SYSTEMS THINKING FOR THE TRANSITION OF EXISTING TECHNOLOGIES TO BLOCKCHAIN TECHNOLOGIES.

Author(s) / Auteur(s) :

PhD Candidate Nikolaos ZOANNOS
University of Piraeus, Hellenic Society for Systemic Studies (HSSS)
nmzoanno@gmail.com

Professor Nikitas ASSIMAKOPOULOS
University of Piraeus, Hellenic Society for Systemic Studies (HSSS)
assinik@unipi.gr

Abstract / Résumé :

The 4th Industrial evolution has brought along a lot of technological achievements which can change the form of humanity. Peer-to-peer networks (Distributed networks), network of sensors (Internet of Things), algorithms capable to take decisions (Artificial Intelligence), computers with the ability of self-learning (Machine Learning), more complex queries for analyzing the data, that we are collecting since the birth of internet (Data Science) and new electronic money(cryptocurrencies) are some of the characteristics of those new technologies. But the adoption of those achievements (known as Digital Transformation or Digitization) demands Managers open-minded, well-educated on those technologies and ready to trace the new possible Risks. They must also be capable to use the Systems Thinking, as the Blockchain Technologies have created an Ecosystem (Sociotechnical Systems); the combination of Social Systems (Organizations - Companies), whose behavior is not predictable, and Mechanical Systems (technical equipment) with a predefined way of function. So, this kind of Systems (Sociotechnical) need a more delicate approach using a combination of, not only Systemic methodologies and technics, but also other theories and proper tools. We are going to publish a series of articles in which we are going to specify the proper theories and methodologies in each phase of the digital transformation. Thus, the purpose of this study is to explain to the new generation of Managers how the Systems Thinking, DCSYM Methodology and VSM Model, are applied on those Ecosystems.

Keywords / Mots-clés :

Blockchain Technolgies, Decentralized Architecture, Distribuded Ledger, Internet of Things, Ecosystem, Sociotechnical Systems, Digital Transformation, Systemic Management, Business Intelligence,DCSYM Methodology,VSM model.

INTRODUCTION

In order to explain as detailed as possible the meaning of the word “Blockchain”, how it was born and the purpose of those technologies, we must firstly explain the exponential growth of the users’ need for disindermediation. In that way we are going to focus on Supply Chain (SC).

Up until today, each time a user wanted to buy or sell a product/good or service he had to use a trusted intermediate organization, like Banks. This way, the transaction was secured and at the same time we knew that the seller had to send the product and that the buyer was going to receive this product. Also, a trusted third party, like Security Insurance companies, could be used in order to secure the product and for the buyer to rest assured. This contract, was going to be enabled only in if the product wouldn’t reach the receiver, on a predefined period of time or if the product was destroyed. In each case, a moajor increase in the final cost of the product was apparent and in some cases the cost of the intermediate organizations was higher than the actual cost of the product. This situation has led to the need for disintermediation.

During the past few years, it has been noticed that although many products were deliverd to receivers, either they were not as they were described (it consisted products of fraud) or they were destroyed, broken, wet and/or unboxed at transportation. Those facts created two (2) differnet needs: (1) the need of a contract between the receiver and the dispatcher (two entities with lack of trust on each other) and (2) the need of tracking and tracing the state of the product while it is being transported (for the assignment of responsibilities).

This contract is called "**smart contract**" (*Ameer Rosic,2016*) and is a piece of code which is written in Solidity programming language and contains with detail all the rules and policies called "**events**" and "**functions**" (*Daniel Drecher,2017*) that should be enabled if something goes wrong (for example if the product has been destroyed, broken, wet, unboxed or if it has been exposed to radiotion / chemicals or even if it has not been maintened on a specific temprature) in order to ensure its quality.

Sensors for humidity, temprature, light exposure, pressure, toxical exposure and others can be used in order to trace the exact circumstances under which a product was damaged. Also, those sensors are going to trigger alarms on the smart contract using 5G Networks in order to enable specific "function" or/and "events" and the contract will automatically decide whether the transportation should be continued or if it should be postponed, and so the product would return to the sender. The fact that an alarm has been triggered on a specific "**timestamp**" creates a record on the network with the exact time: year-month-day-hour-minute-second (*Wikipedia, 2019*) and it can be used to document the responsibility of a freight forwarder or/and a shipping carrier.

Another need, which pusses users to use those new technologies, is to ensure the ownership of their assets. For example, when someone want to sell his house, according to the law, he must first prove that he legally holds the ownership of this house, and then he has the right to sell it. So, the ownership is going to be transferred to the buyer. There must be an easy and secure way to ensure that this ownership is going to be an immutable information, unable to be adulterated from any nefarious agent or activity. The immutability of the data can be achieved by using distributed ledgers, where the data are linked to each other on a specific way creating a binary tree which is called "**merkle tree**" (*Andreas M. Antonopoulos, 2018*). The data are not in the form of clear texts, but are encrypted, using: (1) **asymetric cryptography** (*Hackernoon, 2018*),where each user owns a combination of two keys: (a) a public key which is visible/known to everybody and (b) a secreat key which is called private key, (2) a **hash function** and (3) **hash referencies** (the combination of two hexadecimal strings, which are the output of a hash function in which we have input the data).

As we have seen so far, the new technologies provide techniques and methods that require technical skills and expertise from the users. Moreover, in order to draw up a smart contract with legal rules & policies, which will predict in detail any possible situation that may cause harm to the product, those rules must be prone to be converted to source code.

