CTI Blockchain-Based Sharing using Proof-of-Quality Consensus Algorithm

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

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

***Abstract*—The importance of Cyber Threat Intelligence (CTI) lies in its ability to be shared, consumed and actioned. For threat intelligence to be actionable, it must be shared with the right audience, at the right time and must fulfil quality standards. Without actionable and contextualised CTI, security teams will be making best guesses and assumptions instead of intelligence-based informed decisions. This paper proposes a decentralised, tamper-proof and reputation based solution for delivering vetted CTI information, using quality based CTI parameters in order to further evaluate the quality of CTI Feeds and the reputation of CTI Feed Sources.**

I. Introduction

In the constantly changing cyber environment, the digital landscape has evolved tremendously, bringing to the scene new generations of threats that are known to be complex, persistent, intrusive and resilient. The cyber security community is tackling various aspects of security and contributing to supplying accurate and usable information to those who make security decisions. Generating reliable, accurate intelligence is a dynamic, never-ending process commonly referred to as the intelligence cycle. The intelligence cycle typically comprises of 5 lifecycle stages, Planning & Direction, Collection, Processing, Analysis and Dissemination (sharing) [1].

Cyber Threat Analysis focuses on the analysis of available data, using tools and techniques to generate meaningful information about existing or emerging cyber threats, which helps organisations make timely, accurate, faster, more informed security decisions and change their behaviour from reactive to proactive to combat cyber attacks. The output of the Cyber Threat Analysis is the actionable Cyber Threat Intelligence (CTI) in which the CTI sharing mechanism is one of the most crucial factors for reliable and accurate CTI dissemination.

Based on the latest SANS Cyber Threat Intelligence Survey for 2021 [1], the vast majority of CTI are disseminated and/or collected via non automated mechanisms such as email, briefings, spreadsheets, presentations, reports etc. All the rest dissemination and/or collection methods are based on vendor-created, open-source or homegrown systems. Although there is no specific reference to the tools or techniques that the CTI dissemination/collection is taking place, there is a strong indication that none of the mentioned CTI Feed Sources is using blockchain technology for dissemination of cyber threat intelligence.

978-1-7281-5684-2/20/$31.00 ©2021 IEEE

For the following years, the usage of platforms that share robust, fast, reliable, verified, actionable and immutable CTI is more than required. Nowadays, there are many CTI Feed Sources that provide CTI via a variety of platforms and standards [2]. Furthermore, the volume of shared data is constantly growing and the data models and data types that are used, are scattered across multiple solutions and data standards, negatively impacting the quality of the threat intelligence data [3]. In addition, until now there has not been proposed any robust methodology of resolving the challenge of trust among the CTI community, in order to raise the confidence that the quality of CTI is above a set of standards.

This paper introduces a decentralised, blockchain-based and tamper-proof solution for delivering vetted CTI information, combining 5 main CTI principles: reliable sources, sufficient context, consistent data model, defined process and automation [4]. In this context, it also introduces a new consensus mechanism, namely Proof-of-Quality (PoQ), and a trust-based reputation mechanism for evaluating CTI Feeds and CTI Feed Sources.

The aim of this paper is two-fold. The first objective is to foster the quality-driven CTI sharing challenges [5], by evaluating the quality of CTI Feeds. This evaluation is based on their rating by a set of selected validators, the selection criteria of which are based on their reputation. A secondary goal is to evaluate the CTI Feed Sources themselves, based on the evaluation of their own published feeds. The reputation of the validators plays a significant role on the accomplishment of those goals, since it is one of the decisive elements among the performance and reputation metrics which will be presented.

The rest of this paper is structured as follows: Section II provides an overview of related works. The proposed model is described in Section III, while a discussion and the conclusions of our work are presented in Section IV. Finally, some future research directions are presented in Section V.

II. Background

In this section, two different research areas are considered. 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. Both research

areas are under consideration, since our proposal is covering CTI blockchain sharing based on a trust/reputation mechanism.

