set of CTI Feed quality criteria, as shown in Table 2.

Step 5: The ratings of each validator are distributed to the rest of the validator group via a gossip protocol.

Step 6: Once the validators complete their CTI Feed evaluation/rating, the ratings are distributed across all of them via a gossip protocol in order to ensure that all validators are able to have access to all ratings performed by any other validator. The goal is to reach a consensus on the q-first best performing validators.

Step 7: The block is registered in the ledger once the validator community has reached a consensus.

4. Theoretical Model Simulation and Analysis

In this section, we will present a practical simulation of the model, using a probabilistic approach to define the variables of the system and the described conditions as well. This simulation includes the required abstraction and assumptions in order to specify the domain of application of the model. The simulation environment, available on GitHub [38], was developed in PHP v.7.2 programming language and runs on a server with the following technical specifications:

(i) Processor: Intel(R) Xeon(R) Silver 4114 CPU @ 2.20 GHz (4 cores)

(ii) Memory: 8 GB

(iii) Operating System: CentOS 7

The parameters of the simulation are presented below:

(i) Number of nonmalicious validators: variable shows the total number of nonmalicious or non-misbehaving validators.

(ii) Number of malicious validators: variable shows the number of malicious ones inserted into the simulation in order to assess the negative impact as well as the tolerance of the system. The total number of validators equals the number of nonmalicious and malicious validators as a sum.

(iii) Number of quality parameters: 10, as per Table 2.

(iv) q-first: variable defines the number of the validators to participate into the voting procedure.

(v) Offset of malicious validator rating: variable defines the rating threshold which is closer to the upper and lower limits of the rating boundaries [0..1] for skewing the rating results, based on a potential malicious rating behaviour. Normally, it would be expected that, in the application scope of this article, malicious validators will rate close to 0 or close to 1 in order to skew the rating results to the possible extent and hence decrease the quality of the CTI Feed evaluation process. This variable is set to define the limits of this potential behaviour, shown in Figure 7. This variable is defined to take values in the set of [0..50%]. The variable value of 50 is considered the maximum and simulates that malicious validators are behaving probabilistically similar as all the rest of the nonmalicious validators. The lower

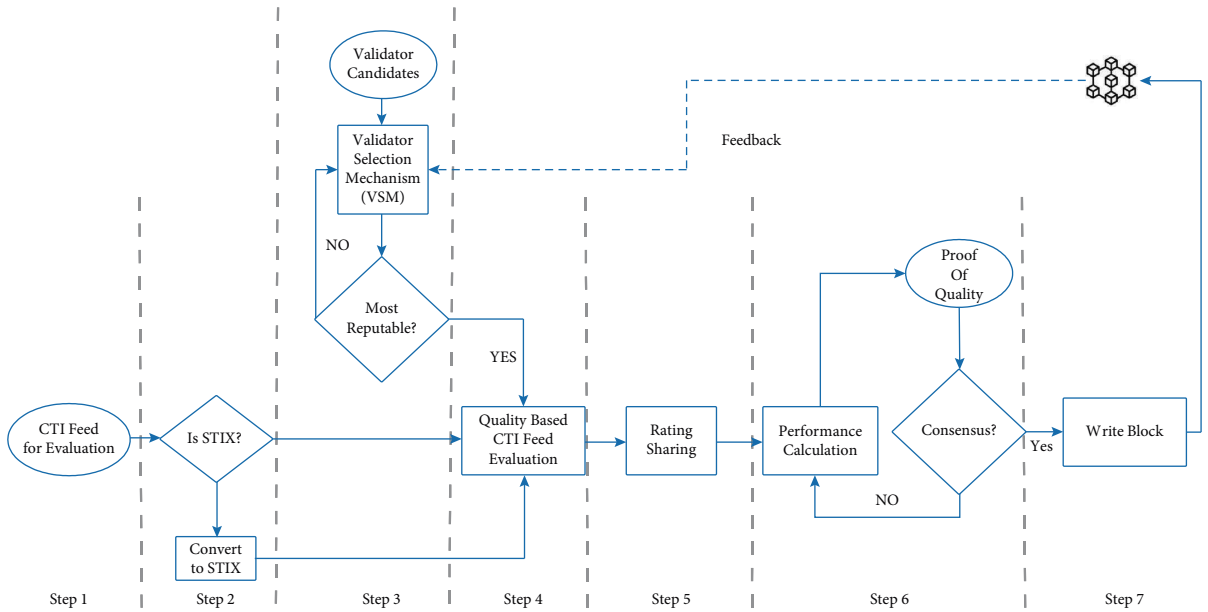

Figure 6: Model's flowchart.

the value is (closer to 0%), the higher the skewing impact on the overall evaluation ratings is, and, at the same time, the outliers are detected more efficiently by our model. On the contrary, the higher the value is (closer to 50%), the lower the malicious impact is and the ability of the model's outlier detection decreases.