Thus, the new generation of managers must be well prepared – educated to be able to understand the the benefits of technologies, such as BT, AI, 5G Networks, IoT, and skilled enough to aid on the digital transformation of the Organizations/Companies that they are working in. In the next chapter we will develop in detail the aspects of those technologies, so as to be understood from the reader before we proceed to examine their systemic point of view.

NETWORK ARCHITECTURES

Over the past few years, many network architectures have been suggested, but only three (3) of them are going to be discussed and compared on this chapter: (a) the Centralized Networks, (b) the Decentrilezed Networks and (c) the Distributed Networks. In each case, we are going to examine: (a) the way that data are stored (a single ledger, a distrubeted ledger or synchronized data base) and (b) the credentials that a user has to own in order to have the ability to read and/or to write on the ledger (*Saurabh Goyal,2015*).

Centralized Networks

Nowadays, the most dominant architecture is the centralized networks (Figure 1), where a central controlling entity is responsible for creating and evaluating the credentials of each user/node in the network. On this architecture, all the data are stored on a single central data base, known as "**ledger**".

Each user/node of the network must have the correct credentials, which are going to be validated from the central controlling entity, and then access on the data is allowed.

Those data can be texts, emails, documents, charts, reports or even transactions. Each transaction can be stored on the central data base as a new record. In this kind of architectures, in order to keep the Confidentiality, the Integrity and the Availability of the data (known as "**CIA**"), proper techniques and equipments, like cryptography, digital signatures, firewalls etc, must be used to prevent malicious users/softwares from penetrating into the network.

Many organizations and companies have already traced the potential risks and they have developed Risk Management Plans and Business Continuity Plans, after having recorded their assets, determined the possible risks, evaluated the propability of each risk etc.

So, the possibility of data manipulation or data loss not only is possible, but is also inacceptable. Especially when those data refer to transactions, because those transactions can be used to prove the ownership of assets.

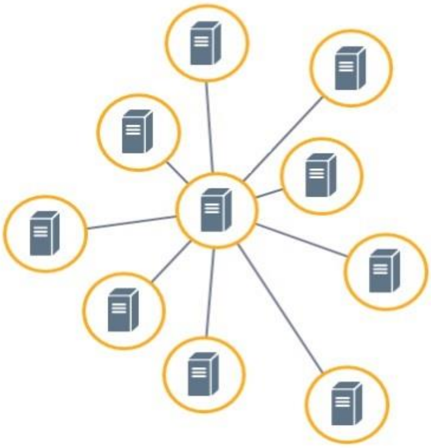

Figure 1. Centralized Networks

Decentralized Networks

The next architecture referes to the decentralized networks (Figure 2), where there is not only one central controlling entity, but the rights to create and evalute users' credentials have been shared among several indipendent entities. In this case the data are not stored to a central location, but they are splintered in parts and stored on different storage servers. At this point, we must stop and discuss the differnet choises that an IT administrator has (*Andrew Tar,2017*). Either he can store the same copies of those data/transactions to each server (known as "**shared ledger**" and it is the default way), or he can split the data according to specific criteria in order to store them on different servers. In each case, those servers are connected through the network. Every node of the network has the ability to read and write data. That explains why if a new record is stored, deleted or edited from a node of the network, then all the nodes are going to have the ability to access this new record. If we study again the matter of a malicious user who wants to gain access on the network, now it becomes more clear the fact that even if he succeeds to penatrate, he can't manipulate all the data, as there are many copies of those data. So, the worst case scenario is to interrupt for a short while the access of a specific group of users/node to the data.

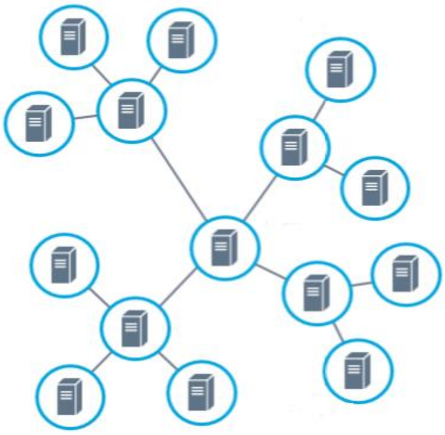

Figure 2. Decentralized Networks

Distributed Networks

The last architecture that we are going to examine referes to the distributed networks (Figure 3). At this kind of networks, there is no central controlling entity, neither indipendent entities which have administration rights. Each node is linked through the network with at least three (3) adjacent nodes and each one of them with another three or more nodes. Thus, when a node needs to store a new record of data/transactions it has to inform all the other nodes of the network, so as to have the same copy of data. A "**consensus mechanism**" is enabled in order to achieve a common agreement/verification of the new transaction. Then the copy of the new transaction is stored on each node (**distributed ledger**). At this point, we can safely conclude that the penetration of a malicious user to the network is a useless movement, as the consensus mechanism has the ability to trace any manipulated data. Also, the transaction between two nodes of this network should be the result of a very well organized/established smart contract, which contains rules and policies that are being agreed upon in common. Legal rules, financial rules and policies, in case a product or a cargo is destroyed, should be the highlights of this contract.