A. Blockchain-based CTI sharing

BloTISRT [6], addresses the need of using blockchain technology, proposing a theoretical rating model, based on agnostic data model and an abstract CTI Feed rating and consensus algorithm. BLOCIS [7], proposes a blockchain-based CTI sharing framework especially for Sybil-Resistance based on the Ethereum platform, referring to a generic STIX-based data model and an abstract mining related consensus algorithm. Mendez Mena et al. [8] research is based on the Ethereum platform, applying the Proof-of-Authority consensus algorithm, with an abstract data-model and a permissioned based network, from an ISP point of view. Cha et al. [9] propose a model which mitigates problems such as data collection efficiency and scalability, using an abstract data-model and blockchain technology to efficiently process large data, and providing security and privacy in a distributed way.

B. Blockchain-based trust establishment

Wu et al. [10] 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. [11] 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. [12] and Gao et al. [13] propose a new reputation management for P2P networks algorithm, 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. [14], [15] 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 behavior is encouraged and bad behavior is punished.

Lee et al. [16] proposed a blockchain-based reputation management for manufactures and customer interaction, including increased reliability by malicious evaluator identification. Oualhaj et al. [17] propose a blochckain-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 provide wrong trust values. Oliveira et al. [18] 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 monitor and sign a reputation score for every miner's action. Feng et al. [19] 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.

The aforementioned research efforts, address the blockchain based CTI sharing and trust/reputation challenges among the CTI sharing community, but not at the same time. Furthermore, the quality of the CTI Feeds is not addressed in a practical way, rather than an abstract general objective. Our proposal is intended to cover this gap, by introducing a more holistic approach for quality-based CTI sharing by utilising the blockchain technology, including a reputation mechanism fostering the trust among the CTI sharing community.

III. Proposed Blockchain Model

A. System Model Introduction

The proposed model comprises a set of mechanisms that select validators to evaluate the quality of CTI Feeds and store validation and CTI data on a blockchain-based, decentralised, permissionless ledger, for distributed dissemination. A reputation mechanism is further applied to assess the reputation of the CTI Feed Sources.

The 3 key roles of the proposed model's participants are:

(a) *CTI Feed Sources*, which offer and share CTI Feeds for evaluation,
(b) *Validators*, who are selected against reputation criteria based on their previous evaluation performance, in order to conduct the *CTI Feed evaluation*, and
(c) *Consumers*, who are using or querying the blockchain to access the evaluated and stored CTI.

The roles of Consumers and CTI Feed Sources could be potentially used interchangeably.

The proposed model, as shown in Fig. 1, receives CTI Feeds from CTI Sources as an input, evaluates them via an evaluation control mechanism and as an output, adds a block to the ledger with the evaluated CTI Feed, once consensus is reached via the proposed Proof-of-Quality consensus algorithm. The aim of the evaluation is to rate the CTI Feeds utilising quality-based criteria and parameters. All CTI Feeds are added to the chain, in order to maintain a historical quality-defined record, which will be further used for assessing the CTI Feed Source reputation.

Both consumers and CTI Feed Sources can participate in the evaluation process as validator candidates, forming the validator candidate pool (bidirectional information flows in Fig. 1). A Validator Selection Mechanism (VSM), screens the validator candidates, under certain criteria, in order to select the best candidates for the evaluation process. A feedback mechanism that utilises historical data already published on the blockchain, provides valuable information to the VSM. Details on the VSM mechanism, will be described later on.

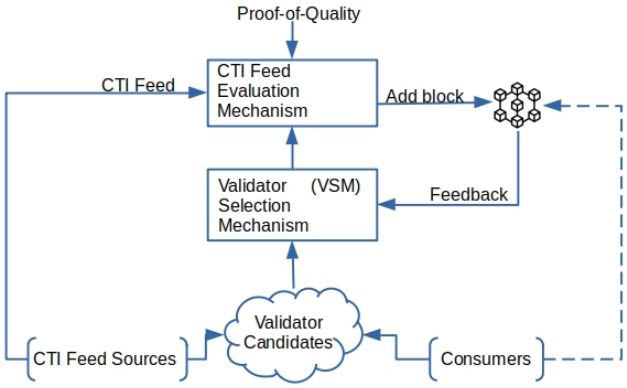

Fig. 1. Model's Block Diagram

B. Block layers

Each block of the ledger is logically divided in 3 layers and are added to the chain only when consensus is reached, via the proposed Algorithm 1.