In this particular simulation, outlier detection is inherited already by the squared deviation from the mean (SDM) equation, which is downgrading the influence of the malicious validators, not by removing them but rather by decreasing their contribution to the overall process.

The simulation covers the CTI Feed Rating procedure and the validator performance calculation, as well as the PoQ algorithm implementation, providing a proof of the tolerance and security against malicious actors. The objective of the simulation is to show that the footprint of malicious validators into the final selection list is as close to zero as possible, even if the ratio of nonmalicious vs, maliciously acting validators is even close to 1: 30. The aforementioned aspects constitute the foundation of an efficient performance of the proposed model, leading to a defined and tolerant reputation-based mechanism for CTI Feed and source evaluation.

The validator selection mechanism and the feedback mechanism were left outside the scope of this simulation, as they require a more robust proof-of-concept environment, which will follow in our future work.

The following assumptions were made during the development:

(i) The rating of all validators against the 10 pre-defined CTI Feed quality parameters was generated based on a random-based number generator using PHP, with values as float numbers between [0..1] with 2 decimals.

(ii) Especially referring to the rating of the malicious validators, this took place similarly as described above, but limiting each rating by applying an offset variable threshold. By that threshold, we are simulating a potential malicious rating, which normally would not follow a normal distribution of the rest of the ratings, rather it would be allocated closer to the upper or lower limits of the space [0..1] with the malicious objective of skewing the rating results as much as possible. The maximum offset limit which is applied is 45%, since a value even closer to 50% would not be able to distinguish the malicious from the nonmalicious rating behaviour.

(iii) On the contrary, the nonmalicious validators are expected to have a normal-based distribution on their rating, of course not excluding the chance that they may rate specific CTI Feeds on the extremities of the rating span [0..1].

(iv) The selection of the validators is assumed to have taken place during the VSM and feedback mechanism functionalities, which are not performed in this theoretical model development.

(v) The value of 0.5% is set as an acceptable health KPI (Key Performance Indicator) of a malicious footprint in the validators' pool.

4.1. Simulation Results. The simulation results are depicted in the table and graph in Figures 8 and 9, respectively. During the simulation, the following aspects were taken into consideration, as they could be applied during potential on production and operational usage of the model:

(i) Several pairs of numbers between validators and malicious validators were applied, a representative

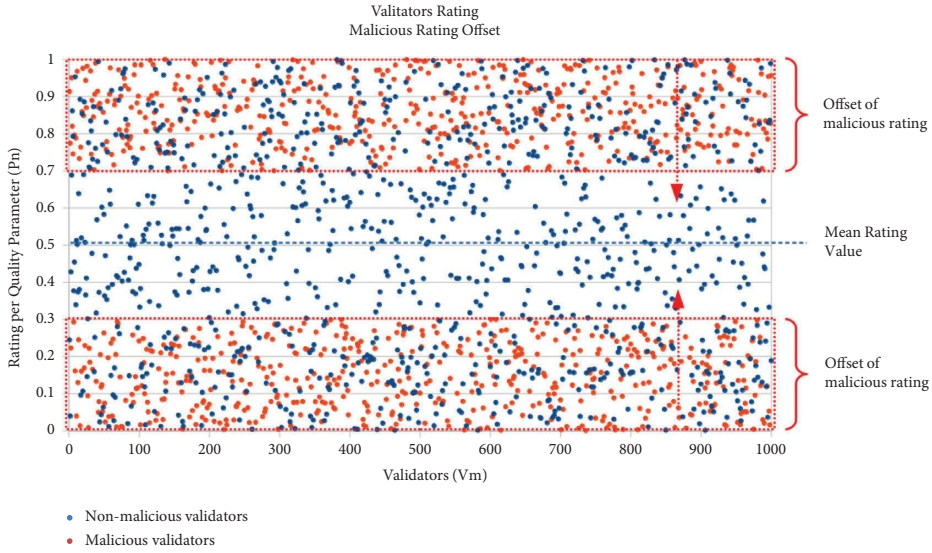

Figure 7: Malicious rating offset.

part of which is shown in the figure. It is noted that the respective ratio was also adapted, starting from 4: 1 and even considering a ratio of 1: 30, which represents a vast dominance of malicious validators against legitimate ones.

(ii) As mentioned earlier, malicious validators are assumed to rate the CTI Feeds closer to the upper and lower limits of the rating span [0..1], hence, not under a normal distribution. During this simulation, it is shown that the malicious offset from rating limits was even close to 45%, meaning that they were almost blended in the rating of nonmalicious validators, making the outlier detection even more difficult and noneffective.

(iii) The q-first parameter was kept in the value of 5 in most of the cases, which represents a realistic value of finalist validators to participate to the voting procedure. The lower this value is, the more tolerance to malicious validators it provides but, at the same time, the less fairness, and vice versa.

