


Blockchain Based Information Sharing Mechanism for Cyber Threat Intelligence

E. BUBER, O.K. SAHINGOZ


Abstract— In recent years, networked computers are extensively used in every aspect of our daily lives. Besides, the anonymous structure of the Internet results in an increase in the number of attacks not only for individual users but also for local area networks. Current attacks are more sophisticated, and they are developed by experienced intruders with the use of automated malware production methods. These organized intrusions can go over the defense lines of the systems due to the weakness of the detection/prevention mechanisms or carelessness of individual users. After sneaking into the system, these attacks can work until they are detected, and they can access many critical resources of the company. Earlier detection of these attacks is very trivial issue for the security admins. This can be accomplished by acquiring the signature (critical information) of the newest attacks as early as possible. One suggested solution is the use of a *Threat Information Sharing* system, which is set up between security firms and authorities. This approach enables the distribution of the marks of the recent (zero-day) attacks and the development of some proactive prevention mechanisms for them. The use of both peer to peer and centralized sharing mechanisms have some inherited deficiencies. Therefore, in this paper, a pure decentralized cybersecurity information sharing system is proposed with the use of blockchain technology. A controlled decision-making mechanism, authorization termination, and rule-sets maintenance are proposed to make distributed decisions within the system. For making a decision, two smart contracts should be used in the blockchain. One holds the positive votes while the other holds the negative ones. Members of the system are able to access cyber threat data by using company-related queries. The system can facilitate the integration of many data sources into cybersecurity management system. Additionally, it enables us to collect in a single repository that can be accessed for implementing real-time cybersecurity applications.

Index Terms— blockchain, cyber threat intelligence, information sharing, controlled decision-making mechanism, smart contract.

EBUBEKIR BUBER, is with Department of Computer Engineering at Yildiz Technical University, Istanbul, Turkey (e-mail: ebubekirbbr@gmail.com).

 <https://orcid.org/0000-0002-0586-7514>

OZGUR KORAY SAHINGOZ, is with Department of Computer Engineering at Istanbul Kultur University, Istanbul, Turkey, (e-mail: o.sahingoz@iku.edu.tr).

 <https://orcid.org/0000-0002-1588-8220>

Manuscript received November 10, 2019; accepted June 10, 2020.
DOI: 10.17694/bajece.644948

I. INTRODUCTION

IN RECENT years, computer technologies have been developed rapidly and continue to evolve. This development has also brought some negative effects with it. Parallel to this enhancement, there is a steady increase in cyber-attacks.

As a result of digitalization, not only the huge companies but also the small ones (even single users) have become more sensitive to the privacy and security of their data where much of their personal information is stored in the cyberworld.

In the 2019 report of Ninth Annual Cost of Cybercrime Study of Accenture [1], the average loss of companies exposed to cyber-attack in 2018 increased to \$ 13.0 M, compared to \$ 11.7 M in 2017. According to the report, the increase in the last year is about 12% and the increase in the last 5 years is about 72%. For the next five years, the total value at risk from cybercrime is expected as \$5.2 trillion. Therefore, to preserve the companies, some additional protection mechanisms should be constructed.

In traditional way the security of the network can be established with the use of firewall mechanisms and intrusion detection mechanisms (IDSs)[2][3][4]. Although the use of these systems is very efficient, the success of them directly related with the definition of threats and attacks in a quick and up to date way for catching the zero-day type attacks.

Many companies do research on detection and prevention systems to make their systems more secure against cyber-attacks. Their experiences are stored as a knowledgebase in their systems that construct intelligence. This intelligence can either be gained after encountering some type of attacks or by accessing this information over some servers, which are maintained and shared by some security firms or agencies. This shared information is called *Cyber Threat Intelligence*. For example, Phishtank [5] shares URL addresses that are used in a phishing attack to anyone. Some additional ones can be listed as follows; IBM X-Force Exchange [6], Palo Alto Networks Auto Focus [7], LogRhythm Threat Lifecycle Management [8], FireEye iSIGHT [9], LookingGlass Cyber Solutions [10], Normshield Inc. [11], Firehol IP Lists [12].

There are 3 different groups of companies who share their cyber threat information as follows.

- Companies, which share the information free of charge (e.g., government agencies)
- Companies, which share the information with a fee (e.g., some commercial firms)
- Companies, which provide the information to users free

of charge after a certain period from the detection of threat, while charging for up to date sharing (e.g., some commercial firms)

These companies can share the information either via their web pages or through an API. Many companies prefer the second method, and their cyber threat information can be accessed from a single centralized platform by using an API. In order to collect data from different platforms, users must perform some additional efforts for each cyber threat information server.

For the threat information sharing companies, the amount of data stream is quite high. This data sharing can be either in peer to peer communication model or in a client server architecture. Each of them has some specific deficiencies. Collecting and distributing data from a single data center slow down the system and make it difficult to scale. It is thought that sharing information with a distributed structure should be more efficient than gathering and sharing in a single center. Therefore, in this study, a blockchain-based approach was proposed to share the cyber threat information data in a distributed way.

Blockchain technology emerged as an acceptable solution for a distributed solution. Setting up a blockchain network gives trust to the information distribution service, which can be on untrusted sources. The system also combines easy access from anywhere in the world by using a global network like the Internet, with cryptographic security to give each member a fast and safe way to verify critical information by establishing trust between them. Members (companies) can easily add threat information for being accessible by each member in the system. However, some information should only be accessible by authorized users depending on their membership type.

In this paper, a distributed cybersecurity information system is proposed to keep the protection mechanism of the system up to date. The system is designed with the blockchain technology to enable a cryptographic security mechanism in a distributed structure. Not only the reliability but also the up to date cyber threat information are very critical for security admins. An axiom for incorrect cyber threat information can have very bad consequences. Cyber threat information can be verified, and information can be extracted about the reliability of this information, with the proposed blockchain mechanism. Many companies can enter data about the same asset (e.g., IP). They can enter cyber threat information for the same malicious IP address. This makes it easier to analyze assets that are false positive, while those that are harmful stand out. The information added to the chain cannot be changed or deleted due to the blockchain structure. This means that the cyber threat information data for the system to be designed should be stored continuously in a historical way.

In the proposal, some decisions need to be taken at some stages. Therefore, a controlled decision-making mechanism is designed to make the necessary decisions to ensure the functioning of the system. This mechanism is built on a voting-based system. Decision-making is carried out on a distributed structure within the system. Smart Contracts are generally preferred to solve his situation used.

The rest of the paper is organized as follows: In the next Section, the background information on blockchain technology is explained. The proposed blockchain structure for the cyber threat information system and detailed analysis of this system is detailed in section III and Section IV, respectively. Finally, the discussion and conclusion about the topic are drawn.