1) The evaluated CTI Feeds are stored on the first layer.
2) The second logical layer stores the CTI Feed's mean evaluation rating result by the validators.
3) The third layer stores the validators' performance as an ordered list, based on their ratings and performance metrics during the CTI Feed evaluation process. The validators reputation is not stored on the chain, but is ad-hoc determined based on the performance values stored in this layer.

This way, the data stored on 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:

- calculating the reputation of CTI Feed Sources
- setting the foundation for a critical mass of reputable validators to carry on with future CTI Feed evaluations, preserving the fairness of the system.

Some of the aspects of the CTI Feeds ratings and therefore, of the validators' performance metrics are objectively measured and some of them not. 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. The same also applies on the anomaly/outlier detection and removal, decision which is left on each validator to be dealt with.

C. Validators Performance Metrics

The following validators performance metrics which are detailed below are the foundation of the *CTI Feed evaluation* mechanism:

- CTI Feed Rating
- Validator Performance

1) CTI Feed Rating: Each selected validator V_m, $m \in [1..i]$, rates each CTI Feed F_f, $f \in [1..k]$, against all chosen quality parameters P_n, $n \in [1..j]$. Such a set of parameters is provided in [5] and shown in Table I.

The rating per each CTI Feed F_f is represented as the following matrix R:

$$\underset{i \times j}{\mathrm{R}_{\mathrm{V_m P_n}}} = \begin{pmatrix} r_{v_1 p_1} & r_{v_1 p_2} & \cdots & r_{v_1 p_j} \\ r_{v_2 p_1} & r_{v_2 p_2} & \cdots & r_{v_2 p_j} \\ \vdots & \vdots & \ddots & \vdots \\ r_{v_i p_1} & r_{v_i p_2} & \cdots & r_{v_i p_j} \end{pmatrix} \quad (1)$$

TABLE I
CTI QUALITY PARAMETERS

Parameters	Description
Extensiveness	Evaluates how many optional parameters are filled
Maintenance	Determines how often messages are updated
False Positives	Determines how often messages of a source are invalidated
Verifiability	Expresses how often a source verifies the information they provide by linking their source.
Intelligence	Indicates how much added value a source offers in their messages by linking it to other objects
Interoperability	The data format a source provides their data in
Compliance	Determines compliance of sources to the standard they use
Similarity	Evaluates how similar entries of two sources are
Timeliness	Analyses which source provides information the quickest
Completeness	Indicates how much of the entire world a single source represents

2) Validator Performance: The validator performance metric is measured by the deviation of each rating compared to the mean rating per quality parameter per each evaluation by all validators, using statistical analysis metrics, for example Squared Deviation from the Mean (SDM). Anomaly/outlier detection is already inherited in the SDM calculation, facilitating the identification of misbehaving or overreacting validators.

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.

The Mean Rating Value MRV, of all validators V_m, $m \in [1..i]$, per quality parameter P_n, $n \in [1..j]$ is the following:

$$MRV_{P_n} = \frac{1}{i} \sum_{m=1}^{i} R_{V_m P_n}$$

The SDM of a validator V_m per quality parameter P_n is:

$$SDM_{V_m} = (MRV_{P_n} - R_{V_m P_n})^2$$

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

$$PERF_{V_m} = \frac{1}{\frac{1}{j} \sum_{n=1}^{j} (MRV_{P_n} - R_{V_m P_n})^2} \quad (2)$$

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

D. Proof-of-Quality Consensus Mechanism

Once the CTI Feed evaluation/rating by the validators is completed, the results in equation (1) are distributed to all validators via a gossip protocol [20]. All validators are able to have access to all ratings performed by any other validator.