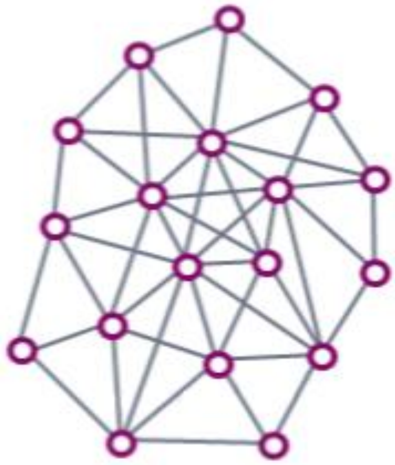

Figure 3. Distributed Networks

BLOCKCHAIN – A DECENTRALIZED NETWORK APPLICATION

The nodes of a network need to have a platform through which they will be able to interact with each other (for example to buy or/and sell a product). So, Blockchain is a Business Network Platform, known as "**Decentralized application - DApp**" (*Supply Chain 247, 2019*), which warrants the transparency of the transaction through which the ownership of an asset is being ensured. Also, the use of a distributed ledger provides data Integrity and Immutability, paperwork reduction, and due to the consensus mechanism, disputes, forgeries and unnecessary Risks are being eliminated.

At this point we will explain how the nodes of the network agree in order to store a new transaction on the next block. Several mechanisms/algorithms have been suggested, like Proof of Work (PoW), Proof of Stake (Pos), Proof of Activity (PoA), Practical Byzantine Fault Tolerance (PBFT) etc, one of them is suitable and it depends on the way the initial stakeholders/creators of a blockchain have defined that this particular blockchain will work. In order to understand how these mechanisms work, we will explain only the Proof of Work (Andrew Tar, 2018), which is the mechanism of Bitcoin.

Let's start with a company (we will call it A) that wants to order a cargo of an industry (we will call it B) that is located on a different country, but both of them are on the same network.

STEP 1: Node "A" deposits the money for the cargo creating a transaction request.

STEP 2: Before node "A" broadcasts the transaction to the network, it will have to use asymmetric cryptography, a random number which is called "nonce" and a hash function, in order to encode the data and to create a digital signature of those data.

STEP 3: All the nodes of the network are trying to solve a mathematical problem which aims to discover the "nonce" (known as mining process). The first node which will discover the correct "nonce" gains the right to create the next Block and at the same time is being rewarded with a small part of the value of the specific transaction.

STEP 4: The Transaction is now stored on a Block and, with the aid of hash functions and hash references, is being combined with other transactions.

STEP 5: The new Block is added at the end of an existing Blockchain and it must be validated form other nodes of the network. The first node that will evaluate the validity of the enclosed data and the cohesion with the previous Block, will gain the right to be rewarded with a small fee.

STEP 6: The transaction is now completed, it is accessible from every node of the network (data transparency) and it can't be changed, it is **immutable**.

DIFFERENT KINDS OF BLOCKCHAINS

Reading the differences of the network architectures, a question may has already been born. Who decides which node has the right to participate in the network and which doesn't? Furthermore, as we have already mentioned on the decentralized architecture, there are some nodes on the network which will be responsible for creating and validating the users' credentials. So, a new question arises: Which are those nodes?

Also, if we go a step further, having in mind the General Data Protection Regulation (GDBR, 2018) it is positively certain that a new requirement is going to emerge. The need of a regulation and/or policies, concerning which node is going to have access on the transactions and which transactions will be able to be read (a part of them or all of them).

In order to answear such questions, we have to describe the four (4) different kinds of blockchains, what network architecture is suitable each time and whether there is a need for a trusted third entity. There are two (2) main criterias for dividing a Blockchain in categories: (a) Which node is going to have access on the network (b) which of those nodes are going to have only reading or reading & writing rights on the Blocks.

For example, if we create a network of raw material companies, pharmaceutical companies, pharmacies and freight forwarders or/and ocean freigt forwarders, then the **blockchain is private**. In this case, there must be some nodes with administartion rights (trusted third entities), which could be for instance the European Medicines Agency – EMA and the National Organization for Medicines of each member state. So, the most **apropriate architecture is the decentralized**. On contrary, if pharmaceutical companies, maritime companies and freight forwarders or/and ocean freigt forwardes could participate at the same time in the blockchain, then the blockchain is free to anyone. In this case, we have a **public blockchain** and the proper **architecture** is the **distributed** one**.**

In both cases, we have to determine which node will have the ability to write transactions on Blocks and on which of the existing transactions are going to have access (reading rights). If any node can create a new transaction request as we have described earlier and at the same time can read all the existing transactions, regardless if those transactions aren't theirs, then we have a **permisionless blockchain** (public or private). But, if specific participants only have the ability to write transactions on the Block and each node can read only its transactions, then we have a **permisioned blockchain** (private or public).

BLOCKCHAIN TECNOLOGIES (BT) AS A MOTIVATING POWER FOR BUSINESS INTELLIGENCE (BI)

As we have seen so far, Blockchain Technologies (BT) have many benefits (data integrity, transparensy, immutability etc) and if we also combine other technologies like Internet of Things (IoT) and Artificial Intelligence (AI), we could transform (**digitization**) businesses and/or organizations.

For instance, we could create a "**smart contract**" (between two specific nodes of the network) using "solidity" programming language and developing special rules, functions and events which will predict what will happen when a product/cargo is being destroyed on the supply channel, either accidentally or deliberately. Thus, a network of clever sensors, like temprature, humidity, light exposure or chemical exposure sensors (IoT), can communicate with the smart contract using the 5G Netwrok. Consequently, depending on the rules of the contract, the sensors will trigger an alarm to inform both the receiver and the dispatcher of the product that there has been a destruction of the product. At the same time, the transportation of the product may be stopped or not, depending on the rules of the contract. In any case, the "**timestamp**" of the destruction has been stored on the contract and it is feasible to assign responsibilities on the culprit.

The most critical question arising by reading the previous paragraph is: Who decides those rules of the smart contract and how is the recipient's money secured in case of product destruction?