II. LITERATURE REVIEW

Cybersecurity is a very critical issue not only in civil life but also in the military field [13]. Cyberpower and abilities are among the most important power elements among states today. Accordingly, we started to see blockchain technology more and more every day in the military field as well as the other fields [14]. The protection of personal data has become a very important issue for all applications today. There are many application areas where blockchain technology is applied in the field of cybersecurity [15]. With the proliferation of the Internet of Things (IoT), the small devices we use in our daily lives have become connected to the internet and can communicate with each other. The security of data transfer between these devices is a very important issue. IoT related studies on networks and machine visualization, public-key cryptography, web applications, certification schemes, and the secure storage of Personally Identifiable Information (PII) are included in the literature.

Systematic integration of the IoT and Cyber-Physical Systems (CPS) into the supply chain has also brought new complexities to the threat environment to increase operational efficiency and quality. And IoT devices can be easily targeted by attackers. [16] introduced an innovative blockchain-based secure and privacy-preserving data sharing mechanism for IoT devices (specifically for smart cities). Identifying cyber threats and planning the axioms required for possible cyber incidents are routine procedures for many computer network systems. Blockchain technology can be applied to intrusion detection systems as it maintains data integrity and provides transaction transparency [17].

For the threat information sharing companies, the amount of data stream is quite high. This data sharing can be either in peer to peer communication model or in a client server architecture. Each of them has some specific deficiencies. Some institutions share cyber intelligence data to reduce the cost of cyber-attacks on a global scale. Integration of these shared data into cybersecurity products and keeping these data up to date can be costly. As a solution to this situation, studies in which blockchain-based cyber intelligence data are shared are proposed [18][19][20].

Blockchain-based systems have risks, as with any application, associated with cyber-attacks [21]. For example, weaknesses arising from blockchain code, vulnerabilities that may result in end-user applications, weaknesses arising from the application environment where blockchain application is run, etc. These risks should be considered in the system to be developed and should be minimized. Besides, blockchain can also be used for cybersecurity such as visualization for security management [22], cyber insurance for cyber risk

management [23], and cyber forensics analysis [24].

Similar to these works, this technology can also be applied in some new and popular concepts such as smart cities for setting up an dynamic and distributes security mechanism by also using different data transfer models such as publish subscribe communication paradigm [25][26].

III. BLOCKCHAIN

Blockchain technology has become more popular in recent years, with Bitcoin [27] and Ethereum [28]. Bitcoin and other virtual currencies are built on blockchain technology briefly are a distributed (decentralized) and common data recording system [29]. This structure provides security, transparency, reliability, and precision for storing data. The transfer between members is done with a smart contract, which is a computerized transaction protocol that fulfills the terms of the contract whose terms have been determined by the contractor [34]. A blockchain is the name given to a chain of consecutive blocks. Each block is linked to the previous and next blocks. The blockchain has recently managed to attract attention. Many researchers from the business and academic backgrounds have begun researching applications that can be developed on this technology [31] [32].

The blockchain can be summarized as a data storage platform that serves as a public ledger. Transaction performed in blockchain technology is written into blocks in a chain. When a new chain is added, this chain grows continuously. The main advantage of the blockchain is its cryptographic security. It is almost impossible to change a block written to the chain. Additionally, a blockchain has features such as decentralization, persistency, and auditability.

The blockchain can operate in a decentralized environment by integrating many key technologies such as cryptographic hash, digital signature (based on asymmetric cryptography), and distributed consensus mechanism. With blockchain technology, a transaction is approved and published in a decentralized manner. For example, money can be transferred between two accounts without any central authority (bank). This decentralized structure, which eliminates central authority, can reduce costs, and increase productivity.

Blockchain can be used for money transfer as well as many other financial applications such as online payment [33] and managing digital assets. In addition, blockchain can also be used in applications such as; smart contract [34], public services [35], Internet of Things (IoT) [36], reputation systems [37] and security services [38].

A. Chain Structure

In the blockchain, all blocks except the first block have a parent. Each block holds the address of the parent block. A representative diagram that shows the mechanism is depicted in Figure 1.



Fig.1. Blockchain Representation

Each block has a hash value, which is calculated by using

the stored data in the block. Therefore, if data in the block is changed, this hash should also be changed. This is used as a validation mechanism for not changing the data in the block. The hash of each block is held by its following block. In this way, a blockchain with a linked list structure is created. In addition to the hash, some values are kept in the block for the operation of the system, and necessary security measures can be taken.

A block consists of two parts: the block header and the block body. The block header contains the following information [39];

- Block version: Specifies which block validation rules to follow.
- The hash of parental block: A 256-bit hash that points to the previous / parent block.
- The hash of the Merkle tree: The hash value of all operations in the block.
- Timestamp: The current timestamp.
- nBits: current hash target in a compact format.
- Nonce: A 4-byte field that usually starts with 0 and shows increments for each hash.

An example image of the information contained in a block header is given in Figure 2.

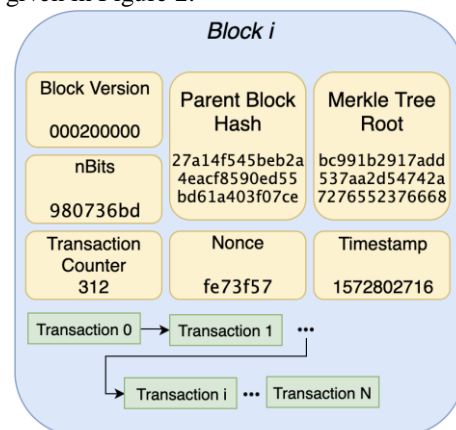


Fig. 2. Block Structure

The block body consists of a transaction counter and transactions. The maximum number of transactions in a block depends on the size of the block and the size of each transaction. The blockchain uses an asymmetric cryptography mechanism to verify transactions [40].

For the blockchain system to work, the entered block data must be validated by all miners (nodes). Consistent reconciliation between all nodes is required. Reconciliation between miners is called Consensus. To establish continuous consensus between many nodes is critical in the highly dynamic blockchain structure. The blocks are prepared and added to the chain, and the consensus is ensured among the miners.

How to reach the Consensus between miners is a trivial problem that must be solved in such a dynamic environment where different miners are constantly being produced and added data to the chain. There is no central node in the blockchain that ensures that the ledger in the distributed nodes is the same. Nodes do not need to trust other ones. Therefore,

some protocols are required to ensure that the ledger on different nodes is consistent. There are many protocols developed in the literature to solve this problem. Two of these are PoW (Proof of Work) [27] and PoS (Proof of Stake) [32]. PoW is the protocol used for Bitcoin Consensus. PoS is an energy-efficient version of PoW. In addition to these protocols, many methods have been developed in the literature to achieve consensus [39].

B. Smart Contract

Smart Contract (SC) is a programmable transaction protocol that fulfills the terms of the contract whose terms are determined by the contractors [34]. A smart contract in a blockchain is a piece of code that can be executed automatically by miners. Smart contracts have been integrated into many blockchain mechanisms, such as the Ethereum [28].

Smart contracts can be defined as a block of programming code containing streams of if-else components. Smart contracts are added to the blockchain like an ordinary block. An SC is a new generation contract type with distributed working mechanism, continuity, and traceability provided by blockchain structure. Smart contracts added to the chain can be operated automatically when the specified conditions are met, or they can also be operated manually.