The proposed 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 to be subject of the consensus algorithm. If i is the number of validators, then q should be much smaller than i, so $q \ll i$.

The expected outcome from each validator, is the production of an ordered list, from the higher performant validator to the lower one, per block, based on the objective performance metric in equation (2). If O_{V_m} is the produced ordered list from each validator, each element o_z represents the validator's V_m, $m \in [1..i]$ position in the list, along with its performance $PERF$, as follows:

$$O_{V_m} =< \overbrace{(o_1, PERF_1), (o_2, PERF_2), ..}^{q-first}, (o_i, PERF_i) > \quad (3)$$

According to the proposed algorithm (Algorithm 1), the validators who find themselves being in the $q - first$ best performant list, share their full ordered list to the rest of the validators community as consensus proposals. The consensus will be reached on the agreement of the $q - first$ best performant validators of the complete list, which will be finally stored in the ledger.

Given that more than one 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. The following matrix D_w depicts the available ordered list, subject for voting:

$$\underset{u\times 1}{\mathrm{D_w}} = \begin{pmatrix} O_1 \\ \vdots \\ O_u \end{pmatrix}$$

For this purpose, the Proof-of-Vote [21] consensus mechanism can be used.

The smaller the q is, the better the probability to reach agreement faster but at the same time the lower the fairness is and the probability of malicious validators to be selected is increased, and vise versa. Furthermore, if consensus is not reached, the algorithm reduces progressively the value of q in order to increase the chances of establishing an agreement.

E. Dynamic Reputation Mechanism and CTI Feed & Source Evaluation

The reputation mechanism is a key contributing element to 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.

Algorithm 1: Pseudocode for Proof-of-Quality Algorithm

```
Data: R_{V_m P_n} : Validator Rating Matrix
      q : q-first variable
Result: Reach Consensus
initialization;
/* each validator calculates PERF */
for m ∈ [1..i] do
    calculate PERF_{V_m};            // equation2
    < L_m >=PERF_{V_m};              // create list L
end
O_z = sorted list L_m;               // order:DESC, eq3
if self(PERF) > PERF(O_q) then
    broadcast(O_{V_m});              // to all validators
end
do
    /* each validator vote for O_{V_m} */
    for w ∈ [1..u] do
        for m ∈ [1..i] do
            vote on O_w
        end
    end
    if votes ≥ 50%;                  // on a specific O
     then
        Consensus = TRUE
    else
        q=q-1;
    end
while Consensus=TRUE;
```

1) Validator Reputation: The stored validator performance per block is shown on the following matrix A:

$$\underset{i\times p}{\mathrm{A_{V_m B_b}}} = \begin{pmatrix} PERF_{V_1B_1} & PERF_{V_1B_2} & \cdots & PERF_{V_1B_p} \\ PERF_{V_2B_1} & PERF_{V_2B_2} & \cdots & PERF_{V_2B_p} \\ \vdots & \vdots & \ddots & \vdots \\ PERF_{V_iB_1} & PERF_{V_iB_2} & \cdots & PERF_{V_iB_p} \end{pmatrix}$$

As a result of the consensus mechanism, the validators have agreed on the ordered list of the best performant ones per block. Based on the consensus, a consensus factor $c_z = \frac{1}{z}$, $z \in [1..u]$ can be applied, which represents the weight of the validators preference results, 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.

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

$$REP_{V_m} = \frac{c_z}{p} \sum_{b=1}^{p} A_{V_m B_b}, \forall A_{V_m B_b} > 0, \forall m \in [1..i] \quad (4)$$

2) Interim CTI Feed Evaluation: Validators ratings are included in the matrix of equation 1. The interim CTI Feed evaluation score is calculated from the average of the mean

values of the ratings that were received from all validators for all quality parameters. Anomaly or outlier detection removal should be included in this procedure, in order to avoid skewing the results. It is called interim because this metric will be the base for a more enriched calculation later, including the validators reputation metric (4).

