




## Transforming Cybersecurity: Leveraging Blockchain for Enhanced Threat Intelligence Sharing



Ahmed El-Kosairy<sup>\*</sup>, Heba Aslan<sup></sup>, Nashwa Abdelbaki<sup></sup>

Center for Informatics Science, School of Information Technology and Computer Science, Nile University, Giza 12588, Egypt

Corresponding Author Email: [ah.elkosairy@nu.edu.eg](mailto:ah.elkosairy@nu.edu.eg)

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijss.140412>

### ABSTRACT

**Received:** 10 June 2024

**Revised:** 27 July 2024

**Accepted:** 7 August 2024

**Available online:** 30 August 2024

#### Keywords:

*Blockchain, Cyber Threat Intelligence, threat sharing, Proof of Work, Proof of Stake, consensus mechanism, 51% attack, double spending attack*

The number of cyberattacks has increased significantly, necessitating the establishment of robust safeguards. To protect networks from intrusion, Cybersecurity Threat Intelligence (CTI) has been employed. CTI must effectively counter these attacks. Sharing CTI is essential for understanding threats, safeguarding assets, and blocking attack vectors. However, conventional CTI faces challenges related to privacy concerns, negative publicity, and issues with quality, which hinder the sharing of threats within the CTI community. This paper introduces a new framework that leverages Blockchain technology to enhance CTI frameworks. We developed a consensus algorithm combining Proof of Work (PoW) and Proof of Stake (PoS) methodologies to maintain CTI network security. This hybrid system requires miners to stake tokens in proportion to their hashing power, aligning incentives with network integrity and defending against double spending attacks. Our framework employs Blockchain features such as privacy, and digital signatures to create a secure and private environment for CTI sharing. We evaluated the effective hash power distribution and discussed the advantages, limitations, and potential improvements for the CTIB mode. The model was tested against 51% attacks, proving its effectiveness statistically. Implementing this Blockchain & CTI algorithm will pave the way for a more resilient and equitable cybersecurity defense mechanism.

## 1. INTRODUCTION

Cybercrime is on the rise. Therefore, organizations are taking precautions to protect their data and prevent it from being stolen or compromised. CTI feed sharing is an important tactic. Following the compromise by a zero-day attack, customers initiate the Incident Response (IR) process. Sharing the attack anatomy and Indicator of Compromise (IoC) with the community is the next step after applying risk mitigation and containment [1]. Attacker-made artifacts can be found in CTI feeds and may include new directories, open ports, or altered registry entries. It is possible to include signatures in the CTI along with file hashes, domain names, and IP addresses. Modern and traditional CTIs were created to establish a standard for exchanging threat intelligence feeds among the CTI community and platforms [2]. These CTIs make use of standards like Structured Threat Information Exchange (STIX), Trusted Automated eXchange of Intelligence Information (TAXII), and Cyber Observable eXpression (CybOX). Current CTI solutions do not permit members of society or communities to publicly share their CTI information or any details about the attacks to protect the privacy of community members. It is important to suggest a solution where people in the community can share data without disclosing their identities.

This is achieved by incorporating Blockchain technology that not only allows for decentralized administration and

immutability but also provides users with the option of remaining anonymous.

This paper aims to introduce a novel system for sharing CTI technology using Blockchain networks as a framework called Cyber Threat Intelligence based on Blockchain (CTIB). We created a framework model to use CTI on the Blockchain network to enhance the current CTI approach. The potential use of Blockchain technology improves CTI frameworks by addressing privacy and negative publicity concerns that prevent contributors from sharing their information in traditional CTI approaches. The use of Blockchain maintains the privacy of the threats' detectors as the user's identity is concealed by using public key encryption. Therefore, the end user can safely share any details related to the attack anatomy and IoCs of any zero-day attack without revealing their identity and gain rewards from the community for this contribution. In addition, our solution includes hybrid consensus algorithm that uses PoW and PoS which significantly enhances the effectiveness of CTI technology while eliminating any Blockchain related difficulties.

Our framework has lessened the power consumption used in the consensus process as it is mainly based on the PoS algorithm. The use of PoW algorithm is only to confirm the decision of the PoS layer. CTIB ensures integrity, privacy, and confidentiality while maintaining quality assurance.

We have devised mathematical equations governing the allocation of hashing influence based on stake contributions to

ensure that the platform is fair and secure. Our system ensures that the influence of miners is proportional to their stake, preventing the centralization of power. We have tested the model against 51% attacks and have demonstrated its effectiveness through statistical analysis. The introduction of this algorithm into Blockchain based CTI will create a more resilient and equitable cybersecurity defense mechanism. Moreover, CTIB has a contingency plan in place to ensure high availability if the primary layer of verification, PoS, is unavailable. In such cases, the system will shift to the secondary layer, PoW, until validators on the primary layer become available. The main paper contributions are:

- Design a new framework to be used for sharing Cyber Threat Intelligence feeds which is based on Blockchain technology and double consensus mechanisms.
- The use of double consensus mechanisms to provide a framework with low power consumption.
- The use of double consensus mechanisms to resist 51% and double spending attacks.
- The use of Blockchain provides integrity, privacy, confidentiality, quality assurance, sharing data anonymously, and high availability.

The paper is structured as follows: Section 2 provides background information on conventional CTI and Blockchain technology and the obstacles to the current CTI approach. Section 3 presents a literature review of existing CTI-based Blockchain models, the challenges these models face, solutions that utilize hybrid consensus algorithms, and a brief introduction to the combination of Blockchain technology and CTI models. In Section 4, we present our proposed CTIB framework. In Section 5, we analyze our results and demonstrate the outcomes. This is followed by a discussion of CTIB’s advantages, limitations, and potential challenges that could be addressed using CTIB and provide directions for model improvement. We conclude our work in Section 6.

## 2. BACKGROUND

Threat intelligence feeds contain malicious techniques, IoCs, Tactics, Techniques, and Procedures (TTP), and any other information that could help the community detect and respond to the attack. This method allows users and entities to participate. Real-time transmission of CTI is essential for detecting zero-day attacks by the community. Typically, the IR team of that entity constructs this report and explains the attack anatomy. Currently, the user or CTI sharing system must set the objectives and aims behind this CTI report before it can be shared. After constructing this report, they must change the format into a CTI standard structured language before sending it to the community through the CTI system. This Section illustrates the CTI formats and standardization. Then, we give the challenges and limitations in the current CTI approaches. Finally, a brief overview of Blockchain is depicted.

### 2.1 CTI formats and standardization

Alternative approaches are taken by vendors, who first gather IoCs and metadata before constructing and generating CTI feeds, which are then published to subscribers. To ensure the community is prepared to stop these waves of zero-day attacks, these standards distribute CTI feeds that explain the attack anatomy. These norms specify the formats used by

automated security tools for storing and retrieving data [3].

The structured language for the CTI was developed and created by several organizations and non-profit entities, including the Internet Engineering Task Force (IETF), which is responsible for several related standards. In 2007, the Incident Object Description Format (IODEF) standard was created by the IETF Managed Incident Lightweight Exchange Working Group (MILE WG) [4]. The vendors, customers, community, and IR groups need to be able to communicate in the same language [5].

When responding to attack vectors and zero-day exploits, IR teams need a thorough understanding of the attack’s anatomy and cause before they can devise an effective mitigation plan and strategy. The end user can now assist the community in preventing this attack by disseminating the CTI data. Table 1 outlines the various categories used to categorize CTI’s various formats. Formats such as STIX make descriptions of threats and their effects more widely readable and usable. There is a primary focus on threat reporting formats stated in Table 1 [6].

**Table 1.** STIX support for various format structures [6]

	Format Structures					
	Vulnerability Format					
STI	CVE	CAPE C	CWSS	CVSS	CPE	CWE
X	✓	✓	X	✓	✓	✓
			IR & Scan Format			
	Open IOC	Yara Rule	IPS Rule	Cybox	MAEC	MMD EF
	✓	✓	✓	✓	✓	✓

For the vulnerability format, we selected the most known formats such as Common Vulnerabilities and Exposures (CVE), Common Attack Pattern Enumeration and Classification (CAPEC), Common Weakness Scoring System (CWSS), Continuous Professional Education (CPE), and Common Weakness Enumeration (CWE).

For the IR and Scan Format, we selected the most known formats such as Open IOC, Yara rule, Intrusion Prevention System (IPS) rule, Cyber Observable Expression (Cybox), Malware Attribute Enumeration and Characterization (MAEC), and Malware Metadata Exchange Format (MMDEF).

### 2.2 Issues with the traditional CTI approach

It is essential to understand the traditional CTI issues to determine how they could be resolved to improve the CTI to become more effective.

The first issue is that the current CTI system needs to offer quality measures to prevent disqualifying CTI reports or the quality of the CTI’s data. An annual subscription fee to a commercial threat intelligence feed provider might be expensive for any entity that wants reliable and up to date information. Without an auditing process for these vendors or a way for the public to review the quality of the CTI data, this creates a single point of failure and distrust.

Secondly, there is the problem of confidentiality and the law to consider. Unfortunately, confidentiality cannot be guaranteed using the current CTI technology especially with public CTI feeds [7]. Users can receive CTI reports but cannot generate reports that could compromise their anonymity. Depending on the severity of the attack and the organization’s

IR capability, an IR will be implemented within minutes or hours to address the problem and contain the risk.

Mean Time to Respond (MTTR) is a crucial metric in IR and cybersecurity that measures the speed with which an organization can implement a complete incident response plan, including five-stage recovery procedures [8] as shown in Figure 1. Details about the incident or zero-day attacks are included in the final report so that this new wave of attacks can be revealed to the public. Information such as the organization’s name, the extent of the attack, the identities of any compromised accounts, and the extent of the attack’s impact are included in this report and are deemed confidential. Reviewing this report before releasing it will take time and effort to ensure that it does not expose the company to legal risks. Regarding the current CTI method.