Smart contracts are prepared / programmed after cryptographic agreements between contractors and signed cryptographically and entered to the blockchain. Loaded smart contracts can interact with other components on the blockchain. This interaction can be the initiation of a transaction or the sending / receiving of information. When contractual situations occur (such as receiving a specific message), smart contracts automatically execute the contract terms defined in it.

For example, a smart contract for a forward transaction can trigger mutual share transfer and payment transactions between contractors if the transaction price of the share reaches a predetermined value. A smart contract for insurance can use the weather information to trigger the corresponding insurance payment to the contractor in case the rain rate falls below (or above) a certain level. A smart contract for a postdated check may trigger the payment to the contractor when the collection date is reached and, if there is not enough balance in the account to be paid, it may trigger the freezing of the smart contract. With the rapid development of blockchain technology, the use of many smart contracted applications in daily life is expected to become widespread.

IV. THE PROPOSED SYSTEM

In this paper, a blockchain-based cyber threat information sharing system is proposed. In this system, anyone, either as an individual or as a security company, can access the blockchain with read-permission. However, information can only be entered into the blockchain by trusted partners. Therefore, different user roles are needed in the proposed system. In order to ensure the distributed functioning of the system, trusted partners must be identified and authorized within the blockchain.

Additionally, some rule-sets should be issued and implemented in order to maintain the continuity of the system. These rule-sets needed to be used for small scale blockchain systems. But over time, there may be a need for new rule-sets to be used for large scale blockchain systems. Therefore, it is for such a system to be able to define rule-set definitions that can be updated over time. Updateable rule-sets allows the system to be scaled more easily.

A partner who is authorized to write to the blockchain can enter cyber threat information into the blockchain. However, the fact that the obtained authorization, which lasts for a lifetime, may cause some problems. For example, a partner can gain permission to write the blockchain. Then after a certain period, this partner may enter incorrect information into the system for various reasons. It is thought that the lifetime use of the given authorizations may create negative effects that prevent the system from functioning properly. Therefore, an authorization mechanism is needed to be designed in an updatable manner. This system should be designed that can be overwritten by a partner who is authorized.

Partners who are registered to the information sharing system in the blockchain mechanism may be non-commercial organizations or institutions with commercial aims. The later may request some money from the clients who want to access this information from the sharing system. It is thought that the existence of a kind of payment mechanism may increase the preferability of the system.

There may be many partners who have write-permission to the system. Some of them may be leading companies in the field or companies that have just started to serve in this field and whose services are still under development. Evaluating these companies which are different in terms of reliability at the same level, can make it difficult to use the provided information efficiently. Therefore, designing a mechanism that demonstrates the reliability and experience levels of firms should facilitate the more efficient use of cyber intelligence data by users.

Only trusted partners can add new blocks in the chain. The number of trusted partners is expected to be much less than the number of users who have reading-permission. It takes some time for all miners to validate the information written to the blockchain. Since the number of users performing a write operation to the chain should be small, it is expected that information added in the chain should be quickly verified. Rapid processing and validation of information are crucial to take immediate preventions against cyber-attacks.

The authorization mechanism and the update of the rule-sets should be made through controlled decisions taken by trusted partners. The proposed platform should also enable other companies to verify the added information. Thus, the accuracy of cyber threat information can be evaluated.

A. Authorizations and User Roles

The system is designed with a User-Based Access Control model. There are be 3 different types of privileges in the system. User profiles can have at least one of these privileges

are “Read”, “Write” and “Vote”.

The data in the blockchain can be readable by all users. This means that all users have the reading privilege. Write authorization is needed to write cyber threat information to the blockchain. Controlled decisions are required within the system in order to continue the operation of the blockchain mechanism. These decisions are built on a voting-based system. Some users who are authorized to write also have the right to vote in the decision-making mechanism. Voting authority is not an authorization granted to all users who have write-authority. This privilege is granted only to users who are trusted partner.

There are 5 different user roles in the system, which are listed as follows;

- *Reader*: Only users who want to read the information in the blockchain are included in this user profile. This user profile is only authorized to read.
- *Standard Partner*: Users who have both read and write privileges in the system are included in this profile.
- *Standard Partner Candidate*: It is the profile of the users who want to become a standard partner during the review stage. Users with this profile do not have write-privileges on the main chain but have write-authorizations on the test chain. This write authorization obtained on the test chain expires after a certain period.
- *Trusted Partner*: Users who have access to the system with read, write, and vote-privileges are included in this profile.
- *Founder Partner*: Trusted Partners who are responsible for carrying out initialization operations for the system to start are included in this profile.

A user can first access the system in the Reader profile except for Founder Partners. If the user fulfills the necessary conditions, he can obtain other privileges and switch to other profiles. Similarly, a user can be downgraded from the Standard Partner profile to the Reader profile with Controlled Decision-Making Mechanism (CDMM). Operations such as user authorization are carried out with a controlled decision mechanism in the system. CDMM can be implemented within the framework of certain rules. The rules for operation are defined in the rule-sets.

B. Initialization

A user must collect a number of votes, in order to be authorized within a CDMM. Many trusted partners are needed for voting. Since the system doesn't have any trusted partner defined in the system at the beginning time, it was necessary to design an initial state for the system to start working.

Initially, there are N trusted partners who must come together to undertake the initialization steps necessary for the system to operate in the initial state. These partners are included in the Founding Partner profile in the system. Founder Partners should add a pair of SCs to the chain, just like any other user to be defined in the system. 3 different types of SCs are used for the operation of the system. These are;

- Positive Vote Contact (PVC)

- Negative Vote Contract (NVC)
- Control Contract (CC)

CC verifies that the requirements for the decision-making mechanism are met. PVC and NVC are used for counting votes whose mechanism is detailed in the ongoing parts.

In the initial state, all the founding partners are needed to vote by running the PVC of all other founding partners except himself. In this way, each founding partner should have N-1 positive votes. The initial state in which the founding partners voted each other is represented in Figure 3.

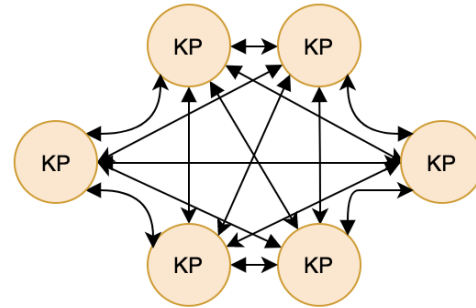


Fig.3. Initial Situation in which Founding Partners Vote for Each Other

The founding partners add the first CC to the blockchain to get the system up and running.

The first CC added to the system is called the Master Control Contract (MCC). The MCC maintains the addresses of other control contracts. The founding partners add only one MCC to the system. Each founding partner then creates its own CC and adds it under to the MCC.