So, the interim evaluation $iEVAL$ of a CTI Feed F_f is the following:

$$iEVAL_{F_f} = \frac{1}{j}\sum_{n=1}^{j}\frac{1}{i}\sum_{m=1}^{i}R_{V_m P_n} \tag{5}$$

3) CTI Feed Enriched Evaluation: Having calculated the reputation REP_{V_m} of each validator V_m, $m \in [1..i]$ in equation 4, we are in position to add this metric in the interim evaluation $iEVAL$ of a CTI Feed F_f which was calculated before (equation 5). This way, we emphasise the importance of the validators reputation to the final evaluation of the CTI Feeds.

In this case, we consider $r_m = REP_{V_m}$ as the reputation factor of each validator V_m, $m \in [1..i]$. The enriched evaluation $eEVAL$ of a CTI Feed F_f embedding the validator reputation is:

$$eEVAL_{F_f} = \frac{1}{j}\sum_{n=1}^{j}\frac{r_i}{i}\sum_{m=1}^{i}R_{V_m P_n}$$

4) CTI Feed Source Reputation: Apart from the evaluation of the CTI Feeds, a more extended approach can be applied, by calculating the reputation of the CTI Feed Sources. The reputation of the CTI Feed Source is linked to the archived evaluation of each own published CTI Feed, therefore the Feed Source reputation is expected to change with the inclusion of more CTI Feeds in the ledger.

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

$$\mathrm{C}_{\substack{\mathrm{F_f B_b}\\ k\times p}} = \begin{pmatrix} eEVAL_{F_1 B_1} & \cdots & eEVAL_{F_1 B_p} \\ eEVAL_{F_2 B_1} & \cdots & eEVAL_{F_2 B_p} \\ \vdots & \ddots & \vdots \\ eEVAL_{F_k B_1} & \cdots & eEVAL_{F_k B_p} \end{pmatrix}$$

Especially concerning the CTI Feed Source evaluation, a special weighted gravity factor g can be applied, via which the latest CTI Feed evaluation data will be taken into stronger consideration than the past ones. The nature of the constantly changing cyber environment, wants the informed decisions to be taken as accurately and timely as possible, and this can be achieved partially by giving more gravity on 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 factor $g_b = \frac{b}{p}$, $b \in [1..p]$, 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.

$$REP_{S_s} = \frac{1}{p}\sum_{b=1}^{p}\frac{g_p}{f}\sum_{f=1}^{k}C_{F_f B_b}, \forall C_{F_f B_b} > 0$$

F. VSM - Validator Selection Mechanism

During the VSM process, the selected validators are clustered using ML algorithms such as K-Means or DBSCAN (including anomaly detection and removal). Validators are mostly selected out of the most reputable cluster, which is calculated out of the combination of number of evaluations per validator and their performance, in particular based on their reputation via the equation (4). In addition, in order to increase the chance of other less reputable validators to increase their reputation, a weighted random choice mechanism is implemented in order to select validators from less reputable clusters, based on a adjustable ratio between most reputable cluster and less reputable ones.

G. System Flow Chart

The flow chart of the system is described as follows:

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

Step 2: CTI Feed Sources and Consumers are eligible to become validators. Once the candidates are nominated, they are screened by the Validator Selection Mechanism (VSM), against the following criteria:

- Own performance stored in the third layer of the ledger,
- IoC (for example malicious IPs) 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.

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

Step 3: Each selected validator, is rating the under evaluation CTI Feed against each one of a pre-defined set of CTI quality criteria [5], shown in Table I.

Step 4: This step deals with the performance calculation of every validator for each CTI Feed. Once the CTI Feed evaluation/rating by the validators is completed, the results are distributed to all validators via a gossip protocol in order to reach to a consensus on the n-first best performant validators. All validators are able to have access to all ratings performed by any other validator.

Step 5: Once the validator community reached to a consensus, the block is written in the ledger.