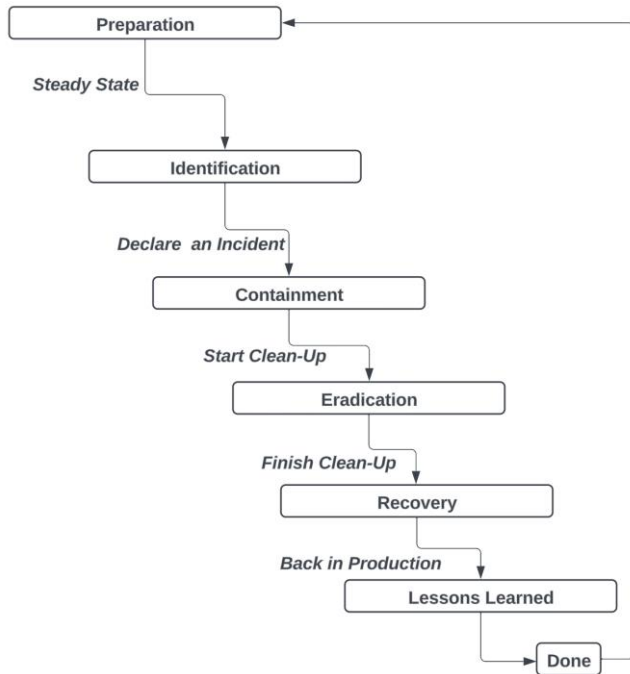


Figure 1. Incident response process

The third concern is credibility and non-repudiation. To ensure that any message is genuine, and that the sender cannot deny their consent, it is crucial to have third-party verification. This way ensures the message reliability and the sender’s commitment to the message. For example, an adversary can easily circumvent any organization’s security measures and compromise the CTI server to inject spoofed CTI reports [7]. Another concern is that businesses do not publish information about internal attacks and data breaches to avoid negative attention. This can be problematic, as it may prevent affected individuals from taking necessary steps to protect themselves. However, to avoid unwanted publicity, some companies choose to keep things under wraps.

The downside to this approach is that it can come across as dishonest and erode trust in the organization. It is a delicate balance to strike, but transparency and honesty are generally the best policies when it comes to cybersecurity incidents [9]. The fifth and last concern is the risk of a Single Point of Failure (SPoF). Hackers can exploit zero-day vulnerabilities to infiltrate the CTI back-end server and introduce harmful scripts and reports that can severely damage the company.

### 2.3 Blockchain architecture

CTIB is based on both Blockchain and CTI, which provides an advantage of the Blockchain to fix the current issues of the traditional CTI. The information in the Blockchain is added to a continuously growing list. The list comprises numerous data blocks recorded, linked, and encrypted using various methods. In the early 1990s, physicist Scott Stornetta and scientist Haber Stuart used cryptographic techniques in a Blockchain to protect digital documents from data tampering. Thus, the concept of a Blockchain was founded. Bitcoin’s whitepaper, written under the alias Satoshi Nakamoto, was released to the public in 2008 [10]. The Blockchain network’s significance lies in providing incentives, such as financial benefits to encourage people to participate.

The advantages of the Blockchain can be summed up as follows [11]:

1. It works without a central authority and cannot be controlled because its system is expanded and decentralized.
2. No one can change or delete the records on Blockchain.
3. Digital signatures ensure that involved participants can trust each other without the help of a third party.
4. Each node holds a copy of the information, and all can access and utilize the data transactions.
5. Every node can see the status of their transaction, and the details of all transactions are shown in Blockchain, which provides transparency.

Application and Presentation Layer			
Smart Contracts	Chain Code	DApps	UI
Consensus Layer			
PoW	PBFT	DPoS	PoS
Network Layer			
Peer to Peer (P2P)			
Data Layer			
Digital Signature	Hash	Merkle tree	Transaction
Hardware/Infrastructure Layer			
Virtual Machine	Containers	Services	Messaging

Figure 2. Blockchain architecture [11]

Figure 2 shows that the Blockchain architecture is divided into five layers [11]: Application and Presentation Layer, Consensus Layer, Network Layer, Data Layer, and Hardware/Infrastructure Layer. The Infrastructure Layer includes all the required hardware to run Blockchain, such as nodes, storage, and network infrastructure. Data Layer includes digital signatures, hashes, Merkle trees, and transactions. The Peer-to-Peer (P2P) protocol and its implementation are found at the Network Layer.

The Consensus Layer describes the type of proof used in this network. The Application and Presentation Layer displays the innovative contracts method, User Interface, Chain Code, and Decentralized Applications (DApps).

Table 2. Smart contract diagram [12]

Block n-1	Timestamp	Root Hash of the Current Block n
		Additional Information
		Smart Contract Record 1
		Smart Contract Record 2
		Smart Contract Record ...
		Smart Contract Record M

In Table 2, each block contains a timestamp, the current block’s hash value, the previous block’s hash value, and other descriptive information [12]. Smart contracts are only possible with the help of the “Event Trigger” mechanism [13]. All nodes have regular intelligent contract traffic between them. To ensure accuracy, each node receives the contract that needs to be checked. As with all Blockchain transactions, the node will verify the contract’s digital signature for security purposes. Once verified, the contract will be executed according to the terms of the agreement. The smart contract system of the Blockchain automates the entire contract processing procedure. Objects, including assets, markets, systems, and behaviors, are given digital characteristics to realize intelligent contracts. By automatically developing and executing digital objects, the Blockchain network can alter the state and values of digital objects. Smart contracts actively and passively receive, keep, manage, and share data.

### 3. LITERATURE REVIEW

CTI is the critical method for sharing threat information. As mentioned in the previous Section, there are numerous problems and constraints with the current CTI, such as lack of quality control, privacy, integrity, non-repudiation. Additionally, Blockchain technology demonstrates a working example of a distributed database that does not rely on a centralized authority. As mentioned in subsection 2.2, the critical advantage of Blockchain is the concealment of users’ identities and locations. Since the Blockchain is distributed, records can be replicated across all nodes. In addition, each node has a copy of every previous record. Therefore, updating them is time-consuming. Given these conditions, Blockchain is the best technology to employ and integrate with the CTI to address and resolve existing issues. The digital signature guarantees that the details in the threat intelligence feeds have not been altered and cannot be denied. The Blockchain’s rewards system ensures its continued quality by incentivizing its parties (nodes) to participate and examine the reports of their peers. This section defines the related works for how Blockchain technology could be used in CTI to enhance the most critical problems in the current CTI technology. It is crucial to explore the potential of using Blockchain technology in CTI to improve existing procedures and address problems commonly encountered in traditional CTI systems. Since Blockchain provides privacy, any entity can share threat intelligence reports without revealing its identity. As discussed in the Blockchain Section, Blockchain employs cryptography

algorithms such as digital signatures to conceal the identity while providing integrity, credibility, and non-repudiation. Using Blockchain’s consensus technique in the CTI improves the quality of the content and reduces the number of deficient CTI reports. Furthermore, it increases the network’s trust for transaction CTI reports. Blockchain provides real-time, shared, and fully transparent information stored on an immutable ledger accessible only to permission network members. Furthermore, there is no need to establish or request a third-party review. As centralized databases require more security controls and a more secure architecture to protect against hacking techniques, decentralized databases are preferable. To prevent negative publicity and ensure that no one can spread rumors or fake news, Blockchain uses consensus algorithms, validators, or miners to review and verify content. The incentives motivate miners and validators to check more blocks and earn more rewards. No one can change the content since hash algorithms and digital signatures provide integrity and protection. Table 3 summarizes how Blockchain has been used to address the current CTI challenges and issues [14].

Table 4 presents the type of proof covered to share “threat” feeds using Blockchain technology. Some of these papers are based on CTI feeds, while others are based on sharing threats’ feeds without a standard format. As exhibited in Table 4, most of the papers cited the use of Blockchain without explaining the methods, such as the type of proofs, the reward system, or the threat intelligence sharing format. In a specific case, the significance of Blockchain technology in resolving CTI problems was highlighted in the study [15]. Nonetheless, the type of Blockchain consensus used for proof or reward was not specified. Therefore, we denoted the value as “-” since no specific value was mentioned. Otherwise, anything that corresponds to our factors is represented as an “\*” as in the study [15], where the authors recognized the Structured Threat Intelligence Sharing Language as shown in Table 4. Also, Tanriverdi and Tekerek [16] focused on Blockchain literature but failed to specify the type of consensus or rewards being discussed. On the other hand, Gong and Lee [17] used Blockchain technology to build CTI feed systems and smart contracts for threat intelligence sharing and rating.

Based on the information in Table 4, several factors must be thoroughly examined to suggest a way to combine Blockchain with CTI feeds. Some of these factors include determining the appropriate proof type for CTI that balances performance and resource usage, determining the compensation for miners and validators, and selecting a compatible sharing format standard that works well with both CTI and Blockchain.

**Table 3.** Blockchain foundations used to address current CTI issues [14]

		CTI Issues and Obstacles			
		Quality Measures	Confidentiality & the Law to Consider	Credibility & non-repudiation	Undesirable Publicity
<b>Blockchain Pillars</b>	Hashing Technique	✓	X	X	✓
	Digital Signature	X	X	✓	✓
	Encryption	X	✓	✓	X
	Consensus	✓	X	✓	✓
	Validators	✓	X	✓	✓
	Rewards	✓	X	✓	✓

**Table 4.** A comparison of the papers based on the type of proof, the threat intelligence sharing format standards, the type of rewards, and whether they were designed for the CTI system [14]

Papers	Blockchain's Type of Proof	The Threat Intelligence Sharing Format Standards			Rewards Mentioned	Papers Were Designed for the CTI System	Papers Were Designed for an Alert Sharing System, But Not CTI
		STIX	TAXII	CyBOX			
[15]	-	*	-	-	-	*	-
[18]	*	-	-	-	-	-	*
[19]	*	-	-	-	*	-	*
[16, 20-24]	-	-	-	-	-	-	*
[25]	-	*	*	*	*	*	-
[26]	-	*	*	-	-	*	-
[27]	*	-	-	-	*	-	*
[17]	*	*	*	-	*	*	-
[28]	*	-	-	-	*	*	-
[29]	*	-	-	-	-	-	*
[30]	*	*	-	-	-	*	-
[31]	*	-	-	-	-	*	-
[32]	-	*	*	-	-	*	-
[33]	-	*	*	-	*	*	-
[34]	*	-	-	-	-	-	*
[35]	*	*	*	-	*	*	-
[36]	*	-	-	-	-	*	-
[37]	*	*	*	-	*	*	-
[38]	*	*	-	-	-	*	-
[39]	*	*	-	-	-	*	-

### 3.1 Type of Blockchain consensus proof

Different proof scenarios, including the most well-known consensus algorithms, PoW, PoS, and PoA, could be used in Blockchain [40]. When processing network nodes, particularly when mining new blocks, the PoW consensus uses techniques that result in higher power consumption. The goal is to defend Blockchain from attacks that rely on computing power, such as DoS attacks. Nodes with more processing power have a greater chance of participating in mining and other similar Blockchain network operations to earn rewards [41].

The validator node for the following blocks is chosen using methods used by the PoS consensus algorithm. Since the reward for the network process is not limited to the most influential players, the objective is to distribute network tasks among the network nodes. Additionally, it is a universal right. PoS, thus, defends the network from 51% attacks [42]. Validators in PoA-based networks certify blocks and transactions that accounts have endorsed. Using run techniques, validators can group transactions into blocks in a routinely automated process without checking their computers. However, it necessitates keeping the authority node. Nodes can become validators and are urged to maintain their position with PoA. Since this is stronger than PoS, incentives may change. The PoA partially shields the network from DoS assaults and 51% other assaults [43]. The critical contrasts between discussed consensus algorithms are shown in Figure 3 [27, 44].