NETWORK NODES CONSTRUCT AN ECOSYSTEM

In both public blockchains (distributed networks) and private blockchains (decentralized blockchains) we have mentioned that there must be a platform which is going to be used from all the nodes of the network in order to buy/sell their products and only after a consensus mechanism validates and stores the transaction with an immutable way.

An **Ecosystem** is created containing: (a) Technical Equipment, which is going to connect the different nodes of the network regardless of their geopolitical position, (b) a Network Platform (Dapp), which contains the proper mechanism to broadcast the new transaction, to validate it and after mutual agreement, to save it on a distributed ledger, and (c) a number of different entities/nodes, which are businesses and/or Organizations with a different vision (strategic goal), structure, culture and different processes to convert inflows to outflows. Thus, using Systemic Thinking we can conclude that an ecosystem is nothing more than a **Sociotechnical System** – STS (*Wikipedia, 2019*), where there is an interaction between people who are working in different Organizations/Businesses and through this interaction, the properties of the Ecosystem actually emerge.

SYSTEM THINKING FOR SOCIOTECHNICAL SYSTEMS

In centralized networks, we defined as a System the Company or the Organization. All the internal Divisions or Subdivisions are going to be the Subsystems of the under study System. The energy and the capital resources are the inflows of a System. The viability, the social responsibility, the financial integrity, the organizational knowledge, the products and the quality control of the products are some of the most important factors of the outflows. The Internal Enviroment of the under study System consists of the inflows, the outflows and the procedures and/or technologies that are being used to convert inflows to outflows.

There are also many factors that affect the Systems' function, like the regulatory/legistlative framework, the politics of the country in which the System is situated, the technological developments, the financial framework etc. All of these form the Indirect Environment of the System. The competitors, the partners, the suppliers and the customers are the main entities of the Direct Environment of the System (*Leah May Cabugao,2016*).

However, an Ecosystem is a network of entities, entities that might be the customers, the suppliers, even other companies that are competitors. As we can see, those entities are the subsystems of a bigger system. Using the definition of "System" we will finally prove the reasons why we must manage those ecosystems using systemic methodologies and theories.

So, "System" (*Russell Ackoff, 1981*) is: "a single set, which has one or more defining functions and consists of two or more essential parts, fulfilling three (3) basic rules". The "defining function" is nothing more than the role that each entity (subsystem) serves within the System,through which we will understand the cause of the System Existence and how it works.

At this point we establish that the word "System" will be used whenever we refer to the whole network of diferrent entities. Subsystems of this System are going to be each entity of the network. More specifically:

1. The "essential parts" are the parts that are vital for the System, if we exlude one of them then the System can't be functional. In order to define what are the essential parts on this System we must consider the first rule (each essential part can influence the behaviour and/or the properties of the system it belongs to). At this point we will examine an example. Suppose that an entity/subsystem in the Blockchain aims to gain as much computer power as possible so as to act malicious (in proof of work mechanism) or to own more than 51% of the cryptocurrencies of the network (in proof of stake mechanism), then the actions of this specific entity/Subsystem or a group of entities/Subsystems are going to influence the whole System. Thus, we can conclude that: (a) each entity/Subsystem is an essential part of the whole System, (b) all the entities/Subsystems must be related to each other and (c) through the interaction of those parts the status/properties of the System will become evident.
2. Considering the third rule (if the divisions or/and subdivisions are organized in subsystems, then they inherit the properties of their hyper system) immediately came to our mind the question that we described earlier about the smart contracts. The rules and the policies of those contracts are going to influence the interaction between two or more Subsystems of the network. For example, if we create a smart contract that has very strict financial rules, concerning the fact that the product may be destroyed accidentally (while is being transported through the supply channel), in this case and due to the disintermediation that we have achieved using the Blockchain Technologies (no need for insurance contracts), the financial damage of the dispatcher it might be much higher than its financial strength. So, not only it raises a need for cautious movements, as far as the management of those contracts is concerned, but we can also define the **essential parts** of a Subsystem which certainly take part while this contract is being established. Those are: (1) the Legal Affairs Department, which will define the legal policies of the smart contract, (2) the Financial Affairs Department, which will decide the contract time limits and the rules of reimbursement in case of product/cargo destruction, (3) the IT Department, which will create the contract, converting the legal and financial rules to source code, and finally (4) the Manager – CEO (or the Management Department depending on the structure of the company/Organization) which will be responsible for the coordination of all those parts and to ensure that the vision of their Company/entity/Subsystem isn't in contrast to the vision of the Blockchain Network (Figure 4).