The graphs depicted in Figures 10–12 show the tolerance of the model against malicious validators for various ratios (nonmalicious vs. malicious validators): 1 : 3, 1 : 10, and 1 : 50, respectively. The graphs show that the malicious footprint is preserved below 0.5%, even though the malicious validators are significantly higher than nonmalicious validators, with the variable of malicious rating offset close to 45%. Those results show that even if the malicious validators are considered as almost blended-in with the rest of the nonmalicious validators, the model has the capability to distinguish them very efficiently, preserving the malicious footprint below 0.5%, which was set previously as a health status KPI of the model.

Those results lead furthermore to the conclusion that the voting mechanism, via which the CTI Feeds are evaluated, can ensure high level of trust amongst the voters (validators), preserving the quality of the CTI Feed evaluations during future iterations, archiving all related information in the distributed ledger for further reference.

4.2. System Initialisation. The system's initialisation is considered vital to the total performance of the model. As shown during the simulation results, the existence of a malicious-proof pool of validators is very crucial, due to the fact that validators are mainly set to be selected out of this pool, in order to participate on the evaluation process. Even though there is a chance that malicious validators will be selected, the model shows that it is tolerant enough, even if the ratio versus the malicious validators is significantly low. Once the system is initially configured to perform the first sets of evaluation iterations, it is reasonable that there will be no best reputable cluster which the validator selection mechanism will select the validators from. So, it is essential that, during the first iterations, the validators should be selected carefully in order to avoid random-based selections which will lead to a nonmalicious-proof validators' core pool.

4.3. Key Consideration Analysis. In this section, the key considerations of the proposed CTI-sharing mechanism are analysed further, including the results of the theoretical model simulation.

4.3.1. Fairness. The VSM process is considered as a key part of the system, due to the fact that the CTI Feed evaluation and CTI Sources reputation are also based on the reputation of the validators. During the VSM process, the validators are selected via a cluster-based separation and are most likely to be selected from the cluster which holds the most reputable validators. Furthermore, less reputable validators have opportunities to increase their

Model Simulation Parameters	q-first parameter:5											
num of non-malicious validators	20	50	100	500	1000	1000	2000	5000	10 K	10 K	10 K	20 K
num of maliciously acting validators	20	50	100	500	1000	2000	5000	15 K	30 K	100 K	500 K	1 M
non-malicious vs malicious ratio	1:1	1:1	1:1	1:1	1:1	1:2	1:2.5	1:3	1:3	1:10	1:50	1:50
malicious offset from rating limits – max tolerance limit	45%	45%	45%	45%	45%	45%	45%	45%	45%	45%	45%	45%
Malicious Footprint in Voting List (any place)	7.5%	2.7%	2.3%	1%	0.8%	1.2%	2.1%	<0.5%	<0.5%	4.8%	10.8%	6.4%
Malicious Footprint in Voting List (1st place)	<5%	<1%	<1%	<0.5%	<0.5%	<1%	1.1%	<<0.5%	<<0.5%	2.4%	<5%	<5%
malicious offset from rating limits – max optimized tolerance limit	39%	42%	43%	44%	44%	44%	44%	45%	45%	44%	43%	43%
Malicious Footprint in Voting List (any place)	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%	<0.5%
Malicious Footprint in Voting List (1st place)	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%	<<0.5%

Figure 8: Simulation results.

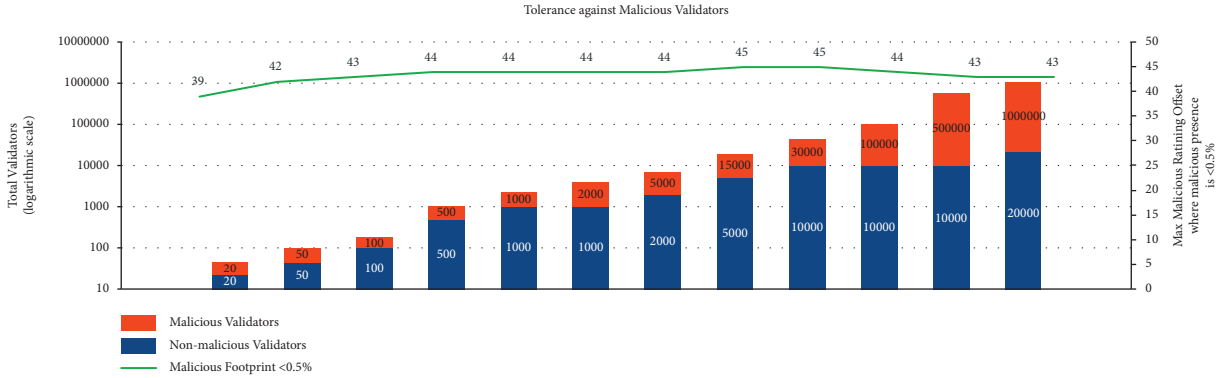

Figure 9: Tolerance against malicious validators.