### 3.2 The expected challenges following CTI and Blockchain integration

When integrating CTI and Blockchain, there are some challenges and concerns that need to be taken into consideration. One of the main concerns is forking and latency [45], which could potentially cause delays and disruptions in the system. Additionally, resource consumption is another

significant concern because multiple hash computations and miners are needed. The Sybil attack could also impact the reliability of CTI by interfering with the Blockchain's reward structure [46].

Type	Security Case	Pros	Cons
PoS	It protects from 51% attacks.	It conserves energy and is environmentally friendly.	The network is dominated by prominent stakeholders, which is a significant disadvantage.
PoA	It protects from DoS attacks.	PoA reduces the required time to verify transactions and serves as a platform for developing.	It is not suitable for most non-enterprise applications because it requires users to trust validators and authorizers, while public Blockchain aims to be trustless.
PoW	Open to 51% attacks, selfish mining, and eclipse attacks.	It achieves consensus quickly, eliminates the possibility of spamming, and has been thoroughly tested over time.	Consumption of energy and resources

**Figure 3.** Comparison of proof types based on consensus [27, 44]

Furthermore, the 51% attack and double spending are potential threats that must be addressed when integrating CTI and Blockchain. It was essential to carefully consider these challenges and concerns when developing and designing the proposed framework.

### 3.3 Hybrid consensus technique in other fields

To our knowledge, consensus techniques have been applied in several applications and technologies other than CTI. However, it is rare for CTI to use more than one consensus technique, unlike our approach, CTIB. Our study revealed a lack of detailed explanation of using this dual consensus Blockchain technology in conjunction with traditional CTI. This Section explains how the hybrid PoS and PoW could be used in a real-life example, such as Decred. Decred is a governance cryptocurrency that uses both PoS and PoW consensus as a hybrid model [47]. A summary of previous studies and their hybrid consensus applications is shown in Table 5.

The application for other studies diversifies between countermeasures to avoid Blockchain attacks such as 51% and double spending attacks. Some contributors mentioned the

scope and fields like cryptocurrency, IoT, e-voting, and organic food supply chains. For instance, the presented research proposes a solution to the PoW consensus algorithm by combining both PoS and PoW on the same network [48]. This approach offers an unbiased mining reward to validators and miners. The experimental results show that this algorithm effectively reduces the number of malicious nodes attempting to engage in double spending. Additionally, the authors have developed a hybrid cryptocurrency that combines PoS and PoW to solve the 51% attack problem.

This system is designed to achieve network dominance, making it impossible for malicious nodes to engage in such attacks. Wu et al. [49] tried to learn more about how Blockchain’s consensus works so that the technology could work better. They used PoS and PBFT algorithms as a hybrid consensus that combines the benefits of both algorithms. The authors improved the idea through throughput, latency, and the ability to grow. Liu et al. [50] explained how to use both PoW and PoS to build a hybrid consensus protocol that does not split. They then combined their fork-free hybrid consensus with PoS to make a flexible version of PoA where the parameters between PoW and PoS can be changed.

**Table 5.** A summary of previous studies and their hybrid consensus applications

Papers	Year	Application	Types of Hybrid Consensus that Have Been Used			
			PoW	PoS	PoA	PBFT or FBA
[47]	2021	Countermeasure	✓	✓	-	-
[49]	2020	Countermeasure	-	✓	-	✓
[50-52]	2019	Countermeasure	✓	✓	-	-
[53]	2020	IoT (Edge Environments)	✓	✓	-	-
[54]	2020	Countermeasure	✓	✓	-	-
[55]	2021	Cryptocurrency	✓	✓	-	-
[56]	2018	Cryptocurrency	✓	✓	-	-
[57, 58]	2019	Cryptocurrency	✓	✓	-	-
[59]	2017	Cryptocurrency	✓	✓	-	-
[60]	2021	E-voting	✓	✓	-	-
[61]	2021	Organic Food Supply Chain	-	-	✓	✓

## 4. THE PROPOSED CYBER THREAT INTELLIGENCE BLOCKCHAIN (CTIB) FRAMEWORK

This section discusses our proposed design (CTIB) and how it differs from traditional CTI with Blockchain integration. Section 4.1 explains the design and workflow. Section 4.2 explains the mathematical formulation and methodology of a hybrid PoW and PoS consensus algorithm.

### 4.1 CTIB’s design and workflow

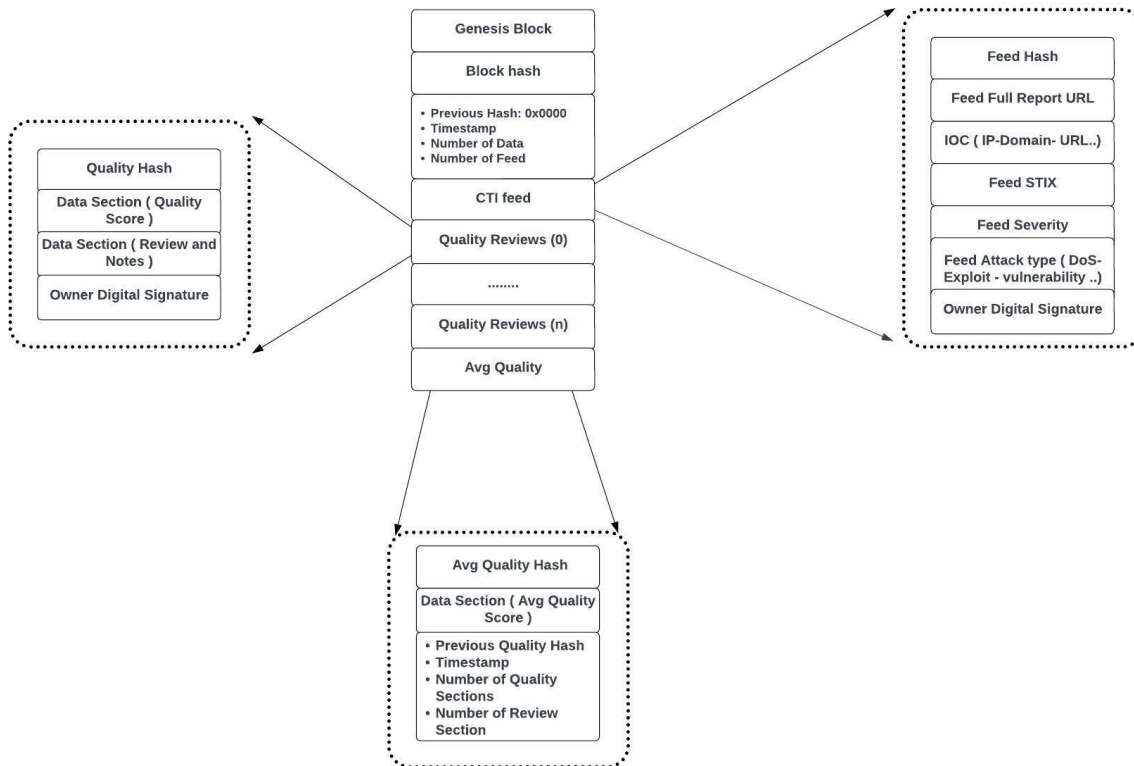
While traditional CTI with Blockchain integration has resolved some of the privacy and confidentiality issues associated with CTI, it has also presented new challenges, such as 51% attacks and double spending, as noted in Section 3.2. In response to the faced difficulties by the integration of CTI and Blockchain technology, a new framework has been developed, which is our CTIB. CTIB framework employs two consensus layers based on papers from other fields and technologies.

In our model, we combined PoS and PoW. PoS supports validators with limiting network consumption and speed. PoW benefits miners by allowing them to review the work of the

validator for each new CTI feed. This method ensures quality. Our system uses PoS and PoW to ensure fairness and security. With PoS, the chosen validator cannot manipulate the outcome or make false claims by depositing coins in their node. PoW allows regular users to verify and confirm the validator’s results. Also, it allows them to be promoted to validator status based on their rank, which depends on their effort and the total number of reviews. Those who mine or validate transactions are rewarded with cryptocurrency or rank, which motivates them to continue their work. The ranking system is essential because it determines the value of each node, and nodes with higher ranks are preferred over those with lower ranks. When a miner’s node achieves a specific rank/score, it may be encouraged to participate more and become a validator.

We display the contents of our proposed genesis block as part of our approach. In the Genesis block, there are two main sections: one is the block hash, and the second is the (header section) which contains the following:

- The previous hash entry with no value because no previous hash exists
- The timestamp
- The total number of data
- The total number of feeds



**Figure 4.** The design of Blockchain blocks for CTIB

The next data section is (CTI feed) as shown in Figure 4, the original feed is stored to be read and reviewed by the validator. The (CTI feed) contains the following entries:

- The feed’s hash value to make sure that any change or modification does not affect the original.
- The full report URL for the feed
- The IoCs include IP domains, URLs, and so on
- The STIX feed-in format must be readable and usable by another CTI system
- Feed severity to identify the severity of the content
- Feed attack type to explain the original feed’s attack vector and category
- Owner’s digital signature

After the (CTI feed) section, there is the (Quality Reviews) sections the validator will add their quality score, feedback, and comments to the original feed. The total number of the data section quality reviews sections will be proportional to the total number of validators and miners. The quality review section contains the following entries:

- The hash value of the feedback and comments to detect any changes or modifications
- The scoring and review of the CTI feed’s quality
- The review and notes section contains the validator’s comments and feedback. In addition, it explains why this score was assigned to the original feed.
- The digital signature of the validator

Finally, the average quality section contains the following:

- The average quality score hash to avoid any modifications or external corruption trial on this block.
- The average score of all assigned validators and that is why there is a section related to the average quality score section.
- The previous quality hashes

- Timestamp
- The number of quality and review sections as mentioned in Figure 4.

Our new framework combines PoW and PoS consensus techniques to mitigate any flaws in each technique. When a Blockchain block is created, the PoS validator votes on whether to approve or discard it. Validators are chosen based on their token deposit, ensuring they perform their duties correctly. To determine the validator rank, the number of participants is crucial, and only an odd number of validators will be chosen. These validators will be sorted based on their honesty rank score. Selecting an odd number of validators ensures that the majority can quickly emerge, and that there are no tie values or equality in the result.