CCs are designed as a tree structure. Each CC is derived from another CC. The first control contract defined in the system is the MCC. Each founding partner then adds its own CC to the system under the MCC. When the initial state is completed, the system has one MCC and one control contract as much as the number of founding partners. The tree structure of the control contract is given in Figure 4.

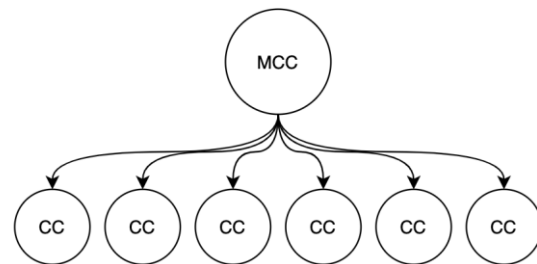


Fig. 4. Tree Structure of Control Contracts

After the initial state, the user authorization steps with the Controlled Decision-Making Mechanism (CDMM) are executed for the users who want to have authority in the system.

Each CC verifies that the requirements for the authorization mechanism are met. Each CC holds the addresses of the users it authorizes and the addresses of the other CC under it. It is much more difficult to de-authorize users who have a founding partner profile. The parameters used for the termination of authorization for the founding partners shall be

separate from those used for other users. These parameters are also defined in the rule-sets.

C. Controlled Decision-Making Mechanism (CCDM)

After the blockchain mechanism started to operate, some decisions are needed to be taken by the community. This decision-making mechanism plays important roles in the operation of the system, such as user authorization and the determination of new rule-sets. CDMM works according to some hyperparameters defined in the rule-set. Some of these parameters are;

- Enough positive votes to increase the authority
- Enough negative votes for termination of authorization
- Time to continue voting (e.g., 1 week, 1 month)

In this study, the decision-making mechanism is designed as a voting-based system. A decision process that receives enough votes within the community is approved and processed in the blockchain. Deciding that enough votes are obtained is made according to the values defined in the rule-set. For example, if enough votes are defined as 50% in the rule-set to increase user authorization, 50% of the trusted partners must vote as positive to increase the authority of the user. A decision that fails to obtain enough negative votes is rejected and cannot be active in the system. Voting is not an activity that can be performed by all users. Only users with Trusted Partners can vote on the system. For the voting system to work successfully, it is assumed that the trusted partners do not vote for bad or harmful purposes but perform fair voting only in legal cases. In order to meet these requirements, the selection of trusted partners must be selective. Voting is carried out with SCs (PVC, NVC) in the controlled decision mechanism designed, as mentioned before.

D. Voting

To keep the SC structure simple, PVC and NVC must be added to the system in the system for voting. This is shown in Figure 5. These two SCs are identical in structure. However, the intended use is different. One of the SCs is used to count positive votes, while the other is used to count negative votes. These two contracts are connected to each other. One voting contract shall hold the address of the other one.

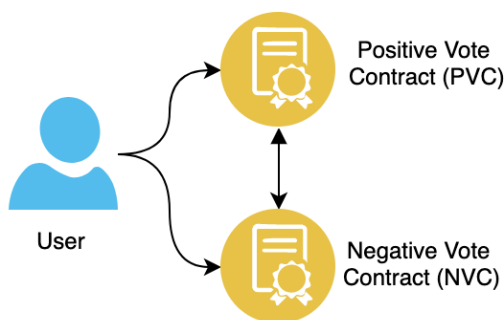


Fig.5. Voting Contracts Added to the System

Vote Contracts basically keep the number of votes and the people who vote. Therefore, a counter is held in the application code. Each time the SC is executed, this counter value is increased by 1, and the address of the trusted partner

running the SC is stored in the block. Each of the trusted partners who have the authority to vote cannot vote more than one vote for a decision. However, votes can be changed. The pseudocode for the voting process is shown in Algorithm 1.

Algorithm 1: Voting Algorithm

```

IF SC is run AND the user is not in the users' list
THEN
  counter += 1
  save user address in the block
ENDIF
  
```

Voting for a user who has not previously vote positive or negative for an SC is executed by the Voting Algorithm. The given algorithm is used for both positive and negative votes. The registered user lists for positive and negative users are different.

A trusted partner who votes positive for a standard partner candidate may want to change its mind over time and turn its vote to negative. In this case, the trusted partner who wants to change the vote is just executed NVC. With this process, the address of the trusted partner who changed the process is deleted from the PVC and written to NVC. As a result, the number of positive votes decreases by 1, while the number of negative votes increases by 1 as shown in Algorithm 2.

Algorithm 2: Vote Change Algorithm

```

IF one tries to change the vote THEN
  Delete user address from the current list
  Decrease previous vote count by one
  Save user address to new vote list
  Increase vote counter
ENDIF
  
```

In this way, it can be ensured that the positive votes given are non-lifetime and can be changed over time. It is also possible to reverse this process, that is, to turn a negative vote into a positive vote. The information contained in the SCs to be used is kept in 3 different parts: header, code, and memory.

The header section includes the following parts;

- SC Address
- Previous SC Address (if applicable)
- Rule-set Version Number
- Peer Voting Contract Address (NVC address for PVC / PVC address for NVC)
- Timestamp

Certain definition of rules is needed in order to carry out the CDMM. The rules consist of preliminary information to be used in the mechanism of the system, such as determining the number of votes enough for the decision to be taken. Rules are defined in rule-sets, and all SCs must comply with the rules in the rule-set. The number of votes defined in the rule-set must be provided in the PVC in order to complete the decision-making mechanism. Otherwise, the decision should be rejected.

E. User Authorization with CDMM

A standard partner candidate must receive enough votes from trusted partners in the system according to the values

defined in the rule-set. The standard partner candidate must contact the trusted partners and ask them to review and vote on them. The first trusted partner to which the user applies to examine raises this user to the standard partner candidate profile, as depicted in Algorithm 3.

Algorithm 3: Authorization Algorithm

```

The user completes the requirements.
The user applies to trusted partners for voting.
Trusted partners examine the user.
IF suitable for a positive vote THEN
  The trusted partner runs the candidate's PVC.
ELSE
  The trusted partner does not vote or give
  negative vote using NVC.
ENDIF

```

Trusted partners require some information from the user to review the applicant. The user is then upgraded to the standard partner candidate level, allowing the user to write to the test chain, which is a small copy of the main blockchain. The candidate user is asked to enter the sample data of cyber threat intelligence information to this test chain. When the candidate user enters the sample data into the test chain, the examination process begins.

Trusted partners examine the standard partner candidate to be voted in terms of the information they provide and the cyber threat intelligence they enter in the test chain. Then, it is concluded whether the candidate user can provide reliable cyber threat intelligence information. The trusted partner who completes the review phase executes the PVC or NVC added by the candidate user to the system. If the user meets the requirements, the trusted partner will run one of these vote contracts of the user. Visual representation of user authorization and inclusion in the system are given in Figure 6.