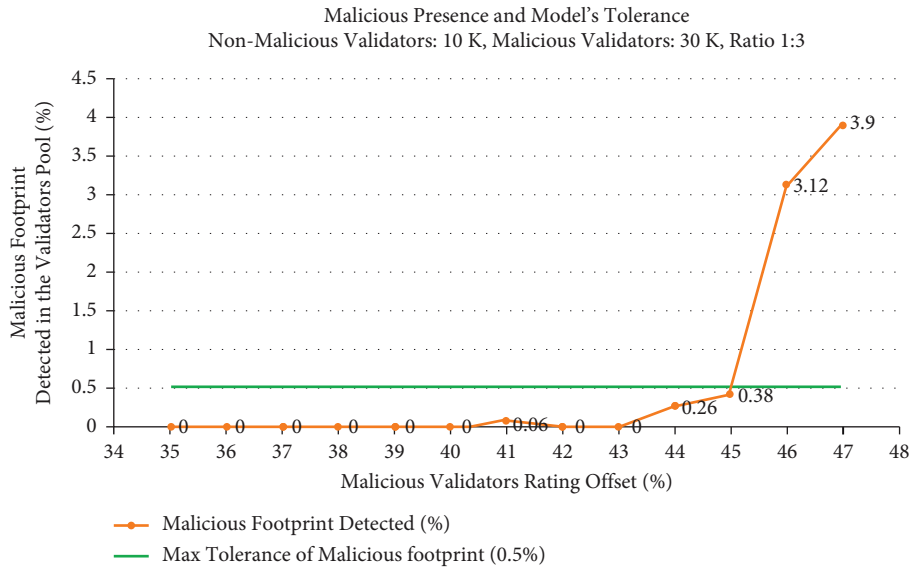

Figure 10: Tolerance against malicious validators (ratio 1 : 3).

reputation, via the application of a weighted random choice mechanism, which is implemented on top, in order to select validators from less reputable clusters, based on adjustable weights. This additional feature increases the fairness of the proposed system, ensuring that all validators' candidates have eventually chances to be selected as validators. In addition, consensus is achieved by using a voting-based mechanism among all validators, which by principle is considered as the most fair mechanism, in comparison to other consensus mechanisms which require different types of resources to achieve agreement.

4.3.2. Scalability. Blockchain scales best with lightweight metadata, which can be retrieved and analysed fast and efficiently. A system can be considered as scalable when the overall performance does not decrease with the addition of

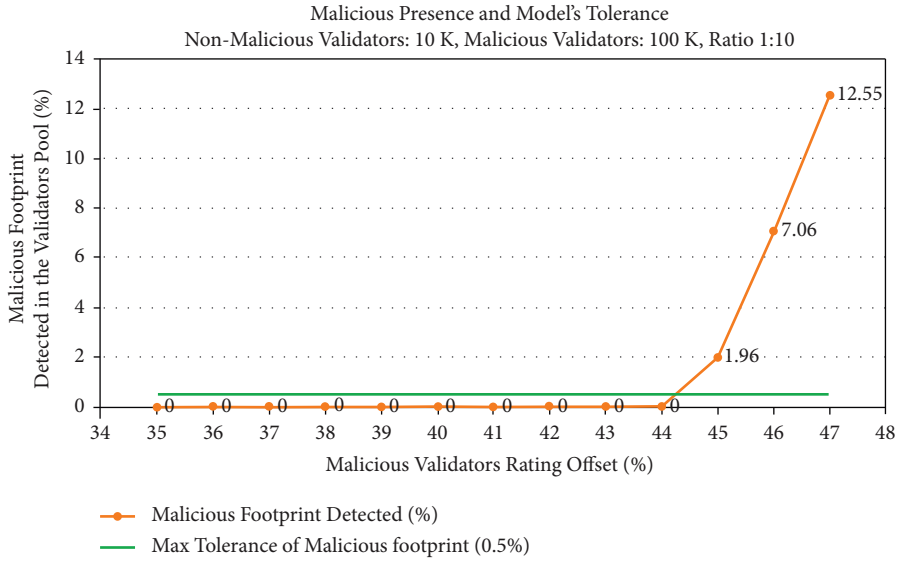

Figure 11: Tolerance against malicious validators (ratio 1 : 10).