In our approach, a minimum of five validators must be selected. The number of tokens among these nodes has a more significant vote to determine the block’s validity. If three of the five selected votes are positive, the block is confirmed and added to the Blockchain network. Validators must include their comments and review notes in the CTI report. The second layer, including regular nodes as miners, reviews the entire Blockchain using the PoW consensus algorithm. This two-layer system aims to protect against 51% and double spending attacks by implementing PoS voting and PoW mining for verification. In the PoS consensus layer, five validators at random evaluate and validate the genesis block created by the researcher who produces the CTI report feed, as illustrated in Figure 5. Meanwhile, Figure 6 outlines our framework’s workflow following the layers’ identification and design. The first validator will be chosen based on honesty rank and deposit amount. The first validator will generate the first block. After the first validator’s review and validation, the CTI research creator will receive his/her portion of the reward as a cryptocurrency; the same is done for each validator based on their honesty rank score.

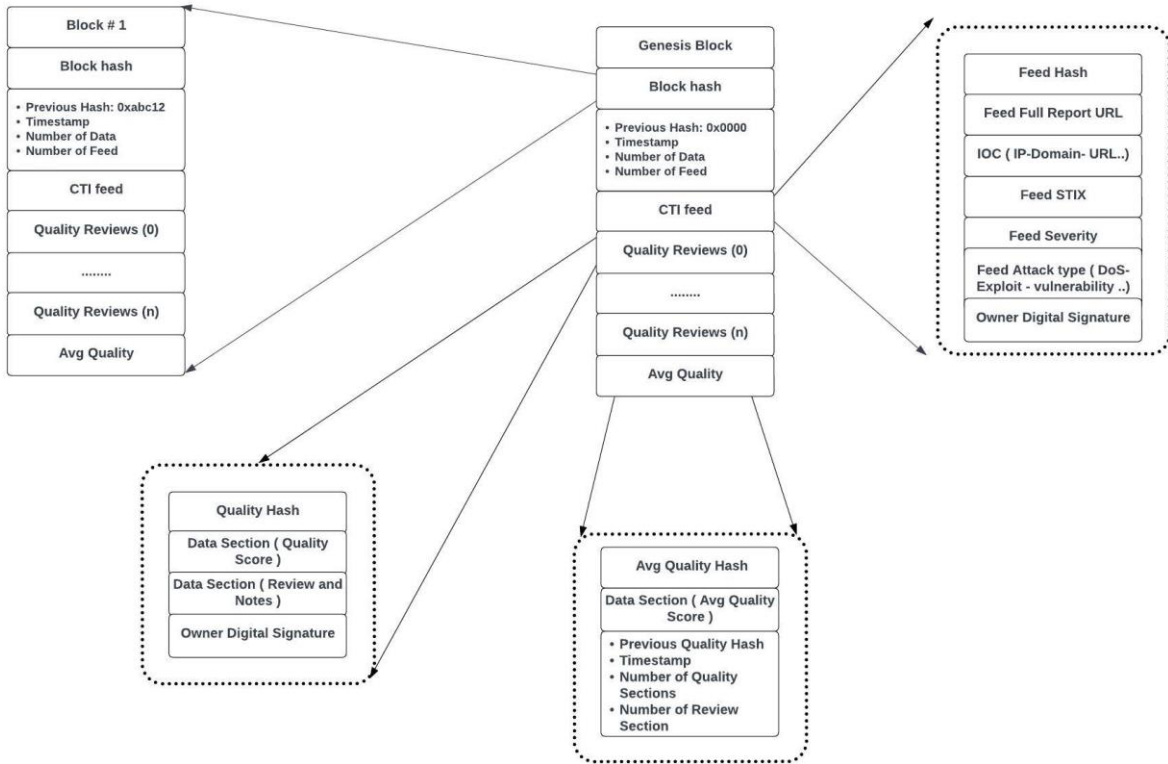


Figure 5. The generated genesis block by the researcher or contributor

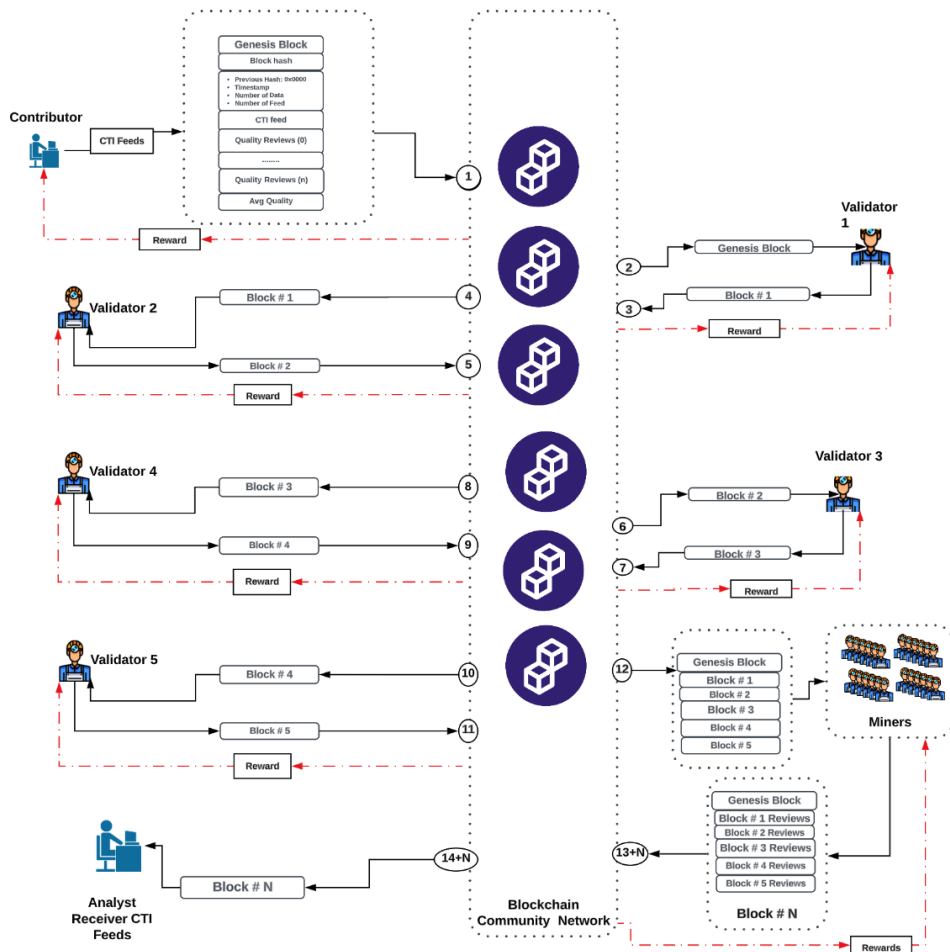


Figure 6. CTIB high level diagram and workflow



Figure 6 shows the delivery of the block to the second layer for review and verification by the regular nodes (miners) following the validators' evaluation and application of the PoS rewards and vault technique. When miners complete their revision in PoW, cryptocurrency is sent to them, and their honesty rank is increased if the other miners confirm their results. The second layer, which utilizes PoW, aims to involve regular nodes (miners) in the review process and motivate them to scrutinize the validator's results.

Our framework will leverage PoW nodes to verify and endorse the validator's decision. Over time, a PoW node (miner) may advance to become a validator in PoS. Cryptocurrencies will be used, and participation rank scores will be raised to incentivize participation. By combining both approaches, we can achieve quality assurance by harnessing their benefits. An essential advantage of dual consensus layers is preventing corruption in the PoS layer, as the PoW layer nodes can detect this. Figure 6 depicts the workflow of our model which begins by the researcher.

In addition, it demonstrates how the first validator reviewed the genesis block. This layer's rewards are based on the PoS consensus, which depends on the deposit strategy as a guarantee against corruption or insufficient validation. This layer includes five validators with known ranks. The second validation layer employs regular nodes as miners, and it is based on the PoW consensus mechanism. This layer is critical for validating and confirming the previous result and encouraging PoW nodes to participate to gain cryptocurrencies and advance in their ranks. The common node is promoted to validator status when the rank reaches a certain threshold or score.

#### 4.2 Mathematical formulation and methodology of a hybrid PoW and PoS consensus algorithm

This section explains integrating PoW and PoS consensus methods to manage Blockchain networks effectively. This section uses the equations and techniques presented in study [62] to manage and secure the Blockchain network. Also, to maintain a secure and decentralized PoW and PoS network, a foundational linear model illustrates the viability of combining these mechanisms. This is further evidenced by various supporting equations used in multiple approaches, such as DASH and Decred, which have been proposed to combine the benefits of PoW and PoS. It means it will be used in our CTIB approach to properly secure and manage the CTIB. The attacker who wants to perform a double-spending attack must stake a certain number of tokens and control 51% of the network's hash power. Moreover, running a mining pool becomes more expensive for the pool owner as they need to acquire a sufficient stake to maximize the efficiency of all the hash power the pool collects.

Zhou [62] provides the following equations:

Maximize  $H'$

subject to

$$H' = \sum_i h'_i \quad (1)$$

$$h'_i \leq h_i, \forall i \quad (2)$$

$$f(s_i) = \min(\alpha * s_i / S, 100\%) \quad (3)$$

$$h'_i \leq f(s_i)H', \forall i \quad (4)$$

where,

- $H'$  is the total effective hash power of the network.
- $h_i$  is the hash power of the miner  $i$ .
- $h'_i$  is the effective hash power of the miner  $i$ .
- $s_i$  is the stake of the miner  $i$ .
- $f(s_i)$  is the maximum percentage of the hash power the miner  $I$  could contribute to the network, namely allowance.
- $S$  is the total circulated tokens.
- $\alpha$  is a system wise constant.

Eq. (1) represents the objective of the PoW and PoS consensus algorithm, which is to maximize the total effective hash power ( $H'$ ) of the network. Maximizing  $H'$  enhances the network's security and resistance to attacks. Eq. (2) is calculating the effective hash power to ensure that the effective hash power of each miner ( $h'_i$ ) cannot exceed their actual hash power ( $h_i$ ). This constraint prevents miners from artificially inflating their influence on the network.  $h_i$  represents the raw computational power of a miner's hardware. It is measured in units like hash rate (hashes per second) and indicates the miner's ability to solve cryptographic puzzles.

Effective hash power ( $h_i$ ), on the other hand, reflects a miner's actual contribution to the network's security, considering not only their raw computational power but also their stake in the network. This means that miners with larger stakes have a greater influence on the network, even if their actual hash power is lower than other miners. Eq. (3) defines the function  $f(s_i)$ , which calculates the allowance for each miner's hash power contribution. The parameter  $\alpha$  represents a system-wise constant, and  $S$  represents the total circulated tokens. This function ensures that miners with larger stakes receive more allowance, but it also limits the maximum allowance to prevent excessive power concentration. We will use  $\alpha$ , where  $\alpha$  is (system-wise constant) and it could be defined as follows:  $\alpha$  represents a system-wise constant that controls the extent to which a miner's stake influences their effective hash power. A higher value of  $\alpha$  places a greater emphasis on staking, while a lower value emphasizes raw computational power. The optimal value of  $\alpha$  depends on the specific characteristics of the network and its desired security profile.