Several cases are analyzed that will have a detrimental effect on the SC code or the unfair treatment of the number of votes when examining VCs. If the VCs code is designed in accordance with standards, the trusted partner will run the partner candidate's PVC once. Since the analysis and SC execution are transactions for a certain fee, the partner candidate will have to pay a certain application fee when he / she applies to the trusted partners in order to get votes.

It is not obligatory to vote after the examination phase. It is also possible that a user who does not have the qualification to vote positively is not allowed to vote at all. For a candidate to become a standard partner or a standard partner to become a trusted partner, he must receive enough votes and meet certain requirements. The necessary conditions will be defined in the rule-sets.

The conditions are first checked by the user's PVC. As soon as the PVC determines that the conditions are met, it applies to any Control Contract. If the Control Contract gives approval after performing the necessary checks, the user is raised to an upper profile. Similarly, the conditions for termination of authorization are controlled by NVC.

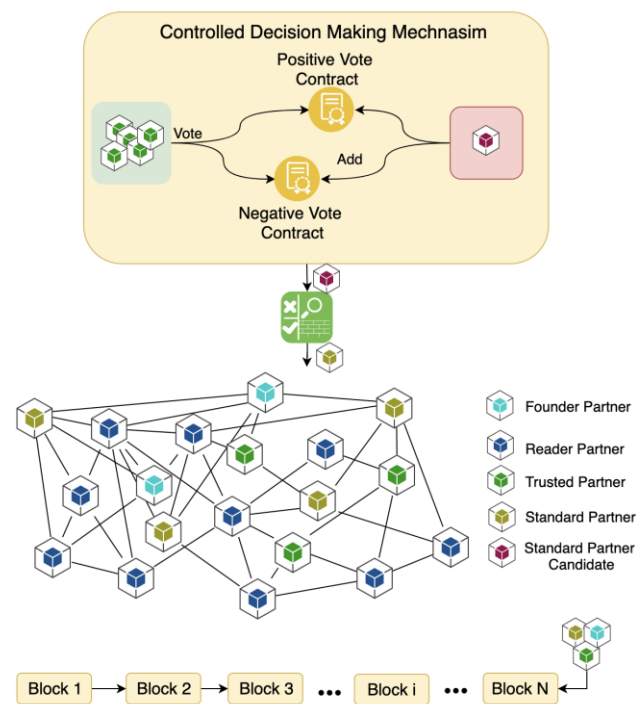


Fig 6. User Authorization with CDMM

In the Standard Partner profile, a user can enter the correct cyber threat information into the system for a while and start to enter incorrect information after a certain period or may exhibit behaviors that may adversely affect system operation. When such situations are encountered, it is necessary to de-authorize the relevant partner. This process is called authorization termination. In the case of a user whose authorization is to be terminated, trusted partners vote for this user's NVC. The profile of the user who has received enough negative votes according to the rules defined in the rule-set is reduced to a lower profile. With this method, a trusted partner level can also be reduced to the standard partner level.

In this case, the CC is applied. After checking with the Control Contract, which checks the necessary conditions for the termination of authorization, the profile of the partner concerned is reduced to a lower level, as depicted in Algorithm 4.

Algorithm 4: Termination of Authorization

```

Trusted partners vote negative for a user if they
consider it necessary

```

```

IF requirements are met THEN
  The user's privileges are dropped

```

```

ENDIF

```

The parameters required for the termination of authorization are defined in the rule-set. CCs are SCs that are added to the system by trusted partners. These contracts are derived from the tree structure. CCs ensure that the requirements for authorization have been met. Authorization and termination of authorization are carried out by CC. Each of the trusted partners is responsible for adding one CC to the system. Each CC is established as a node under the CC to which the trusted

partner is authorized. In this way, the tree structure of the CCs is preserved. A user who wishes to increase his authorization may apply to any CC. Each CC maintains the addresses of the users it authorizes and the addresses of the other CCs under it.

The structure of the CC is standard. The first CC is entered into the system by the Founder Partners. All CCs added to the system are copies of the contracts added by the founding partners to the system. It is important that each trusted partner adds a CC to the system so that the authentication verification step can be performed in a distributed architecture. In this way, even if some of the CCs have been damaged for various reasons, the system continues to operate smoothly.

Since the authorization and termination of the authorization are important steps, it is considered that an extra verification mechanism and CCs will contribute to the sustainability of the system. CCs also play an important role in updating rule-sets.

A separate blockchain will be used to examine the information that the standard partner candidate will enter the system. This chain is called the Test Chain. A standard partner candidate cannot enter data into the main chain until it is included in the standard partner profile; only data can be entered the test chain. The test chain can only be read by trusted partners. The authority to write data to the test chain is also defined for a certain period. The time definition is defined in the rule-sets. These steps are shown in Figure 7.

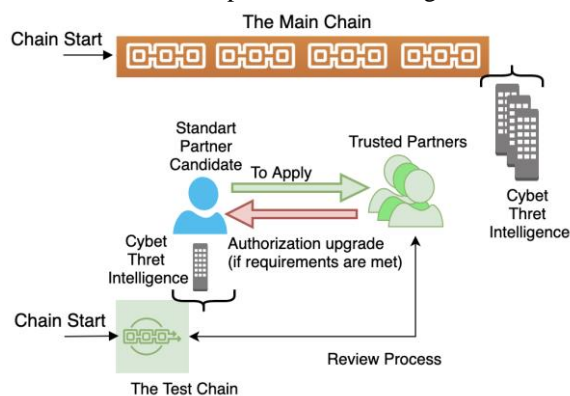


Fig 7. Standard Partner Candidate Review Steps

With the authorization termination process, the privileges granted to the users are not available for the lifetime. A user who has write-privileges in the system can be disqualified if he does not enter useful information as promised in the system. In this way, problems that may occur in the system are minimized.

F. Rule Sets

Some rules should be defined in CDMM and at other points. For example, the number of votes required for decision-making in a CDMM is one of these rules. The rules to be determined must meet the system requirements. Some of the rules that can be included in the rule-set are as follows;

- Percentage of positive votes required to become a trusted partner (positive vote count/ all trusted partner count)
- Percentage of negative votes required to authorize a trusted partner (negative vote count/ all trusted partner

count)

- Percentage of negative votes required to authorize a standard partner (negative vote count/ all trusted partner count)
- Enough percentage of votes to update rule-set (positive vote count/ all trusted partner count)
- The default value for voting time

Since the defined rule-sets can be updated over time, the version information of the rule-set must be kept in each partner's Vote Contracts. If the rule-set version is changed, users are informed that the new rule-set has been changed.

G. Updating Rule Set with CDMM

The update of the rule-sets can be tracked by version numbers. Vote Contracts operate according to the rules in the currently defined and accepted rule-set. All SCs of all partners in the system must be renewed, and the version number of the new rule-set must be entered in these SCs, in order to update the rule-set. When renewing SCs, the address of the previous SC is entered into new contracts. This creates a link between SCs.

Each of the trusted partners in the system can propose a new set of rules. The trusted partner who makes the rule-set suggestion should add the system with the candidate rule-set on a pair of Vote Contracts. The steps in CCMM are performed using VCs entered into the system with the new suggested rule-set.