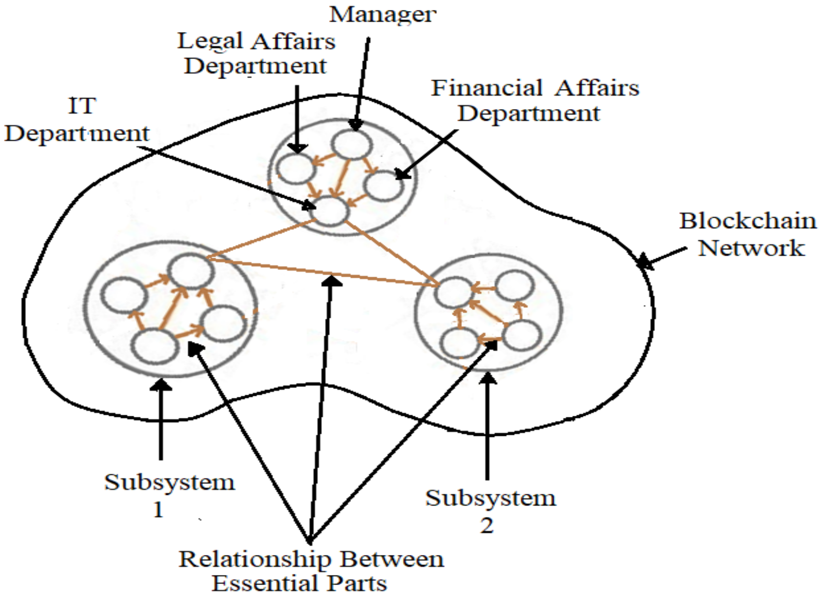

Figure 4. Blockchain Network as a System

DCSYM METHODOLOGY FOR VISUALIZATION OF SOCIOTECHNICAL SYSTEMS

As we have seen in the previous chapter, System Thinking can be applied on a network of entities, but how can we depict the structure of this System by drawing? Thus, we must use a systemic methodology to visualize this System in order to trace its structure, the inheritance of properties from the System to its Subsystems and to define how they communicate and what are their controls.

In order to apply the Design and Control Systemic Methodoly – DCSYM (*Assimakopoulos Nuikitas, 2009*), first we need to define a few factors. So, suppose that a network of 4 entities (three pharmaceuticals companies and one freight forwarder company), located in Greece has been established and that they have mutually agreed to participate in a Blockchain platform (DApp), in order to buy and sell their products. They have also agreed that their cryptocurrency will be a coin similar to euro and that each company will have the ability to participate simultaneously in other Blockchains too, for example with the pharmacies that they cooperate or with other retailers.

Prior to Blockchain, those companies were separate entities and in fact, in many cases, they were competitors. Thus, using the DCSYM Methodology to imprint those Systems, we would have observed an image like the one in Figure 5. Where, companies 2,3 and the freight forwarder company are situated in the External Environment of company 1. We have also used the "Purposeful Action - U" for the control relationships between the Chief Executive Manager-CEM and other Department Chiefs (CMO, CFO, CLO and CITO). The "General Interaction or Influence - g" has been used to define the communication between companies 1,2,3 and 4.

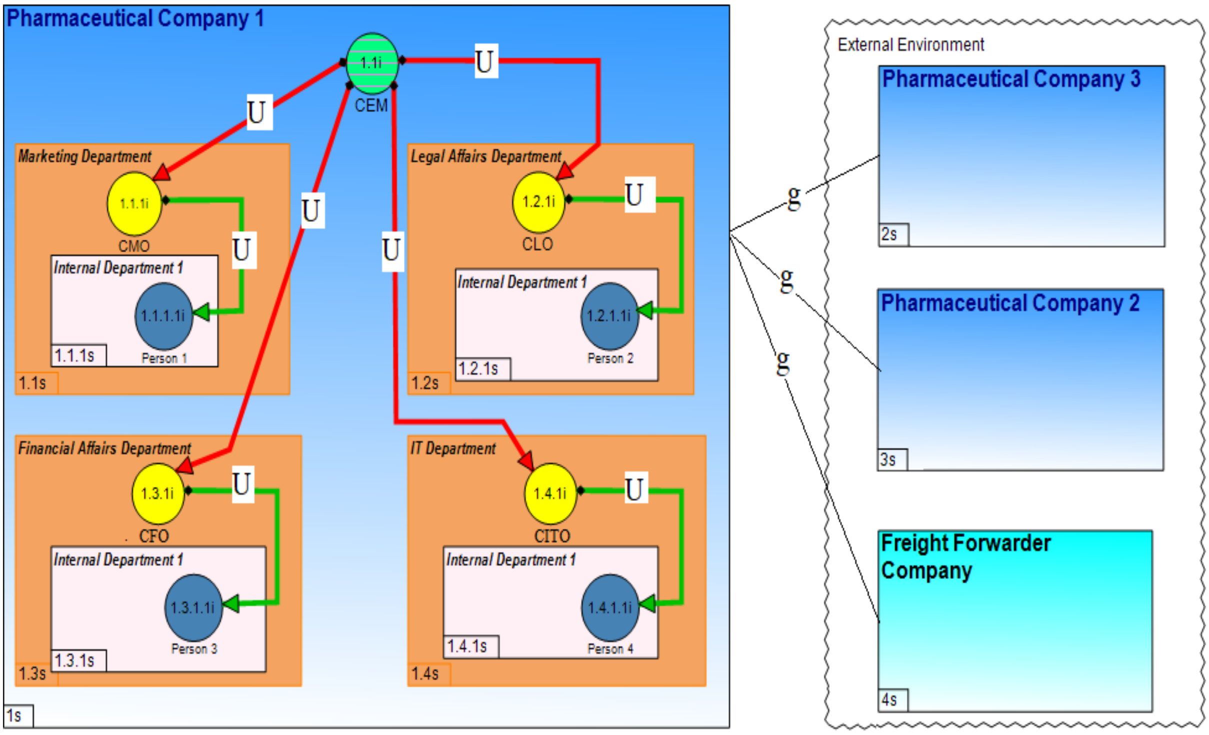

Figure 5. Before the usage of DApps

Nevertheless, using a Blockchain Platform over a distributed network (public blockchain), where everyone has access and there is no need for entities with administration rights, the System that is being created is visualized in Figure 6. In this network each company can append a smart contract with another company of the network, using the freight forwarder company of the same network. Due to the fact that the contract is just source code, the Chief of Informatics and Technology Officer- CITO of company 1 must communicate with the CITOs of company 2 and the freight forwarder company. Also, in order to develop the correct legal and financial rules/polices, the Chief Executive Manager - CEM of company 1 must communicate and agree with the Chief Executive Manager of company 2. In addition, in order to develop the correct rules in case of product/cargo destruction, the communication between the Chief Executive Manager of company 1 and the CEM of the freight forwarder company is called for. (On figure 6 we have used one control entity, although we have mentioned that there must be more than one controlling entity in decentralized architecture. The scope of this figure is just to be understood from the reader by visualizing the structure and the possible communications and/or the control relationships between the Subsystems of a small decentralized network).