Also, we need to define  $S$ , where  $S$  is the total circulated tokens, and it could be defined as follows:

- $S$  represents the total number of tokens circulating in the PoW and PoS networks. This value is constantly changing as new tokens are created and transactions occur. The total circulated tokens serve as a denominator in the calculation of effective hash power, ensuring that the overall influence of miners is proportional to the total stake in the network.
- Together,  $\alpha$  and  $S$  play a critical role in balancing the influence of computational power and stake in the PoW and PoS consensus mechanisms. By adjusting  $\alpha$ , network administrators can fine-tune the balance between these two factors to achieve the desired level of security and decentralization.

Here's a simplified explanation of how  $\alpha$  and  $S$  affect the effective hash power of miners:

##### High $\alpha$ :

- Miners with larger stakes have a more significant impact on the network's security.
- Encourages greater participation and stake holding among miners.

- Potential risk of excessive power concentration among large stakeholders.

Eq. (4) establishes an upper bound on the effective hash power of each miner based on their stake in the network ( $s_i$ ). The function  $f(s_i)$  determines the maximum allowance for each miner's hash power contribution. This constraint promotes fairness and prevents excessive power concentration among miners.

Low  $\alpha$ :

- Miners with higher computational power have a greater influence.
- Rewards miners for investing in powerful hardware.
- Potential risk of centralization if a few miners own a majority of the network's hash power.

By carefully adjusting  $\alpha$  and considering the total circulated tokens ( $S$ ), network administrators can strike a balance between these factors to maintain a secure and decentralized PoW and PoS network and, to ensure that a miner cannot get more allowance by splitting its stake.

The effective hash power of the first miner ( $h'_1$ ) is calculated as follows:

- Calculate the total stake ( $S$ ) by summing up the stakes of all miners.
- Calculate the allowance ( $f_i$ ) for each miner using the function  $f(s_i) = \min(\alpha * s_i / S, 100\%)$ 
  - Calculate the effective hash power ( $h'_i$ ) of each miner by multiplying its hash power ( $h_i$ ) by its allowance ( $f_i$ ).
  - Calculate the total effective hash power ( $H'$ ) by summing up the effective hash powers of all miners.
- Calculate the effective hash power of the first miner ( $h_i$ ) by taking the first element of the  $h_i$  array.

The function  $f(s_i)$  must satisfy the following two properties:

- $f(s_i)$  is a non-decreasing function.
- $f(s_i)$  is a super-additive function, i.e.,  $f(x) + f(y) < f(x + y)$ .

This ensures that a miner cannot gain more allowance by splitting its stake. In the results section, we illustrate two use cases with numerical examples to demonstrate how to apply the four equations to calculate the appropriate power and the summation of ( $H'$ ).

## 5. RESULTS' ANALYSIS AND DISCUSSION

This section presents the analysis of the test results and includes a discussion of our framework. Section 5.1 demonstrates the effective management of the Blockchain network with the corresponding test results. Section 5.2 illustrates how the CTIB framework successfully defends against a 51% attack. We discuss our results in Section 5.3.

### 5.1 Test results for the effective hash power percentage distribution by stake per $\alpha$

This section demonstrates how to manage the Blockchain network effectively after integrating PoW and PoS consensus methods and the results of the effective hash power percentage distribution by stake per  $\alpha$ .

Example 1:

Eq. (1) is a Linear Programming (LP) problem, which can

be efficiently solved by LP solvers in polynomial time. We assume the following parameters to be used in Eq. (1):

- Total Stake ( $S$ ) = 1
- Percentage stake:  $s = [5\%, 10\%, 25\%, 60\%]$
- There are four miners each of them having equal hash power of the network, e.g., 25 H/s,  $h = [25, 25, 25, 25]$
- $\alpha = 2$

To calculate the maximum percentage of the hash power, we need to get the  $f(s_i)$  from Eq. (3).

**Step 1:** For the first miner, we calculate the stake of the first miner

$$s_1 = 0.05$$

**Step 2:** Now we calculate the allowance ( $f_i$ ) from Eq. (3) for the first miner  $f(s_1)$

$$f_1 = 0.1$$

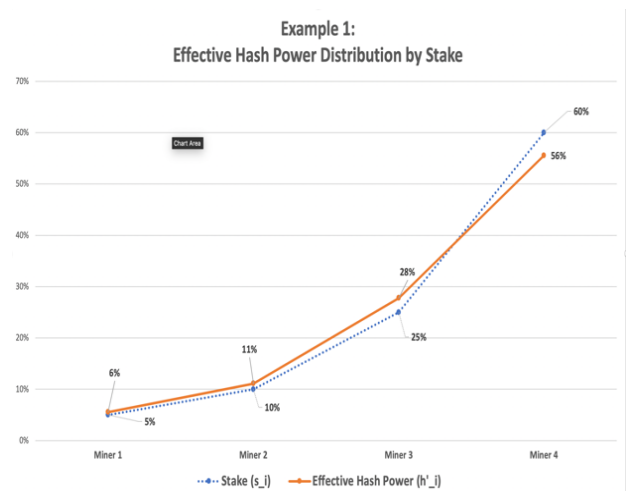
Therefore, the allowance for the first miner is 0.1. The same steps will be repeated for the remaining  $f_i$ . Table 6 illustrates the values of the effective hash power for all miners.

So, the summation of the  $H'$  is 45. The percentage of effective hash power contributed to the network by each miner is: [5.56% 11.11%, 27.78%, 55.56%]. Figure 7 shows the relation between the effective hash power distribution by stake.

The Python Script for the above Formula is given in Figure 8, as shown in the figure the output of the effective hash power of the first miner: 45.

**Table 6.** The effective hash power

Step	Calculation	Result
1	Calculate the total stake ( $S$ ) by summing up the stakes of all miners.	$S = 1.0$
2	Calculate the allowance ( $f_i$ ) for each miner using the function $f(s_i) = \min(\alpha * s_i / S, 1)$ .	$f_i = [0.1, 0.2, 0.5, 1.0]$
3	Calculate the effective hash power ( $h'_i$ ) of each miner by multiplying its hash power ( $h_i$ ) by its allowance ( $f_i$ ).	$h'_i = [2.5, 5.0, 12.5, 25.0]$
4	Calculate the total effective hash power ( $H'$ ) by summing up the effective hash powers of all miners.	$H' = 45.0$



**Figure 7.** Example 1: Effective hash power distribution by stake

If the hash powers were not equal, like in Example 1, the effective power distribution by stake would be different and not aligned. This was tested in the following example

(Example 2).

Example 2:

We assume the following parameters to be used in Eq. (1):

- Total Stack ( $S$ ) = 1
- Percentage stake:  $s = [5\%, 10\%, 25\%, 60\%]$
- There are four miners each of them having equal hash power of the network, e.g., 25 H/s,  $h = [71.4286, 71.4286, 50, 25]$
- $\alpha = 2$

To calculate the maximum percentage of the hash power, we need to use Eq. (3):

Step 1: For the first miner, we calculate the stake of the first miner.

$$s_1 = 0.05$$

Step 2: Now we calculate the allowance ( $f_i$ ) from Eq. (3) for the first miner  $f(s_1)$ .

$$f_1 = 0.1$$

By using the same steps, we calculate the allowance ( $f_i$ ) for the 2nd, 3rd, and 4th miner as follows:

$$f_1 = 0.1$$

$$f_2 = 0.2$$

$$f_3 = 0.5$$

$$f_4 = 1 \text{ (Capped at 1)}$$

Based on this example, the effective hash power of the first miner is 7.14286, the remaining values for the 2nd, 3rd, and 4th effective hash power are as follows.

$$h'_1 = 7.14286$$

$$h'_2 = 14.2857$$

$$h'_3 = 25$$

$$h'_4 = 25$$

The summation of the  $H'$ :

$$H' = 71.4286$$

The percentage of effective hash power contributed to the network by each miner is [10%, 20%, 35%, 35%], Figure 9 shows the relation between the effective hash power distribution by stake. It is proffered that the effectiveness of the hashing capacity may be lower than the combined hashing power. This implies that a miner who has a significant stake in the process may have an easier time mining if the other miners do not have enough stake, as shown in Figure 9.

In the following, we examine the effect of  $\alpha$  on the effective hash power of miners by changing the value of  $\alpha$  in Example 2 and checking the outcome to see how  $\alpha$  affects the effective hash power of miners (using Eqs. (1), (3), and (4)). We calculated the percentage of effective hash power for each  $\alpha$  up to the value of 12 and summarized these percentages in Table 7. Based on the outcomes, we can conclude that by adjusting  $\alpha$ , we can tune the system to be more advantageous to the miner or stakeholders and how combining two consensus, such as PoW and PoS, will reduce the gap between the stakeholder and the miners.

Based on the results, we can observe the following:

1. Even if all miners have the same hash power as Example 1, their stake limits their effective hash power. This encourages miners with insufficient stakes to acquire more stakes to maximize their hash power. This means more participation to get more tokens (stakes).
2. The overall effective hashing capacity might be less than the aggregate hashing power. This suggests a miner with sufficient stake may be easier to mine if the remaining miners do not have sufficient stakes as in Example 2.

```
import numpy as np

# Define the parameters
h = [25, 25, 25, 25] # Hash power of each miner
s = [0.05, 0.1, 0.25, 0.6] # Stake of each miner
alpha = 2 # System-wise constant

# Calculate the total stake
S = sum(s)

# Calculate the allowance for each miner
f = lambda s: min(alpha * s / S, 1)
f_s = np.array([f(si) for si in s])

# Calculate the effective hash power for each miner
h_prime = np.multiply(h, f_s)

# Calculate the total effective hash power
H_prime = sum(h_prime)

# Calculate the effective hash power of the first miner
h_prime_1 = h_prime[0]

print("Effective hash power of the first miner:", h_prime_1)
```