The rule-set that succeeds in getting the required number of votes to update can now be used in the system.

Announcing Updated Rule-set

Notifying users of the rule-set update and triggering the renewal of the required VCs is a crucial step in the functioning of the system.

It is first checked by the VCs associated with the rule-set to see if the requirements for updating the rule-set are met. If the necessary conditions are met, PVC applies to the Master CC. Once a CC confirms that the necessary requirements have been met, it reports the situation to the Master CC. The main CC is announced to the CCs under it. Each CC that receives the relevant announcement transmits the information to the VCs and CCs under it.

CCs are in a tree structure. Each CC is derived from a CC. The first CC defined in the system is the master CC. In case there are many users in the system, the tree structure of the CCs is given in Figure 8.

After the announcement, a new VC pair is created on the system for each user, even if their memory space is not full. The system operation is continued by entering the address of the previous SC, and the new rule-set version to the new SC created.

Users who do not renew their VC is downgraded from the standard partner or trusted partner profile to the Reader profile until they renew their contracts.

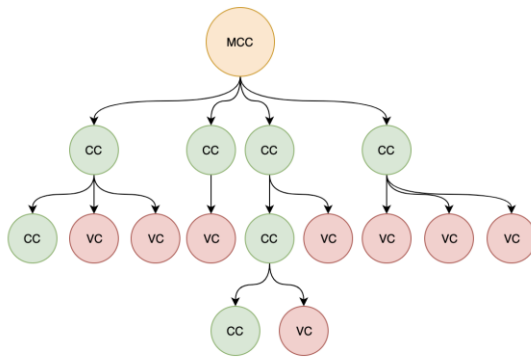


Fig 8. Tree Structure of Control Contracts

The ability to update the set of rules is very important to make it easier to scale the system over time and is a very costly process. Because of the cost, it is expected that rule-set updates are not operated very often, but only when necessary at a critical level.

V. ANALYSIS OF THE SYSTEM

In this study, a blockchain-based approach to cybersecurity information sharing is proposed. A decentralized decision-making mechanism is needed to ensure the distributed functioning of the system. The CDMM is also proposed to make decisions within the system. This mechanism is executed with a voting-based approach. A standard partner candidate can be promoted to the standard partner profile; he must collect enough votes. An initial situation is designed where there are no users with voting rights in the startup phase. In the first case there are N founding partners. Founding partners also have trusted partner privileges. The founding partners are also responsible for performing a few operations of the system. These operations are;

- Each founding partner votes for the other founding partners. In this way, each founding partner should have $n-1$ votes.
- The founding partners create and add a set of rules to be executed for the initial state.
- Founding Partners add one master CC to the system.
- Each founding partner adds its own CC under the main CC.
- Some of the initialized parameters in the rule-set created by the founding partners are as follows;
 - Percentage of positive votes to be obtained from trusted partners to become standard partners.
 - Percentage of positive votes required to become a trusted partner
 - Percentage of negative votes required to authorize a trusted partner
 - Percentage of negative votes required to authorize a standard partner
 - Enough percentage to update rule-set
 - The default value for voting time

When the system initialization phase is completed, the founding partners start to enter cyber threat intelligence

information in the chain. Anyone can read this information and can now add standard partner users to the system.

CDMM is carried out in order to decide to increase authority. The candidate user adds a pair of VCs to the system to become a standard partner. One of the voting contracts holds positive votes, while the other one is used to count negative votes. The candidate user applies to the trusted partner level users in the system after the VC added to the system. At the time of application, a few documents are submitted to trusted partners. The documents contain information about the user as well as information about the cyber threat information obtained. In addition, the candidate user transmits a few documents on how he obtains cyber threat information data to the trusted partners during the application.

The first of the trusted partners applied to gives this candidate the authority to write to the test chain. The candidate user is then expected to enter some cyber information data into this test chain. After the candidate enters data in the test chain, the trusted partners applied for review the data entered by the candidate user in the test chain and the documents submitted by the candidate to the trusted partners during the application. Trusted partners who decide that the entered cyber threat information data are useful and consistent, run the Positive Vote Contract (PVC) of the relevant candidate, and vote positive. Trusted partners who do not feel that the candidate is qualified to vote positively may not vote at all or vote negative.

The candidate user who succeeds in obtaining the number of votes defined in the rule-set from the trusted partners currently present in the system is upgraded to the standard partner level. If the percentage of votes required to become a standard partner in the rule-set is 50% and the number of currently trusted partners is 10, the candidate user must receive at least 5 positive votes. First, the voting contracts of the candidate are checked whether the necessary conditions are met. The candidate user who meets the requirements defined in the rule-set to become a standard partner applies to any CC in the system. If the CC confirms that the necessary conditions are met, the candidate user is promoted to the standard user authorization, and the address of the user's VCs is added to the CC that authorizes the user.

Similarly, if the trusted partner meets the conditions set in the rule-set, he / she rises to the trusted partner level. The required conditions are first checked by the voting partner of the trusted partner candidate. The voting contract applies to any CC for the authorization upgrade when the necessary conditions are met. If the CC confirms that the necessary requirements are met, the trusted partner candidate is raised to the trusted partner level. The user who reaches the trusted partner level creates a CC. The created CC is added to the CC, which authorized from.

With this approach, CC has a tree structure. The top node is the master CC that the founding partners add to the system. At the first level, there are CCs entered by the founding partners. Two types of data can be found in CC.

These are;

- Address of the voted partners of the authorized standard

partners

- Address of the CC of authorized partners

The tree structure of the CCs grows over time by branching, as in Figure 8.

These steps are repeated for each standard partner and trusted partner. Over time, many standard partners and trusted partner-level users are created in the system.

The list of trusted partners running VCs is saved into the VCs memory area. VCs are entities with limited memory space. Storing a number of addresses results in high memory usage in VCs. If the SC becomes out of memory space so that the contracts do not function due to the memory space being filled, a new VC is created, and the address of the previous VC is entered into the new VC. For example, when there is no space in the memory area of the PVC for a decision, a new PVC is automatically added to the system. The address of the previous PVC is entered into the newly created PVC. This makes it easier to scale the system. Adding the new VC to the system and entering the old VC address into the new VC is coded / defined into the code area of VC. That is to say, the processes required to fill the memory space and the entry of new contracts into the system are performed automatically when the appropriate conditions are met.

The requirements of the system may change over time, or some additions may be needed to make the system more secure. The requirements for operating a system with 100 partners may differ from those required for a system with 1,000,000 partners.

For example, If there are 100 trusted partners in the system and the percentage of enough votes is decided as 50%, At least 50 trusted partners' votes are needed to increase the authority. However, in the system with 1,000,000 trusted partners, if the percentage of enough votes is 50%, 500,000 trusted partners must vote. When the system is getting growth, decreasing the percentage value of enough votes can increase the sustainability of the system. In order to overcome this, the rulesets are designed to be updated timely.