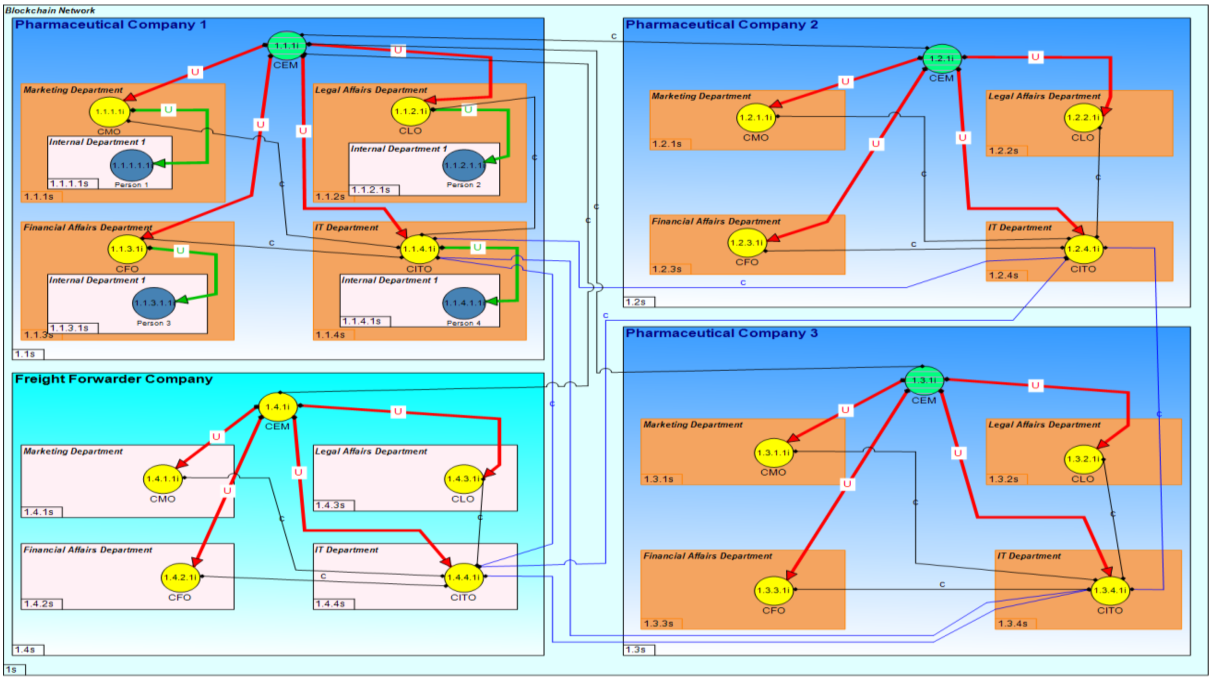

Figure 6. Using DApp over Distributed Network

But, in a private network there are some entities (q.v. company 1) that have administration rights. Those Subsystems are responsible for defining which node/Subsystem has the right to write on Blocks and which data it can read. In this case, the System is a little bit different as the administration rights will be drawn as control relationships with "Potential Conflict -P" between those Subsystems (Figure 7).