Figure 8. Python script for the effective hash power

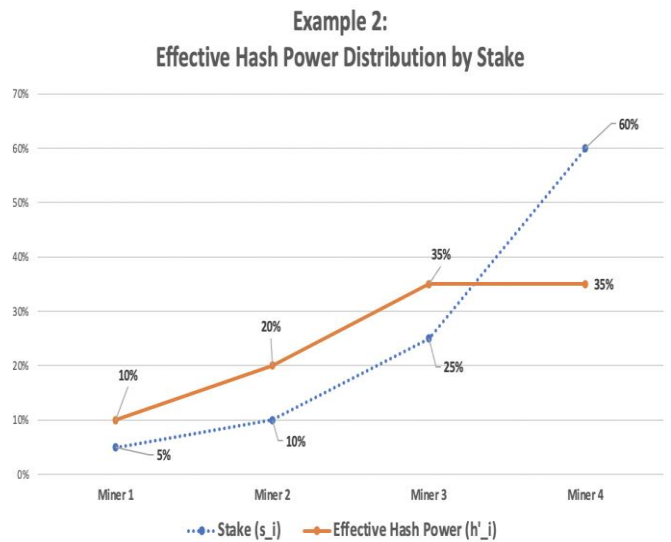


Figure 9. Example 2: Effective hash power distribution by stake

Table 7. The effective hash power percentage distribution by stake per  $\alpha$

Miner	Stake ( $s_i$ )	$\alpha = 2$	$\alpha = 3$	$\alpha = 4$	$\alpha = 5$	$\alpha = 6$	$\alpha = 7$	$\alpha = 8$	$\alpha = 9$	$\alpha = 10$	$\alpha = 11$	$\alpha = 12$
Miner 1	5%	10.00%	11.32%	12.03%	13.90%	15.40%	12.72%	15.40%	15.40%	17.14%	18.85%	20.54%
Miner 2	10%	20.00%	22.65%	24.07%	27.80%	30.79%	25.45%	30.80%	30.80%	34.29%	34.29%	34.29%
Miner 3	25%	35.00%	39.49%	42.15%	38.91%	35.92%	25.46%	24.00%	24.00%	24.00%	24.00%	24.00%
Miner 4	60%	35.00%	26.44%	21.75%	19.44%	17.89%	12.72%	11.99%	11.99%	11.99%	11.99%	11.99%

3. A double-spending attack requires 51% of the effective hash power and  $1/\alpha$  percent of the stake to create a fork mined solely by the attacker as illustrated in Example 1 and Example 2.
4. By adjusting  $\alpha$ , we can tune the system to be more favorable to the miner or stake holder.
5. One challenge arises when miners lack sufficient stake, while staking entities (stake holder) have no interest in mining. This echoes the availability issue inherent in pure PoS systems where validators lack mining capacity. However, in this hybrid PoW and PoS setup, low network hash power incentivizes stake holder to contribute their mining power and maintain stability. To further prevent miners without sufficient stake, we propose an alternative which is to allow them to mine, but at a significantly higher difficulty level compared to well-staked miners.
6. Mining pools in PoW and PoS require significantly more cost than PoW. To efficiently mine blocks, depending on the percentage of the pool's adequate hash power, the pool must acquire the corresponding stakes in the network. In contrast, the running cost of a decent-sized mining pool in PoW is almost negligible compared to its hash power.

Using the described model will combine two consensus, such as PoW and PoS, explaining how we can implement the same steps and concepts in our CTIB framework to prove that our model can resist 51% attacks and properly manage the network.

### 5.2 Test results for CTIB against 51% attack

This section examines the greatest threat to PoW, which is the 51% attack. This attack is successful when a majority of the network agrees on an inaccurate result, with this majority being more significant than 50%. The malicious node (or user) then becomes the key decision maker on the network, allowing them to double-spend their funds and impersonate the original recipient of the transaction. 51% attacks can cause significant

damage to any PoW based network and disrupt the exchange on a Blockchain network. To combat this, a hybrid protocol can be employed, combining two or more existing proofs (PoW and PoS), to improve consensus and make the network sufficiently resistant to the 51% attack. While PoS can prevent 51% attacks, PoW is not as secure. Therefore, we have used PoS as the dominant layer to ensure sufficient security.

If a 51% attack occurs in the PoW layer, the PoS validator detects it. The use of both PoW and PoS results in reduced power and computation consumption compared to using PoW alone. Moreover, in case the primary layer (PoS) is busy or unreachable, the system will automatically shift to the secondary layer (PoW), until a validator from the primary layer becomes free to review and initiate the validation process.

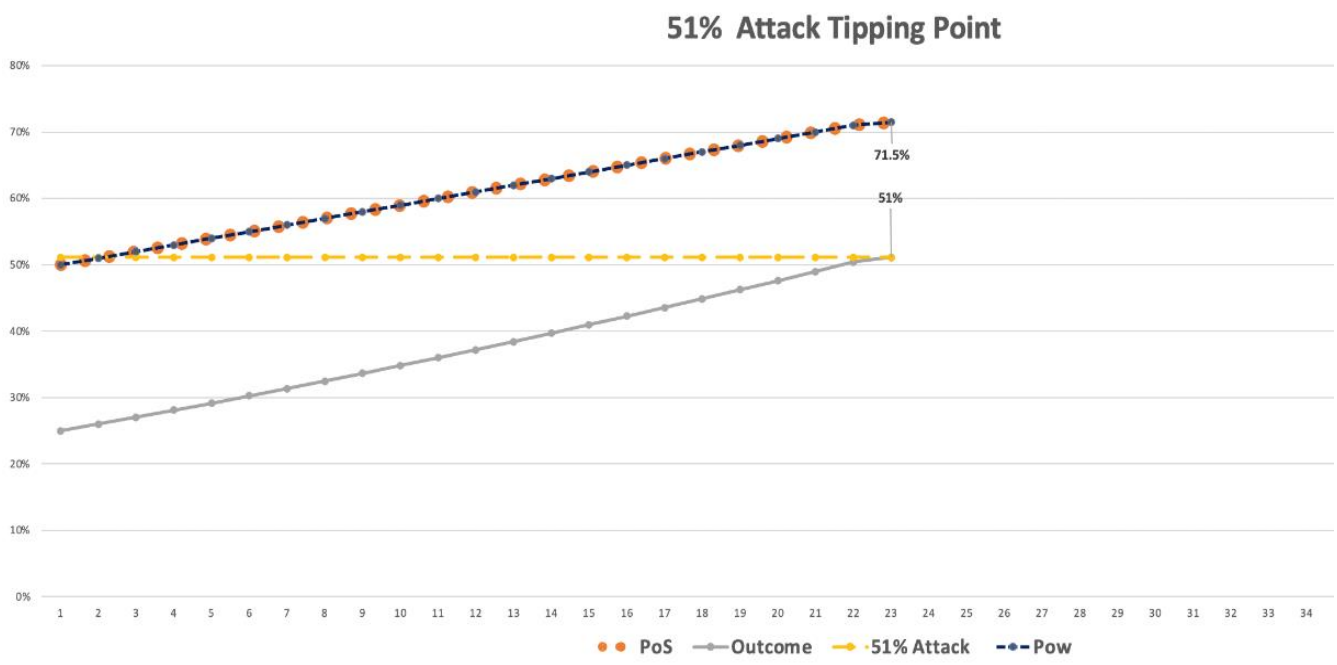
We proved that applying a 51% corruption ratio to both PoW and PoS separately results in a 51% attack. By applying our combined two layers Integrity Blockchain (CTIB), which comprises the two consensus algorithms, we achieved a remarkable performance improvement by reducing the corruption percentage to 26.01% based on Eq. (5).

$$\text{Prob}(\text{combined}) = \text{Prob}(\text{PoW}) \times \text{Prob}(\text{PoS}) \quad (5)$$

Table 8 shows the results of the corruption probability equation for a 51% attack. The attack was implemented on each consensus method to demonstrate how CTIB offers superior protection against such attacks.

**Table 8.** The results of the corruption probability equation for a 51% attack

PoW Corrupted Ratio	PoS Corrupted Ratio	Outcome
50%	50%	25%
51%	51%	26%
52%	52%	27%
...	...	...
70%	70%	49%
71%	71%	50%
71.5%	71.5%	51%



**Figure 10.** The 51% tipping point in CTIB

According to Table 8, the CTIB network can be taken down through a majority attack, which would be a complex process. The table displays the outcomes of implementing CTIB against a 51% attack, considering two methods of consensus, PoW and PoS. For a 51% attack to be successful, the malicious node must have control over at least 71.5% of the processing capacity in PoW and 71.5% of the staked coins in PoS. For a 51% attack to succeed, the node carrying out the attack must have control over at least 71% of the processing power in a PoW system and 71% of the staked coins in a PoS system. If this threshold is met, the chances of a successful attack are greatly heightened. However, achieving such capabilities is highly unlikely and unrealistic. This is how our system protects itself against a 51% attack, as illustrated in Figure 10.

### 5.3 Discussion

In this section, we discuss the advantages, limitations, and potential challenges that could be addressed using CTIB and provide directions for model improvement.

#### 5.3.1 Advantages of CTIB

In the previous sections, we tested CTIB against 51% and demonstrated how CTIB prevents 51% attack. However, threats and challenges still need to be addressed and tested for CTI. The significant threats and challenges for CTI with traditional only one consensus are as follows:

- 1) Fork Attack
- 2) Double Spending
- 3) Resource Consumption
- 4) Sybil Attack
- 5) High Availability and Single Point of Failure (SPoF):

If the consensus network is unavailable or congested for any reason, how will it be restored?

- 6) Multilayer of Corruption

What steps should be taken to resolve a 51% attack if it occurs?

CTIB is designed to defeat and solve these threats by:

1. Preventing Fork Attacks
  - a. Combining PoW and PoS significantly increases the difficulty and cost of executing a Fork attack.
  - b. Diversified Attack Vectors: In a hybrid system, an attacker must overcome the security measures of both PoW and PoS simultaneously.
  - c. This dual-layer security makes it much harder to execute a successful attack. PoW provides robust protection against brute-force attacks, while PoS protects against

economic attacks and ensures validators are financially committed to the network's integrity.

- d. Improved Chain Selection and Finality: A hybrid system can implement checkpoints or finality mechanisms from PoS to solidify the blockchain at regular intervals, preventing long-range attacks. PoS checkpoints can ensure that once a block is finalized, it cannot be reverted, even if a temporary PoW fork occurs.
2. Preventing Double Spending
  - a. The hybrid system provides a redundant layer of security. If an attacker compromises one consensus mechanism, the other mechanism still protects the network.
  - b. This makes it highly unlikely for double spending to occur, as both mechanisms would need to be compromised simultaneously.
3. Managing Resource Consumption
  - a. By using PoW for initial block creation and PoS for block validation, the system can balance the high security of PoW with the energy efficiency of PoS. This approach reduces the overall energy consumption compared to a pure PoW system.
  - b. PoS eliminates the need for energy-intensive computations. Validators are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they hold and are willing to "stake" as collateral, significantly reducing energy use.
  - c. PoS reduces the need for expensive hardware, lowering the entry barrier for validators and reducing overall resource consumption.
4. Ensuring High Availability
  - a. To ensure high availability, we have designed two consensus layers to ensure that the second layer takes over if the primary layer is busy or unreachable, allowing for smooth result generation.
5. Managing Multilayer Corruption

The CTIB hybrid approach can identify any corruption, as tested successfully in Section 5.