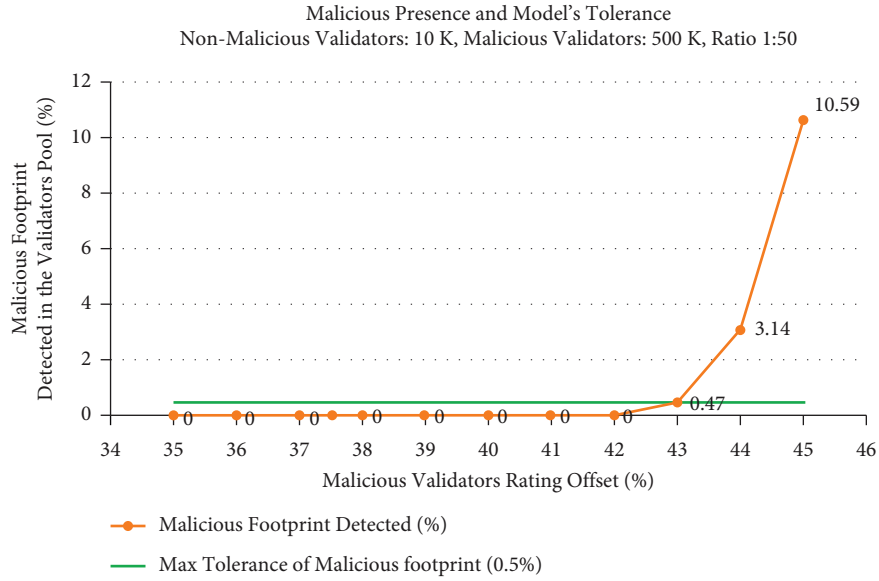

Figure 12: Tolerance against malicious validators (ratio 1 : 50).

nodes. In this context, the proposed ledger is divided into three logical layers. The information, which is recorded in the ledger per block, is the evaluated CTI Feed itself in the first layer, the CTI Feed evaluation in the second one, and the validator performance as the agreed ordered list in the third one. Furthermore, the rating matrix is proposed to be exchanged via a gossip protocol in order to preserve bandwidth during the data exchange. Although there is no analytical data available yet, the data storage and the bandwidth requirements are expected to be efficient. Related use case scenarios will be produced during the proof-of-concept development in our future work.

4.3.3. Consensus. The proof-of-quality consensus algorithm is proposed to be based on the Borda voting system or on any other voting-based mechanisms, preserving further fairness of the system, as mentioned above. No special resources are required to reach consensus apart from participation in the voting procedure by the validators. Furthermore, the absolute finality method is applied, which means that a block transaction is immediately finalised after its inclusion in the blockchain, in comparison to the probabilistic finality, where the block once gets deeper into the chain the chance of its reverting decreases [39].

Table 3: Comparison with existing research studies.

Proposals	Key considerations			
	Reliability and quality	Reputation and trust	Tolerance and security	Consensus
He et al. [5]	Similarity criteria are addressed via a smart contract algorithm	No reputation or trust criteria are defined	Tolerance and security topics are not addressed	No specific consensus mechanism is referenced
Gong and Lee [6]	Abstract data verification mechanism	Abstract evaluation of contributors credibility	Presents a mechanism to prevent sybil attacks from malicious contributors	Abstract miner-based consensus mechanism
Mendez Mena and Yang [7]	No quality criteria are defined	Trust is established only via utilising a permissioned block chain environment	Tolerance and security topics are not addressed	Proof of authority
Cha et al. [8]	CTI data are subject to verification via a collaborative architecture but is not clear under which criteria	No reference to reputation criteria or supported mechanisms	No reference to tolerance against malicious activities	No reference to consensus algorithms
Meier et al. [11]	The quality evaluation is based on correlation and contribution graphs with no detailed quality criteria	No reputation or trust metrics are addressed, since this proposal does not require a ground truth	Robust against a small percentage of dishonest contributors but susceptible to malicious attempts of a larger percentage	Not applicable
Riesco et al. [9]	Quality criteria of identity, authority, motive, access, timeliness, and consistency are defined	Trust is presented as an overall benefit using a blockchain-based network, but there is no reference of quantification of reputation and/or trust between peers; a Cobb–Douglas utility function is presented combining trust and quality	Inherited by the block chain technology with no specific reference	No reference to consensus algorithms
Wu et al. [12]	Quality criteria of completeness, freshness and relevance are applied but the assessment is performed under a vague methodology	The reputation assessment is using EigenTrust algorithm [14] to calculate a reputation score based on peer transaction histories and produce global trust values for all participants	No reference to tolerance against malicious activities	It is inferred that the consensus algorithm of proof of elapsed time (PoET) is proposed
Proposed solution	The model depends on literature-referenced quality criteria evaluation with explicit methodology, metrics and indicators	Trust is created via specific mechanisms and processes as well as the reputation is derived from the data stored on the ledger as a historical immutable reference	The theoretical simulation showed that there is tolerance against malicious validators even if the ratio of legitimate vs malicious validators is 1 : 50	The model proposes a new consensus algorithm, namely, proof-of-quality which is based on a voting procedure among the best performant validators

4.3.4. Integrity and Consistency. The integrity of the data stored in the ledger and by extension the integrity of the overall system is preserved by the inherited immutability characteristics of the blockchain itself, preventing alteration of transactions that have already been confirmed and agreed.