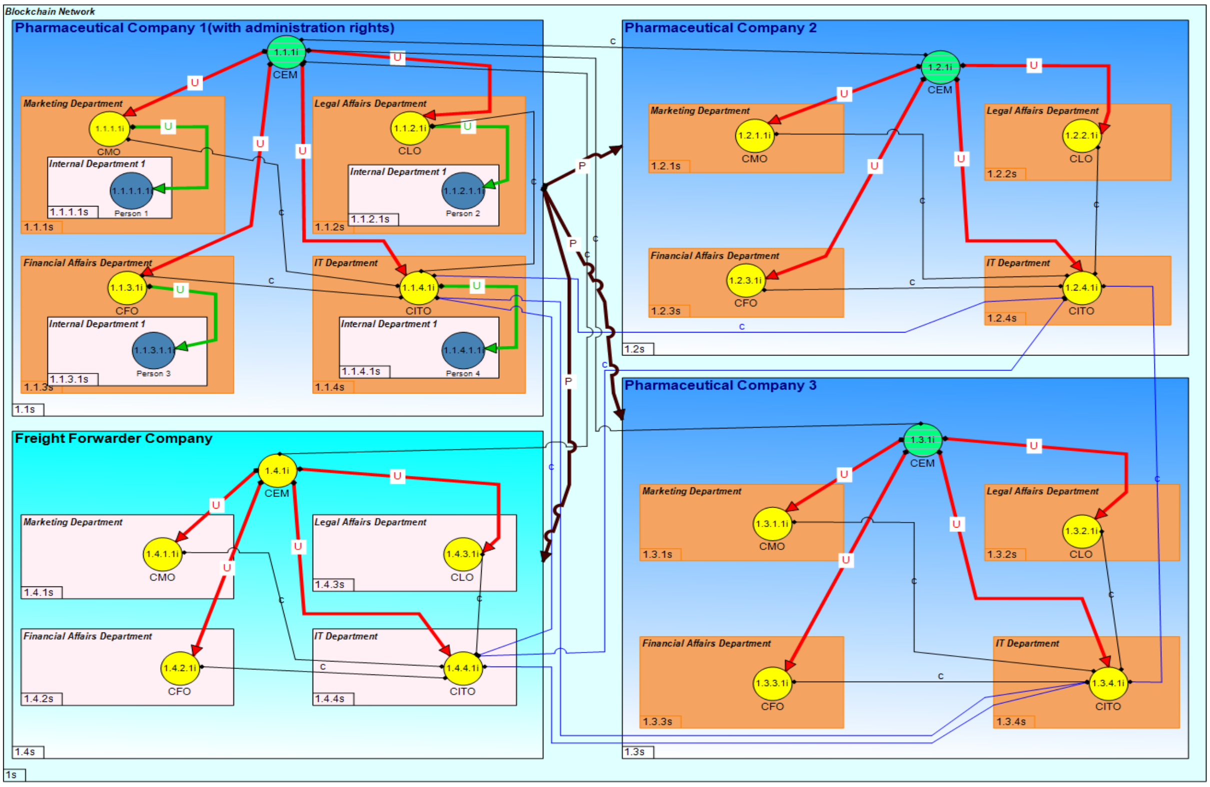

Figure 7. Using DApp over Decentralized Network

VSM MODEL FOR THE VIABILITY OF THE BLOCKCHAIN NETWORK

At this point we use the definition of Viable System: "A system is viable when is capable to ensure its independent existense". The Viable System Model - VSM (*Anthony Stafford Beer*,*1972*) has created the roots for the "Cybernetics management", which is applicable on all kinds of organizations, on the interconnections among organizations and on the interconnections among the essential parts of an organization (Figure 8). Thus, we consider the whole decentralized network as an organization of nodes, which must maintain the balance with its dynamically changing environment in order to achieve its viability/existanse.

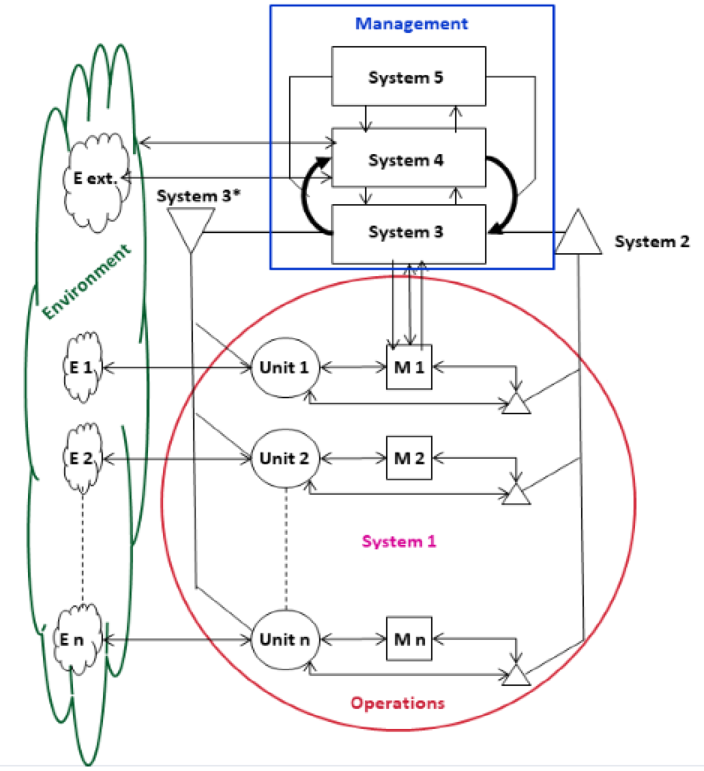

Figure 8. Viable System Model

We have chosen the private Blockchain as we can observe all the five (5) Systems of this Model. More specifically, we consider as:

<u>For Layer 1 (Figure 9):</u>

System 1: The basic activity of each entity of the private network is to interact with other entities of the same network for creating, validating and storing transactions (crucial operations). Thus, the operations in System 1 will be all the **nodes/entities/companies** devided depending on their subject matter. For example, an operation of System 1will contain the companies that provide raw metirials, another one will contain those companies which convert the raw meterials to a final product/good. The freight forwarders or the ocean freight forwarders companies will be contained to another operation of System 1, and so on. The reason why we divided the operations of System1 based on this criteria is to enforce the drawing of the next Layer (recursiveness).

System 2: (Monitoring the internal stability of the network and the coordination of System 1). The interoperability between the entities of System 1 can be achieved only with the use of the common platform (Decentralized Application). Through this DApp, the different companies/entities can communicate either with other entities (for example the Subsystems 12s,13s and 14s in Figure 7) or with the entity which has administartive rights (Subsystem 11s in Figure 7).

System 3*: Is the Sporadic Audit of System 1. We can use an **Artificial Intelligent (AI) algorithm** which will record all the alarms that have been triggered on smart contracts and which of the Operations of System 1 were responsible for these triggers. The evaluation of the specific entity in System1 of the next Layer will define whether there is a need of improvement, or if there is a need to exlude this specific entity from the network.

System 3: This System controls the whole System 1 (Direction and Optimization) because, according to Stafford Beer, System 3 is a day-to-day administration. Due to the fact the the whole System 1 communicates with System 2 through the Decentralized Platform, that is why we suggest that System 3 must contain **all the IT Departments** of those entities that have administration rights on the platform and that are responsible for the creation and the validation of the nodes' credentials.