Table 9 compares CTIB with other methods integrating CTI and Blockchain mentioned in Table 4 [15-39].

**Table 9.** Comparison of CTIB and other integrated CTI with Blockchain papers

Papers	Quality Measures, Confidentiality, Credibility & Non-Repudiation, Undesirable Publicity	Challenges						
		51% Attack	Fork Attack	Double Spending	Resource Consumption	Sybil Attack	High Availability	Multilayer of Corruption
CTIB	Solved	Solved	Solved	Solved	Solved	Affected	Covered	Detected
our model [15-39]		Affected					Not Covered	Not Detected

### 5.3.2 Limitations and prospect challenges in CTIB

For our new CTIB module framework to function effectively, the following factors must be fulfilled:

1. The Blockchain network should be designed as outlined in Section 4.

2. Both types of consensus (PoW & PoS) are required.

3. CTI technology with Threat Intelligence Sharing Format Standards, utilizing one of the following: STIX, TAXII, or CybOX.

Without these key factors, the CTIB will not function effectively. The Blockchain network must be properly designed, as discussed in Section 4, to ensure its proper functioning. Additionally, the intranet protocol between the Blockchain and CTI should facilitate seamless communication, and the two types of consensus should be implemented to integrate and communicate effectively with the CTI technology through the threat intelligence sharing format standards for unity.

As a prospect, challenges in CTIB are a Blockchain based framework that uses two consensus' algorithms, exposing it to the challenges and flaws inherent in Blockchain technology. Using two consensus layers in CTIB emphasizes Blockchain's technical challenges. Our analysis identified challenges affecting Blockchain and CTI [63], abstracted below. One of the main challenges for our CTIB framework is the consumption of resources in the second layer, PoW. While a consensus algorithm like PoW protects against adversaries, it generates high computational costs and electricity charges, leading to daily energy consumption of around 15 million dollars [63]. An alternative consensus algorithm, such as PoA, should be considered to address this issue to reduce power consumption. The second prospect challenge is Sybil's attack. Sybil's attack is an assault on a Blockchain network service. An adversary subverts the service's reputation system by creating many anonymous identities and utilizing them to gain massively significant influence [33].

### 5.3.3 Directions for model improvement for CTIB

One direction for improving the CTIB model is to create a simulation to test our approach against other consensus protocols. This involves comparing various scenarios and analyzing the results to identify the optimal hybrid consensus for constructing a unified CTIB. Another direction for improvement is to explore how artificial intelligence can be leveraged to address anticipated issues in the CTIB, such as Fork and Sybil attacks. Additionally, AI can be used to build better reports, assist in evaluations, and review and assess the content.

## 6. CONCLUSIONS

As Internet technologies become the foundation of human life, cybercrime is rising. Defending against cybercrime with traditional methods is ineffective as attackers will change their methods and techniques to circumvent these security controls. Since most of these attacks are sophisticated, it is necessary to share the attack anatomy and details once the attack has been detected. This method is known as CTI. The current CTI faces several challenges and limitations, including the lack of quality control, privacy, integrity, and the inability to provide non-repudiation. These issues indicate the need for enhanced CTI systems. The ability of Blockchain to conceal one's identity and location across the network distinguishes it. Due

to decentralization, records can be shared across all Blockchain nodes, ensuring data replication. For the reason that all historical records are already copied at every node, changing them is difficult. As a result, Blockchain is the most appropriate technology for use and integration with the CTI.

After integrating CTI with a Blockchain using a single consensus mechanism, threats such as Fork attacks, Double Spending, Resource Consumption, Sybil Attacks, Single Point of Failure, and Multilayer Corruption persist. To address these challenges, we developed CTIB, a new framework that resolves issues in traditional CTI and systems integrating CTI with Blockchain using only one consensus. CTIB facilitates anonymous data sharing and ensures high availability by switching to PoW if the PoS layer is occupied.

In conclusion, we tested our CTIB model against 51% attacks and demonstrated its effectiveness statistically. For an attack to succeed, the malicious node has to control at least 71.5% of both the processing power in PoW and the staked coins in PoS. This threshold makes such an attack highly unlikely. Our system effectively protects against a 51% attack by requiring these high control levels. In addition, CTIB model can resist Double Spending and Fork attacks. This is achieved with low power consumption as the use of PoS results in a reduction of the power needed. Finally, we evaluated the effective hash power distribution by stake and discussed the advantages, limitations, and potential improvements for the CTIB model.

In the future, we will focus on creating a simulation to test our new approach, comparing various contests, and analyzing the results to determine the best hybrid consensus for constructing a unified CTIB. We will also explore how artificial intelligence can help addressing any expected issues in the CTIB, such as Fork and Sybil attacks.

## REFERENCES

- [1] Kure, H.I., Islam, S., Mouratidis, H. (2022). An integrated cyber security risk management framework and risk predication for the critical infrastructure protection. *Neural Computing and Applications*, 34(18): 15241-15271. <https://doi.org/10.1007/s00521-022-06959-2>
- [2] Couretas, J.M. (2022). Cyber systems design. In: *An Introduction to Cyber Analysis and Targeting*. Springer, Cham, pp. 173-195. [https://doi.org/10.1007/978-3-030-88559-5\\_8](https://doi.org/10.1007/978-3-030-88559-5_8)
- [3] Coulter, R., Zhang, J., Pan, L., Xiang, Y. (2022). Domain adaptation for windows advanced persistent threat detection. *Computers & Security*, 112: 102496. <https://doi.org/10.1016/j.cose.2021.102496>
- [4] Shi, H., Wang, W., Liu, L., Lin, Y., Liu, P., Xie, W., Wang, H., Zhang, Y. (2022). Threat intelligence sharing model and profit distribution based on blockchain and smart contracts. In: Liu, Q., Liu, X., Chen, B., Zhang, Y., Peng, J. (eds) *Proceedings of the 11th International Conference on Computer Engineering and Networks*. Lecture Notes in Electrical Engineering, vol 808. Springer, Singapore. pp. 645-654. [https://doi.org/10.1007/978-981-16-6554-7\\_70](https://doi.org/10.1007/978-981-16-6554-7_70)
- [5] Borges Amaro, L.J., Percilio Azevedo, B.W., Lopes de Mendonca, F.L., Giozza, W.F., Albuquerque, R.D.O., García Villalba, L.J. (2022). Methodological framework to collect, process, analyze and visualize cyber threat

- intelligence data. *Applied Sciences*, 12(3): 1205. <https://doi.org/10.3390/app12031205>
- [6] Özdemir, A. (2021). Cyber threat intelligence sharing technologies and threat sharing model using blockchain. Ph.D. dissertation. Middle East Technical University, Ankara, Turkey. <https://hdl.handle.net/11511/90897>.
- [7] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. *IEEE Access*, 8: 79764-79800. <https://doi.org/10.1109/ACCESS.2020.2988579>
- [8] von Wangenheim, G. (2020). Blockchain-based land registers: A law-and-economics perspective. In: LeHAVI, A., Levine-Schnur, R. (eds) *Disruptive Technology, Legal Innovation, and the Future of Real Estate*. Springer, Cham, pp. 103-122. [https://doi.org/10.1007/978-3-030-52387-9\\_6](https://doi.org/10.1007/978-3-030-52387-9_6)
- [9] Prieto, Y., Figueroa, M., Pezoa, J.E. (2021). Maximizing network reliability to 0-day exploits through a heterogeneous node migration strategy. *IEEE Access*, 9: 97747-97759. <https://doi.org/10.1109/ACCESS.2021.3095149>
- [10] Saxena, S., Bhushan, B., Ahad, M.A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications*, 181: 103050. <https://doi.org/10.1016/j.jnca.2021.103050>
- [11] Mollah, M.B., Zhao, J., Niyato, D., Lam, K.Y., Zhang, X., Ghias, A.M., KOH, L.H., Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things Journal*, 8(1): 18-43. <https://doi.org/10.1109/JIOT.2020.2993601>
- [12] Ismail, L., Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, 11(10): 1198. <https://doi.org/10.3390/sym11101198>
- [13] Antonopoulos, A.M. (2014). *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*. O'Reilly Media, Inc., Sebastopol, California. <https://dl.acm.org/doi/abs/10.5555/2695500>.
- [14] El-Kosairy, A., Abdelbaki, N., Aslan, H. (2023). A survey on cyber threat intelligence sharing based on blockchain. *Advances in Computational Intelligence*, 3(3): 10. <https://doi.org/10.1007/s43674-023-00057-z>
- [15] Riesco, R., Larriva-Novo, X., Villagr a, V.A. (2020). Cybersecurity threat intelligence knowledge exchange based on blockchain: Proposal of a new incentive model based on blockchain and Smart contracts to foster the cyber threat and risk intelligence exchange of information. *Telecommunication Systems*, 73: 259-288. <https://doi.org/10.1007/s11235-019-00613-4>
- [16] Tanrıverdi, M., Tekerek, A. (2019). Implementation of blockchain based distributed web attack detection application. In 2019 1st International Informatics and Software Engineering Conference (UBMYK), Ankara, Turkey, pp. 1-6. <https://doi.org/10.1109/UBMYK48245.2019.8965446>
- [17] Gong, S., Lee, C. (2020). BLOCIS: Blockchain-based cyber threat intelligence sharing framework for sybil-resistance. *Electronics*, 9(3): 521. <https://doi.org/10.3390/electronics9030521>
- [18] Aljihani, H., Eassa, F., Almarhabi, K., Algarni, A., Attaallah, A. (2021). Standalone behaviour-based attack detection techniques for distributed software systems via blockchain. *Applied Sciences*, 11(12): 5685. <https://doi.org/10.3390/app11125685>
- [19] Guha Roy, D., Srirama, S.N. (2021). A blockchain-based cyber attack detection scheme for decentralized Internet of Things using software-defined network. *Software: Practice and Experience*, 51(7): 1540-1556. <https://doi.org/10.1002/spe.2972>
- [20] Gadekallu, T.R., MK, M., Sivarama Krishnan, S., Kumar, N., Hakak, S., Bhattacharya, S. (2020). Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. *IEEE Internet of Things Magazine*, 4(3): 30-33. <https://doi.org/10.1109/IOTM.1021.2000160>
- [21] Rathore, S., Kwon, B.W., Park, J.H. (2019). BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications*, 143: 167-177. <https://doi.org/10.1016/j.jnca.2019.06.019>
- [22] Suhail, S., Jurdak, R. (2021). Towards trusted and intelligent cyber-physical systems: A security-by-design approach. arXiv:2105.08886. <https://doi.org/10.48550/arXiv.2105.08886>
- [23] Banerjee, M., Lee, J., Choo, K.K.R. (2018). A blockchain future for internet of things security: A position paper. *Digital Communications and Networks*, 4(3): 149-160. <https://doi.org/10.1016/j.dcan.2017.10.006>
- [24] Homayoun, S., Dehghantanha, A., Parizi, R.M., Choo, K.K.R. (2019). A blockchain-based framework for detecting malicious mobile applications in app stores. In 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, pp. 1-4. <https://doi.org/10.1109/CCECE.2019.8861782>
- [25] Cha, J., Singh, S.K., Pan, Y., Park, J.H. (2020). Blockchain-based cyber threat intelligence system architecture for sustainable computing. *Sustainability*, 12(16): 6401. <https://doi.org/10.3390/su12166401>
- [26] Smys, S., Haoxiang, W. (2020). Data elimination on repetition using a blockchain based cyber threat intelligence. *IRO Journal on Sustainable Wireless Systems*, 2(4): 149-154. <https://irojournals.com/iros/ws/article/view/2/4/2>.
- [27] Si, H., Sun, C., Li, Y., Qiao, H., Shi, L. (2019). IoT information sharing security mechanism based on blockchain technology. *Future Generation Computer Systems*, 101: 1028-1040. <https://doi.org/10.1016/j.future.2019.07.036>
- [28] Wu, Y., Qiao, Y., Ye, Y., Lee, B. (2019). 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, pp. 474-481. <https://doi.org/10.1109/IOTSMS48152.2019.8939192>
- [29] Putz, B., Pernul, G. (2020). Detecting blockchain security threats. In 2020 IEEE International Conference on Blockchain (Blockchain), Rhodes, Greece, pp. 313-320. <https://doi.org/10.1109/Blockchain50366.2020.00046>
- [30] Hajizadeh, M., Afraz, N., Ruffini, M., Bauschert, T. (2020). Collaborative cyber attack defense in SDN networks using blockchain technology. In 2020 6th IEEE Conference on Network Softwareization (NetSoft), Ghent,