4.3.5. Reliability and Quality. The reliability of the system is achieved via the CTI Feed quality evaluation via the selected validators, referring to the value it brings to the CTI community by utilising quality-based parameters.

4.3.6. Reputation and Trust. The proposed system uses constantly updated reputation metrics, based on the historical records of the system's ledger, which enables the trust among the stakeholders, either consuming or contributing to CTI Feed evaluation. The reputation and trust are started and based on a green-field approach derived solely from the CTI Feed data evaluation process and not based on any existing reputation that an organisation might already have. It needs to be highlighted that, in the context of this article, reliability and trust are approached differently; the first one being a quantitative criterion linked to quality metrics, while the second one is a qualitative criterion linked to reputation metrics.

4.3.7. Tolerance and Security. The overall observations of the theoretical simulation of our model is that it provides a very efficient tolerance against malicious or nonlegitimate behaving validators, even if the ratio is 1: 50 (nonmalicious versus malicious). Furthermore, there are plenty of options to adjust the tolerance levels according to the operational requirements.

4.4. Comparison with Existing Research Studies. This section, is presenting a comparison between the existing research studies and our proposed model, depicting which key considerations are supported by each proposal, in order to highlight the benefits and value of our work. The key considerations which are shown in Table 3 are the ones which provide a value of comparison, since the ones excluded are either considered as a common baseline for all proposals in the ground that all of them use blockchain technology or they are of lower importance of comparison.

After such a comparison matrix, we believe that the proposed solutions so far do not cover a broad range of aspects from a CTI lifecycle perspective, but rather focus on a limited area of conceptual or technical proposals. On the contrary, our research proposes a coherent methodology of a trust-enabled environment, based on explicit metrics and performance indicators, supported by mechanisms towards this end. Furthermore, a new consensus algorithm is proposed, namely, the proof-of-quality algorithm, via which consensus is achieved based on a voting process approach. In addition, our proposal enhances the concept of reliability and trust, based on quality parameters, which leads by extension to the capability of evaluating not only CTI Feeds but also the reputation of CTI Sources feature which is missing from the existing proposals.

5. Conclusions: Summary

In this article, we propose a new reputation-based CTI Feed evaluation system called Awareness Architecture Based on Blockchain CTI Convergence $(ABC)^2$, which deals with the CTI sharing using blockchain technology. CTI Feed evaluation is the primary goal of the system, based on a definite set of quality-based parameters. The evaluation is conducted by validators who are part of the CTI-sharing community. The quality parameters, on which the evaluation of the CTI Feed is based on, are considered equally important, and if required, each parameter can be weighted accordingly on an ad hoc basis, in line with the applied methodology and context.

Furthermore, a new consensus algorithm is proposed, which bases its consensus results on a voting process. Once the evaluation results have been distributed to all validators, each validator is called to create an ordered list, containing q most performant ones. If a validator finds itself in the q – first most performant ones in the self-produced ordered list, it shares the list among other validators who fulfil the same criterion and make the list available for a voting process. The PoQ algorithm ensures the consensus of the community and the results are archived in the three-logical layer blocks of the ledger. Based on the data stored on the ledger, the CTI Source reputation is possible to be calculated, based on the own archived CTI Feed data which has already been evaluated.

Among the key aspects of the model, which is the ability to select validators via the Validator Selection Mechanism (VSM), for conducting the CTI evaluation process, each validator is selected mainly based on its reputation and derived from historical data derived from the ledger, by applying a feedback mechanism. This historical data provide available evidence of the validators' past behaviour and contribution to past evaluation metrics and data. VSM is meant to collect and analyse this evidence, which results in a reputation score, further to be taken into account whether a specific validator should be considered as trusted and further selected to contribute further to the CTI Feed evaluation process. Similar reputation metrics can be applied also in order to calculate the reputation of the CTI Sources, based on the relevant results of its CTI Feed evaluation.

After conducting research on the existing literature and proposals on similar scopes, focusing on the CTI evaluation, and storing and sharing mechanisms, we created a comparison matrix, showing the benefits and advantages of our holistic proposal, on key aspects such as Reliability, Quality, Reputation, Security, and Consensus. Furthermore, during the simulation of the model's performance, it is shown that our model has significant tolerance on malicious behaviour which will potentially try to skew the CTI performance rating results, showing that even with a 1 : 50 ratio of legitimate vs. malicious validators, the model produces significantly secure and legitimate evaluation results.