Updating the rule-set can be done by assigning new values to existing rules or adding new rules to the rule-set. In this way, it can easily adapt to changing conditions. The rule-set is updatable; It is an important step in terms of scalability of the system and adaptation of the system to changing conditions.

Any trusted partner can make suggestions for updating the rule-set. For the update process, the steps of the control decision-making mechanism proposed in this study are carried out. The trusted partner who suggests adds the proposed set of rules and a pair of VCs to the system. Then, they announce their proposal to all trusted partners. Trusted partners review and vote for a new set of rules. The rule-set, which receives enough votes defined in the rule-set, can be used in the system in this step. Proposing a new set of rules can be considered as a collective decision rather than an individual activity. A community of trusted partners can decide on the rules in the proposed rule-set, as a result of extensive analysis, the rules can be proposed, as well as through the surveys carried out among trusted partners, and update recommendations can be

suggested.

After it is decided to update the rule-set, all SCs in the system must operate according to the rules in the new rule-set. Therefore, the update of the rule-set should be announced to SCs. The announcement of rule-sets is an important step for system operation. The announcements for the rule-set update is made by the CCs. Since the authorization process is carried out through CC, each partner must add a CC to the blockchain. The standard partner level users' voting contract address, and the trusted partner level user CC address is kept in the CC. This allows CCs to dominate a tree structure, as given in Figure 8. If enough votes for the rule-set update are collected, the situation is announced to the MCC. The MCC informs the CCs under it. Each CC shall inform the VCs and other CCs under it. Whenever it communicates to all assets under each CC, the system is informed of the use of the new set of rules in all VCs.

The new rule-set can be very different from the previous rule-set. Therefore, when the rule-set is updated, the current status of the VCs may not meet the requirements for the operation of the rules in the new rule-set. In order to avoid this situation, VCs are updated in every rule-set update. A new SC is created for each SC, and the address of the current rule-set and the addresses of the previous SC have entered the new SC. With the completion of all these processes, the updated set of rules becomes active.

Operations such as the execution of VCs and the creation of new SCs are transactions with a certain cost. These costs need to be covered in some way. Otherwise, operations cannot be performed. Due to the nature of the system, the costs of running SCs are collected from the person who runs the contract. VCs must be run many times for voting.

Standard partner candidates need votes to increase their authority. They must also apply to trusted partners for voting purposes. The standard partner candidate pays a certain fee to the trusted partner to whom he applies. The trusted partner reviews the standard partner candidate for this fee and, if deemed necessary, runs the candidate's SC. Although the cost of the SC that is run for the standard partner candidate to collect votes is paid by the trusted partner, who votes, this cost is covered by the standard partner candidate.

SCs may need to be renewed because the memory space is full. In this case, a new SC is created and associated with the old SC. By creating a new SC, the costs associated with the old SC are covered by the SC owner. For example, user A's positive PVC has been filled, and a new PVC has been created. In this case, the necessary fee is covered by person A.

Updating the rule-set is a process to improve system operation. The improvement achieved by updating the rule-set applies to all users in the system. Therefore, in order to update the rule-set, the full cost of the transactions is not charged to the trusted partner who proposes to update the rule-set. All users who vote for the new set of rules must pay for their own votes.

When the reader users want to read cyber threat information data from the system, they can make company-based queries or data-based queries. For example, user A can filter all cyber

threat information entered the system by company C, as well as all cyber threat information entered for the IP address x.x.x.x. In addition, statistical information such as which partner enters the blockchain can be displayed in the system.

VI. DISCUSSION AND CONCLUSION

In order to protect the systems against new cyber-attacks, their signatures (information) should be reached as early as possible. This information can be accessed either when it is encountered in the system, or when this information is gotten from other signature servers, which share their knowledgebase to others. The latter one is preferred by the security admins, and they can contact others either in peer to peer model, or in a client server manner. Both these approaches have some negative effects, especially in maintenance.

Therefore, in this paper, a blockchain based cyber threat information sharing system is proposed. The use of blockchain technology enables cryptographic security and distributed structure for us, which are two trivial issues that are needed to be solved for the scalability of the system. The design details are detailed by showing the structure of block/data adding mechanisms with the use of a Voting mechanism and Smart Contracts.

The blockchain mechanism is set up by partners as companies, government agencies, or computer security firms. The dynamic addition of partners/users is also enabled. A candidate user must collect some votes for the authorization upgrade. The candidate user applies to trusted partners to collect votes. Trusted partners may vote positively or negatively if they deem necessary after reviewing the candidate user. The authority of the candidate user who receives enough votes is increased. Adequate votes are defined in the rule-sets. Rule-sets can be updated so that the system can adapt to changing conditions. CCs are used to validate the authorization process and to announce the update of the rule-set.

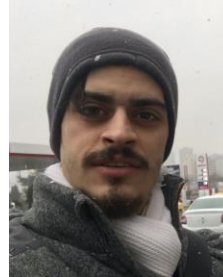
The proposed system is in the design phase. In the ongoing studies, the design of the system is aimed to be implemented. Additionally, the payment system is very important for the preferability of this system. It is thought that commercial firms may want to use a common platform where they can sell their products. It is planned to make improvements to the proposed system to increase preferability and sustainability. In addition, it is planned to conduct research to extract the experience and reliability levels among the trusted partners in the following studies. In this way, the reliability of the shared information can be accepted as a measurable metric.