- Belgium, pp. 487-492. <https://doi.org/10.1109/NetSoft48620.2020.9165396>
- [31] Mendez Mena, D., Yang, B. (2020). Decentralized actionable cyber threat intelligence for networks and the Internet of Things. *IoT*, 2(1): 1-16. <https://doi.org/10.3390/iot2010001>
- [32] Allouche, Y., Tapas, N., Longo, F., Shabtai, A., Wolfsthal, Y. (2021). Trade: Trusted anonymous data exchange: Threat sharing using blockchain technology. *arXiv:2103.13158*. <https://doi.org/10.48550/arXiv.2103.13158>
- [33] He, S., Fu, J., Jiang, W., Cheng, Y., Chen, J., Guo, Z. (2021). 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. <https://doi.org/10.1145/3444370.3444623>
- [34] Falco, G., Li, C., Fedorov, P., Caldera, C., Arora, R., Jackson, K. (2019). NeuroMesh: IoT security enabled by a blockchain powered botnet vaccine. In *Proceedings of the International Conference on Omni-Layer Intelligent Systems*, pp. 1-6. <https://doi.org/10.1145/3312614.3312615>
- [35] Dunnett, K., Pal, S., Jadidi, Z. (2022). Challenges and opportunities of blockchain for cyber threat intelligence sharing. In: Pal, S., Jadidi, Z., Foo, E. (eds) *Secure and Trusted Cyber Physical Systems. Smart Sensors, Measurement and Instrumentation*, vol 43. Springer, Cham, pp. 1-24. [https://doi.org/10.1007/978-3-031-08270-2\\_1](https://doi.org/10.1007/978-3-031-08270-2_1)
- [36] Khalil, U., Malik, O.A., Hussain, S. (2022). A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. *IEEE Access*, 10: 76805-76823. <https://doi.org/10.1109/ACCESS.2022.3189998>
- [37] Jiang, T., Shen, G., Guo, C., Cui, Y., Xie, B. (2023). BFLS: Blockchain and federated learning for sharing threat detection models as cyber threat intelligence. *Computer Networks*, 224: 109604. <https://doi.org/10.1016/j.comnet.2023.109604>
- [38] Chatziamanetoglou, D., Rantos, K. (2023). Blockchain-based cyber threat intelligence sharing using proof-of-quality consensus. *Security and Communication Networks*, 2023(1): 3303122. <https://doi.org/10.1155/2023/3303122>
- [39] Dunnett, K., Pal, S., Jadidi, Z., Jurdak, R. (2023). A blockchain-based framework for scalable and trustless delegation of cyber threat intelligence. In *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Dubai, United Arab Emirates, pp. 1-9. <https://doi.org/10.1109/ICBC56567.2023.10174885>
- [40] Nazir, A., He, J., Zhu, N., Wajahat, A., Ullah, F., Qureshi, S., Ma, S., Pathan, M.S. (2024). Collaborative threat intelligence: Enhancing IoT security through blockchain and machine learning integration. *Journal of King Saud University-Computer and Information Sciences*, 36(2): 101939. <https://doi.org/10.1016/j.jksuci.2024.101939>
- [41] Cao, B., Zhang, Z., Feng, D., Zhang, S., Zhang, L., Peng, M., Li, Y. (2020). Performance analysis and comparison of PoW, PoS and DAG based blockchains. *Digital Communications and Networks*, 6(4): 480-485. <https://doi.org/10.1016/j.dcan.2019.12.001>
- [42] Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of Financial Studies*, 34(3): 1156-1190. <https://doi.org/10.1093/rfs/hhaa075>
- [43] Chatziagiannis, P., Chalkias, K. (2021). Proof of assets in the diem blockchain. In: *Applied Cryptography and Network Security Workshops (ACNS 2021)*. Lecture Notes in Computer Science, vol 12809. Springer, Cham, pp. 27-41. [https://doi.org/10.1007/978-3-030-81645-2\\_3](https://doi.org/10.1007/978-3-030-81645-2_3)
- [44] Liu, W.J., Chiu, W.Y., Hua, W. (2024). Blockchain-enabled renewable energy certificate trading: A secure and privacy-preserving approach. *Energy*, 290: 130110. <https://doi.org/10.1016/j.energy.2023.130110>
- [45] Khan, F.A., Asif, M., Ahmad, A., Alharbi, M., Aljuaid, H. (2020). Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development. *Sustainable Cities and Society*, 55: 102018. <https://doi.org/10.1016/j.scs.2020.102018>
- [46] Douceur, J.R. (2002). The Sybil Attack. In: Druschel, P., Kaashoek, F., Rowstron, A. (eds) *Peer-to-Peer Systems. IPTPS 2002*. Lecture Notes in Computer Science, vol 2429. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/3-540-45748-8\\_24](https://doi.org/10.1007/3-540-45748-8_24)
- [47] Decred. Decred – Money Evolved. <https://www.decred.org/>, accessed on Mar. 23, 2024.
- [48] Akbar, N.A., Muneer, A., ElHakim, N., Fati, S.M. (2021). Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensus. *Future Internet*, 13(11): 285. <https://doi.org/10.3390/fi13110285>
- [49] Wu, Y., Song, P., Wang, F. (2020). Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain. *Mathematical Problems in Engineering*, 2020(1): 7270624. <https://doi.org/10.1155/2020/7270624>
- [50] Liu, Z., Tang, S., Chow, S.S., Liu, Z., Long, Y. (2019). Fork-free hybrid consensus with flexible proof-of-activity. *Future Generation Computer Systems*, 96: 515-524. <https://doi.org/10.1016/j.future.2019.02.059>
- [51] Gupta, K.D., Rahman, A., Poudyal, S., Huda, M.N., Mahmud, M.P. (2019). A hybrid POW-POS implementation against 51 percent attack in cryptocurrency system. In *2019 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, Sydney, NSW, Australia, pp. 396-403. <https://doi.org/10.1109/CloudCom.2019.00068>
- [52] Sun, Y., Rajasekaran, A. (2019). An interleaving hybrid consensus protocol. *arXiv:1911.09262*. <https://doi.org/10.48550/arXiv.1911.09262>
- [53] Huang, Y., Zeng, Y., Ye, F., Yang, Y. (2020). Incentive assignment in PoW and PoS hybrid blockchain in pervasive edge environments. In *2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)*, Hang Zhou, China, pp. 1-10. <https://doi.org/10.1109/IWQoS49365.2020.9212842>
- [54] Baudlet, M., Doudou, F.A.L.L., Taenaka, Y., Kadobayashi, Y. (2020). The best of both worlds: A new composite framework leveraging pos and pow for blockchain security and governance. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, Paris, France, pp. 17-24. <https://doi.org/10.1109/BRAINS49436.2020.9223280>
- [55] Ouyang, Z., Shao, J., Zeng, Y. (2021). PoW and PoS and related applications. In *2021 International Conference on*



- Electronic Information Engineering and Computer Science (EIECS), Changchun, China, pp. 59-62. <https://doi.org/10.1109/EIECS53707.2021.9588080>
- [56] Santos, R.P.D., Swan, M. (2018). Pow, PoS, & hybrid protocols: A matter of complexity? arXiv:1805.08674. <https://doi.org/10.48550/arXiv.1805.08674>
- [57] Prashant, B., Makrant, I., Mansi, M. (2019). Migration from POW to POS for Ethereum. Engineering Archive. <https://doi.org/10.31224/osf.io/ad8en>
- [58] Harvilla, M., Du, J. (2019). Prospective hybrid consensus for project PAI. arXiv:1902.02469. <https://doi.org/10.48550/arXiv.1902.02469>
- [59] Duong, T., Chepurnoy, A., Fan, L., Zhou, H.S. (2018). TwinsCoin: A cryptocurrency via proof-of-work and proof-of-stake. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, pp. 1-13. <https://doi.org/10.1145/3205230.3205233>
- [60] Abuidris, Y., Kumar, R., Yang, T., Onginjo, J. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. ETRI Journal, 43(2): 357-370. <https://doi.org/10.4218/etrij.2019-0362>
- [61] Thanujan, T., Rajapakse, C., Wickramaarachchi, D. (2021). A community-based hybrid blockchain architecture for the organic food supply chain. In 2021 International Research Conference on Smart Computing and Systems Engineering (SCSE), Colombo, Sri Lanka, pp. 77-83. <https://doi.org/10.1109/SCSE53661.2021.9568325>
- [62] Zhou, Q. (2019). Proof staked work – A simple hybrid PoW/PoS with potential stronger 51%-attack resistant. <https://ethresear.ch/t/proof-staked-work-a-simple-hybrid-pow-pos-with-potential-stronger-51-attack-resistant/4740>.
- [63] Sharad Mangrulkar, R., Vijay Chavan, P. (2024). Bitcoin. In: Blockchain Essentials. Apress, Berkeley, CA, pp. 83-121. [https://doi.org/10.1007/978-1-4842-9975-3\\_3](https://doi.org/10.1007/978-1-4842-9975-3_3)