Our future work will be focused on improving the model and developing a Proof-of-Concept (PoC) environment to demonstrate the theoretical results presented earlier. The PoC will materialise the PoQ and VSM algorithms, will include real CTI Feeds mostly from existing CTI Feed dissemination platforms, and is planned to engage real validators from the CTI community, while the evaluation will be based on the already referred quality criteria. Furthermore, one of our objectives is to develop this model as a dynamic feeding mechanism, which will further contribute to a near real-time Dynamic Risk Management concept, where the analysis of the historical data which is stored in the proposed blockchain ledger could play a significant role.

Data Availability

The code that enabled the production of the probabilistic data presented in this article is located in the publicly accessed GitHub repository (https://github.com/dimhatzi/PoQ/blob/main/poq).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] Enisa, "ENISA Threat Landscape 2021," ENISA, Attiki, Greece, Tech. Rep, Oct 2021.

[2] R. Brown and R. M. Lee, "SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, Scandinavia, UK, 2021, https://www.sans.org/white-papers/40080/ Tech. Rep.

[3] Enisa, *ENISA Threat Landscape 2020*, ENISA, Tech. Rep, Oct 2020.

[4] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, "Cyber threat intelligence sharing: survey and research directions," *Computers & Security*, vol. 87, Article ID 101589,

2019, https://www.sciencedirect.com/science/article/pii/S016740481830467X.

[5] S. He, J. Fu, W. Jiang, Y. Cheng, J. Chen, and Z. Guo, "BloTISRT: blockchain-based threat intelligence sharing and rating technology," in *Proceedings of the 2020 International Conference on Cyberspace Innovation of Advanced Technologies*, pp. 524–534, ACM, Guangzhou, China, Dec 2020.

[6] S. Gong and C. Lee, "BLOCIS: blockchain-based cyber threat intelligence sharing framework for sybil-resistance," *Electronics*, vol. 9, no. 3, p. 521, 2020, https://www.mdpi.com/2079-9292/9/3/521.

[7] D. Mendez Mena and B. Yang, "Decentralized actionable cyber threat intelligence for networks and the internet of things," *IoT*, vol. 2, no. 1, pp. 1–16, 2020, https://www.mdpi.com/2624-831X/2/1/1.

[8] J. Cha, S. K. Singh, Y. Pan, and J. H. Park, "Blockchain-based cyber threat intelligence system architecture for sustainable computing," *Sustainability*, vol. 12, no. 16, 2020, https://www.mdpi.com/2071-1050/12/16/6401.

[9] R. Riesco, X. Larriva-Novo, and V. A. Villagra, "Cybersecurity threat intelligence knowledge exchange based on blockchain," *Telecommunication Systems*, vol. 73, no. 2, pp. 259–288, 2020.

[10] D. Homan, I. Shiel, and C. Thorpe, "A new network model for cyber threat intelligence sharing using blockchain technology," in *Proceedings of the 2019 10th IFIP International Conference On New Technologies, Mobility And Security (NTMS)*, pp. 1–6, IEEE, Canary Islands, Spain, Jun 2019.

[11] R. Meier, C. Scherrer, D. Gugelmann, V. Lenders, and L. Vanbever, "Feedrank: a tamper- resistant method for the ranking of cyber threat intelligence feeds," in *Proceedings of the 2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 321–344, Tallinn, Estonia, May 2018.

[12] Y. Wu, Y. Qiao, Y. Ye, and B. Lee, "Towards improved trust in threat intelligence sharing using blockchain and trusted computing," in *Proceedings of the 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 474–481, IEEE, Granada, Spain, Oct 2019.

[13] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Novel trust consensus protocol and blockchain-based trust evaluation system for M2M application services," *Internet of Things*, vol. 7, Article ID 100058, 2019.

[14] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust algorithm for reputation management in P2P networks," in *Proceedings of the Twelfth International Conference on World Wide Web - WWW '03*, p. 640, 2003.

[15] S. Gao, T. Yu, J. Zhu, and W. Cai, "T-PBFT: an EigenTrust-based practical Byzantine fault tolerance consensus algorithm," *China Communications*, vol. 16, no. 12, pp. 111–123, 2019.

[16] E. K. Wang, Z. Liang, C.-M. Chen, S. Kumari, and M. K. Khan, "PoRX: a reputation incentive scheme for blockchain consensus of IIoT," *Future Generation Computer Systems*, vol. 102, pp. 140–151, 2020.

[17] E. K. Wang, R. Sun, C.-M. Chen, Z. Liang, S. Kumari, and M. Khurram Khan, "Proof of X-repute blockchain consensus protocol for IoT systems," *Computers & Security*, vol. 95, Article ID 101871, 2020.

[18] Y. Lee, K. M. Lee, and S. H. Lee, "Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment," *Peer-to-Peer Networking and Applications*, vol. 13, no. 2, pp. 671–683, 2020.

[19] O. A. Oualhaj, A. Mohamed, M. Guizani, and A. Erbad, "Blockchain based decentralized trust management framework," in *Proceedings of the 2020 International Wireless Communications And Mobile Computing (IWCMC)*, pp. 2210–2215, IEEE, Limassol, Cyprus, Jun 2020.