IV. Conclusions

In this paper, we propose a new reputation-based CTI Feed evaluation system, which deals with CTI dissemination using blockchain technology. The primary goal of the system is to perform evaluation of the CTI Feed data based on a definite set of quality based parameters by validators which are part of the CTI community. The validators are selected based on their reputation and other criteria, utilising a feedback mechanism from the ledger. The quality parameters are considered as equally important. If required, a weighted approach can be

applied to the stored data on an ad-hoc basis, in-line with the used methodology and context.

Furthermore, a new consensus algorithm is proposed and outlined. Once the evaluation results have been distributed to all validators, each of them is creating an ordered list, starting from the q most performant ones to the least 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 on the ordered list and the results are archived onto the ledger. Finally, the CTI Feed Sources reputations can be calculated, based on their own respective CTI Feeds which have already been evaluated and stored on the three-logical-layer ledger.

V. Future work

Only the high level description of the proposed system is covered in the present paper. The authors are working on a low level description providing details on how the new PoQ consensus mechanism works. In addition, we are planning to develop a proof of concept environment for a more analytical and experimental approach. Finally, our intention is to develop the necessary Smart contracts so that the stored CTI data could dynamically feed a process which will contribute to a Dynamic Risk Management concept, utilising the real time access of the data stored on the blockchain.

References

[1] R. Brown and R. M. Lee, "2021 SANS Cyber Threat Intelligence (CTI) Survey," SANS Institute, Tech. Rep., Jan 2021.

[2] 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, Mar. 2020. [Online]. Available: https://www.mdpi.com/2073-431X/9/1/18

[3] 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, Jan. 2018. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404817301839

[4] ENISA, "Threat Landscape 2020," ENISA, Tech. Rep., Oct 2020.

[5] T. Schaberreiter, V. Kupfersberger, K. Rantos, A. Spyros, A. Papanikolaou, C. Ilioudis, and G. Quirchmayr, "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*. Canterbury CA United Kingdom: ACM, Aug. 2019, pp. 1–10. [Online]. Available: https://dl.acm.org/doi/10.1145/3339252.3342112

[6] 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*. Guangzhou China: ACM, Dec. 2020, pp. 524–534. [Online]. Available: https://dl.acm.org/doi/10.1145/3444370.3444623

[7] S. Gong and C. Lee, "BLOCIS: Blockchain-Based Cyber Threat Intelligence Sharing Framework for Sybil-Resistance," *Electronics*, vol. 9, no. 3, p. 521, Mar. 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/3/521

[8] 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, Dec. 2020. [Online]. Available: https://www.mdpi.com/2624-831X/2/1/1

[9] 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, p. 6401, Aug. 2020. [Online]. Available: https://www.mdpi.com/2071-1050/12/16/6401

[10] Y. Wu, Y. Qiao, Y. Ye, and B. Lee, "Towards Improved Trust in Threat Intelligence Sharing using Blockchain and Trusted Computing," in *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. Granada, Spain: IEEE, Oct. 2019, pp. 474–481. [Online]. Available: https://ieeexplore.ieee.org/document/8939192/

[11] 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, p. 100058, Sep. 2019. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S2542660519301234

[12] 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*. Budapest, Hungary: ACM Press, 2003, p. 640. [Online]. Available: http://portal.acm.org/citation.cfm?doid=775152.775242

[13] 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, Dec. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8968727/

[14] 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, Jan. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X19310581

[15] 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, p. 101871, Aug. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167404820301449

[16] 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, Mar. 2020. [Online]. Available: http://link.springer.com/10.1007/s12083-019-00730-6

[17] O. A. Oualhaj, A. Mohamed, M. Guizani, and A. Erbad, "Blockchain Based Decentralized Trust Management framework," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*. Limassol, Cyprus: IEEE, Jun. 2020, pp. 2210–2215. [Online]. Available: https://ieeexplore.ieee.org/document/9148247/

[18] 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, p. 107367, Oct. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1389128620300360

[19] 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, Apr. 2020. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S0167739X19313044

[20] 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.

[21] K. Li, H. Li, H. Wang, H. yao An, P. Lu, P. Yi, and F. Zhu, "Pov: An efficient voting-based consensus algorithm for consortium blockchains," in *Frontiers in Genetics*, 2020.