REFERENCES

- [1] Ninth Annual Cost Of Cybercrime Study, THE COST OF CYBERCRIME, <https://www.accenture.com/acnmedia/pdf-6/accenture-2019-cost-of-cybercrime-study-final.pdf>, The Last Access: May 2020
- [2] G. Karatas, O. Demir and O. K. Sahingoz, "A Deep Learning Based Intrusion Detection System on GPUs," 2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 2019, pp. 1-6, doi: 10.1109/ECAI46879.2019.9042132.
- [3] B. Reis, S. B. Kaya, O. K. Sahingoz, "A Clustering Approach for Intrusion Detection with Big Data Processing on Parallel Computing Platform", Balkan Journal of Electrical and Computer Engineering Volume 7 , Issue 3, Pages 286 - 293, 2019
- [4] B. Reis, S. B. Kaya, G. Karatas and O. K. Sahingoz, "Intrusion Detection Systems with GPU-Accelerated Deep Neural Networks and Effect of the Depth," 2018 6th International Conference on Control Engineering & Information Technology (CEIT), Istanbul, Turkey, 2018, pp. 1-8, doi: 10.1109/CEIT.2018.8751784.
- [5] PhishTank | Join the fight against phishing, <https://www.phishtank.com/>, The Last Access: May 2020
- [6] IBM X-Force Exchange, <https://exchange.xforce.ibmcloud.com/>, The Last Access: May 2020
- [7] AutoFocus Threat Intelligence, <https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/autofocus>, The Last Access: May 2020
- [8] LogRhythm Threat Lifecycle Management (TLM) Platform, <https://logrhythm.com/products/threat-lifecycle-management-platform/>, The Last Access: May 2020
- [9] iSIGHT Intelligence Subscriptions, <https://www.fireeye.com/products/isight-cyber-threat-intelligence-subscriptions.html>, The Last Access: May 2020
- [10] LookingGlass Cyber Solutions, <https://www.lookingglasscyber.com/>, The Last Access: May 2020
- [11] Normshield Free Cyber Threat Intelligence, <https://services.normshield.com/honeypotfeed>, The Last Access: June 2020
- [12] FireHOL IP Lists | IP Blacklists | IP Blocklists | IP Reputation, <http://iplists.firehol.org/>, The Last Access: October 2019
- [13] R. Koch, & M. Golling, (2018, May). The cyber decade: cyber defence at a x-ing point. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 159-186). IEEE.
- [14] T. R. Vance, & A. Vance (2019, October). Cybersecurity in the Blockchain Era: A Survey on Examining Critical Infrastructure Protection with Blockchain-Based Technology. In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T) (pp. 107-112). IEEE.
- [15] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, & K. K. R. Choo, (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks.
- [16] I. Makhdoom, I. Zhou, M. Abolhasan, J. Lipman, & W. Ni, (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. Computers & Security, 88, 101653.
- [17] Meng, W., Tischhauser, E. W., Wang, Q., Wang, Y., & Han, J. (2018). When intrusion detection meets blockchain technology: a review. Ieee Access, 6, 10179-10188.
- [18] R. Graf, & R. King, (2018, May). Neural network and blockchain based technique for cyber threat intelligence and situational awareness. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 409-426). IEEE.
- [19] D. Homan, I. Shiel, & C. Thorpe (2019, June). A New Network Model for Cyber Threat Intelligence Sharing using Blockchain Technology. In 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-6). IEEE.
- [20] Y. Wu, Y. Qiao, Y. Ye, & B. Lee (2019, October). 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) (pp. 474-481). IEEE.

- [21] C. Killer, B. Rodrigues, & B. Stiller, (2019, May). Security Management and Visualization in a Blockchain-based Collaborative Defense. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 108-111). IEEE.
- [22] Cybersecurity Tech Basics: Blockchain Technology Cyber Risks and Issues: Overview, <https://www.stepoe.com/images/content/1/8/v2/189187/Cybersecurity-Tech-Basics-Blockchain-Technology-Cyber-Risks-and.pdf>, The Last Access: June 2020
- [23] Feng, S., Xiong, Z., Niyato, D., Wang, P., Wang, S. S., & Zhang, Y. (2018, December). Cyber Risk Management with Risk Aware Cyber-Insurance in Blockchain Networks. In 2018 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE.
- [24] G. Ahmadi-Assalemi, H. M. Al-Khateeb, G. Epiphaniou, J. Cosson, H. Jahankhani, & P. Pillai (2019, January). Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3) (pp. 1-9). IEEE.
- [25] R. Yetis and O. K. Sahingoz, "Blockchain Based Secure Communication for IoT Devices in Smart Cities," 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2019, pp. 134-138, doi: 10.1109/SGCF.2019.8782285.
- [26] G. Dinc and O. K. Sahingoz, "Smart Home Security with the use of WSNs on Future Intelligent Cities," 2019 7th International Istanbul Smart Grids and Cities Congress and Fair (ICSG), Istanbul, Turkey, 2019, pp. 164-168, doi: 10.1109/SGCF.2019.8782396.
- [27] S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system.", 2008.
- [28] G. Wood. "Ethereum: A secure decentralized generalized transaction ledger.", Ethereum Project Yellow Paper, 2014.
- [29] G. Foroglou, A. L. Tsilidou, "Further applications of the blockchain.", In 12th Student Conference on Managerial Science and Technology, 2015.
- [30] S. Sayeed, H. Marco-Gisbert and T. Caira, "Smart Contract: Attacks and Protections," in IEEE Access, vol. 8, pp. 24416-24427, 2020, doi: 10.1109/ACCESS.2020.2970495.
- [31] K. Lee, J. I. James, T. G. Ejeta, H. J. Kim, "Electronic voting service using block-chain.", The Journal of Digital Forensics, Security and Law: JDFSL, 11(2), 123, 2016
- [32] Z. Zheng, S. Xie, H. N. Dai, H. Wang, "Blockchain challenges and opportunities: A survey.", International Journal of Web and Grid Services, 14(4), 352-375, 2018
- [33] R. Adams, G. Parry, P. Godsiff, P. Ward. The future of money and further applications of the blockchain. Strategic Change. 2017; 26: 417– 422. <https://doi.org/10.1002/jsc.2141>.
- [34] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts.", In Proceedings of IEEE Symposium on Security and Privacy (SP), pages 839–858, San Jose, CA, USA, 2016.
- [35] B. W. Akins, J. L. Chapman, J. M. Gordon, "A whole new world: Income tax considerations of the bitcoin economy.", 2013.
- [36] Y. Zhang, J. Wen, "An IOT electric business model based on the protocol of bitcoin.", In Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), pages 184–191, Paris, France, 2015.
- [37] M. Sharples, J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward.", In Proceedings of 11th European Conference on Technology Enhanced Learning (EC-TEL 2015), pages 490–496, Lyon, France, 2015.
- [38] C. Noyes, "Bitav: Fast anti-malware by distributed blockchain consensus and feedforward scanning.", arXiv preprint arXiv:1601.01405, 2016.
- [39] Z. Zheng, S. Xie, H. N. Dai, H. Wang, "Blockchain challenges and opportunities: A survey. Work Pap", 2016.
- [40] NRI, "Survey on blockchain technologies and related services. Technical report", 2015.

BIOGRAPHIES



EBUBEKIR BUBER He received the B.S. and M.S. degrees in Computer Engineering from Yildiz Technical University, Istanbul, Turkey. He is currently a student of Ph.D. at Yildiz Technical University since 2019. His research interest are cybersecurity focused artificial intelligence applications and cybersecurity related blockchain systems.



OZGUR KORAY SAHINGOZ received the B.S. degree from the Computer Engineering Department, Boğaziçi University, in 1993, and the M.S. and Ph.D. degrees from the Computer Engineering Department, Istanbul Technical University, in 1998 and 2006, respectively.

He is currently working as an Associate Professor with the Computer Engineering Department, Istanbul Kültür University. He is the author of more than 100 articles. He has been working in two research projects. He graduated more than 13 M.Sc. students and supervised around six Ph.D. students. He has reviewed more than 80 national projects especially related to TUBITAK, KOSGEB-Ministry of Industry and Technology, Turkey. He is also a regular Reviewer for more than 40 Science Citation Index (/Expanded) international journals. His research interests include artificial intelligence, machine/deep learning, data science, software engineering, and UAV networking. Dr. Sahingoz has also been very active in scientific conferences, organized and/or works as program committee members more than 100 conferences/workshops on different research areas, especially on artificial intelligence and information sciences. He has developed and taught around 20 different academic courses.