[20] M. T. d. Oliveira, L. H. Reis, D. S. Medeiros, R. C. Carrano, S. D. Olabarriaga, and D. M. Mattos, "Blockchain reputation-based consensus: a scalable and resilient mechanism for distributed mistrusting applications," *Computer Networks*, vol. 179, Article ID 107367, 2020.

[21] J. Feng, X. Zhao, K. Chen, F. Zhao, and G. Zhang, "Towards random-honest miners selection and multi-blocks creation: proof-of-negotiation consensus mechanism in blockchain networks," *Future Generation Computer Systems*, vol. 105, pp. 248–258, 2020.

[22] K. Rantos, A. Spyros, A. Papanikolaou, A. Kritsas, C. Ilioudis, and V. Katos, "Interoperability challenges in the cybersecurity information sharing ecosystem," *Computers*, vol. 9, no. 1, p. 18, 2020.

[23] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & Security*, vol. 72, pp. 212–233, 2018.

[24] D. Chatziamanetoglou and K. Rantos, "Cti blockchain-based sharing using Proof-of-Quality consensus algorithm," in *Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 331–336, Rhodes, Greece, July 2021.

[25] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A density-based algorithm for discovering clusters in large spatial databases with noise," in *Proceedings of the Second International Conference On Knowledge Discovery And Data Mining, Ser. KDD'96*, pp. 226–231, AAAI Press, Miinchen, Germany, 1996.

[26] T. Schaberreiter, V. Kupfersberger, K. Rantos et al., "A quantitative evaluation of trust in the quality of cyber threat intelligence sources," in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–10, ACM, Canterbury, CA, UK, Aug 2019.

[27] D. Schlette, F. Böhm, M. Caselli, and G. Pernul, "Measuring and visualizing cyber threat intelligence quality," *International Journal of Information Security*, vol. 20, no. 1, pp. 21–38, 2021.

[28] H. Griffioen, T. Booij, and C. Doerr, "Quality evaluation of cyber threat intelligence feeds," in *Applied Cryptography and Network Security*, M. Conti, J. Zhou, E. Casalicchio, and A. Spognardi, Eds., pp. 277–296, Springer International Publishing, New York, NY, USA, 2020.

[29] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," *IEEE Transactions on Information Theory*, vol. 52, no. 6, pp. 2508–2530, 2006.

[30] K. Li, H. Li, H. Wang et al., "PoV: An Efficient Voting-Based Consensus Algorithm for Consortium Blockchains," *Sec. Blockchain Technologies*, vol. 3, p. 11, 2020.

[31] C. Kuhlman and E. Rundensteiner, "Rank aggregation algorithms for fair consensus," *Proc. VLDB Endow*, vol. 13, no. 12, pp. 2706–2719, 2020.

[32] O. Kosheleva, V. Kreinovich, and G. Wei, "Ranking-based voting revisited: maximum entropy approach leads to Borda count (and its versions)," in *Behavioral Predictive Modeling in Economics*, S. Sriboonchitta, V. Kreinovich, and W. Yamaka, Eds., vol. 897, pp. 145–152, Springer International Publishing, New York, NY, USA, 2021.

[33] S. Mondal and R. Nasre, "Hansie: hybrid and consensus regression test prioritization," *Journal of Systems and Software*, vol. 172, Article ID 110850, 2021.

[34] A. Karpov, *Combinatorics of Election Scores*, Springer International Publishing, New York, NY, USA, 2021.

[35] A. Battah, Y. Iraqi, and E. Damiani, "Blockchain-based reputation systems: implementation challenges and mitigation," *Electronics*, vol. 10, no. 3, p. 289, 2021.

[36] F. Sadique, S. Cheung, I. Vakilinia, S. Badsha, and S. Sengupta, "Automated structured threat information expression (stix) document generation with privacy preservation," in *Proceedings of the 2018 9th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)*, pp. 847–853, New York, NY, USA, November 2018.

[37] Y. Ghazi, Z. Anwar, R. Mumtaz, S. Saleem, and A. Tahir, "A supervised machine learning based approach for automatically extracting high-level threat intelligence from unstructured sources," in *Proceedings of the 2018 International Conference on Frontiers of Information Technology (FIT)*, pp. 129–134, Islamabad, Pakistan, 2018.

[38] D. Chatziamanetoglou, "Code for Simulating Proof-of-Quality Consensus Algorithm for CTI Sharing," vol. 12, 2021, https://github.com/dimhatzi/PoQ.

[39] D. P. Oyinloye, J. S. Teh, N. Jamil, and M. Alawida, "Blockchain consensus: an overview of alternative protocols," *Symmetry*, vol. 13, no. 8, p. 1363, 2021.