System 4: Is responsible for the Long Term viability of the whole System. At the same time, it monitors the changes of the environment and makes any appropriate changes. For example, changes on laws, a new framework for Information management or Risk management, financial changes on ICOs or new rules/policies from the European Council about the stablecoins. So, System 4 is going to be a **group of Legal Affairs Departments and Financial Affairs Departments of all the nodes who have administartions rights.** Also, they will be responsible to inform their IT Departments for adding new source code on the common Platform regarding those new rules.

System 5: This System keeps the Identity of the whole. At the same time, it is an ultimate authority, who is responsible for the management of the differences between System 3 & System 4 and promotes the business intelligence of the whole network. That is why we propose to be the group of CEMs of those entities which have administrative rights.

Environment (of each unit of System 1): Companies that are not yet members of the private Blockchain that we are examining and that they are cooperating with one or more companies of an entity in System 1.

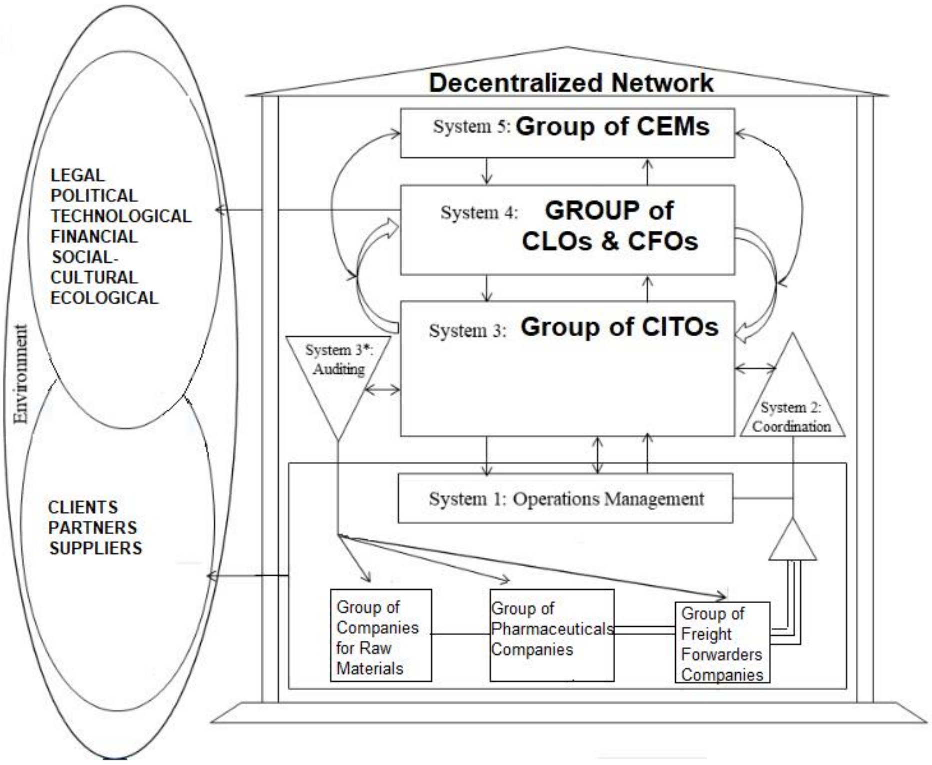

Figure 9. VSM on Decentralized Networks -Layer 1

For Layer 2:

System 1: Each operation of System 1 is a different company/entity/Subsystem of the same subject matter (for example raw materials companies) in Figure 7.

System 2: The smart Contracts through which new transactions will be created and will be saved through the use of the common Platform on Level 1.

System 3*: The specific rule, event and/or function of a smart contract, which will be enabled when an alarm will be triggered by a specific sensor of the IoT network.

System 3: The group of IT departments of the entities in System 1.

System 4: A group of Legal Affairs Departments and Financial Affairs Departments of the entities in System 1.

System 5: The group of CEMs of those entities in System 1.

Environment (of each unit of System 1): As we have mentioned before, a company might participate in a private Blockchain (so it is an entity in System 1), but it might also be a member of another Blockcain (for example, a Blockchain with its retail clients). In this case, those retail clients make up for the environment of the group, to which this System 1 entity belongs to.

We must mention that it is possible to identify the next Level (level 3), but it is out of the scope of this study.

CONCLUSIONS

In this study, we attempted to approach the Blockchain Technologies from a Systemic point of view. We started explaining what are the possible network architectures that can be applied on Decentralized Applications and we also described how Proof of Work mechanism works. We enriched the knowlowdge of our reader about the network of sensors (IoT) that should be used combined with the 5G Networks, in order to trace the product on the supply channel and so to trigger alarms on the smart contract in case of a product/cargo destruction.

We continued, describing the differences of the Blockchains so as to highlight their benefits, which in our oppinion the most important are: (a) the data transparency and (b) the data immutability because through those we can prove the ownership of an asset. Certainly, the Blockchain Technologies possess a motivating power for Business Intelligence but there is a lot of work in front of us, as a legal framework needs to be developed.

Our study went one step further by applying a systemic approach on this Ecosystem (the network of entities which are located in different geopolitical positions). We presented which are the proper systemic methodologies not only for visualazing this Sociotechnical System, but also for ensuring its viability.

This study is just the beginning, it includes the first phase from a multi-phase process through which we will explain to the next generation of managers what are the proper methodologies, theories, models and tools that should be used in order: (a) to manage the stakeholders of a decentralized application, (b) to develop the proper policies and rules which will ensure the viabilty of the network (especially in decentralized architectures – private Blockchains), (c) to develop a risk management process in case of a malicious user or a group of malicious users. Finally, through our research we aim to educate them and to empower them with the proper knowledge on legal terms, financial terms and on code development regarding the Blockchain Technologies (BT).

RÉFÉRENCES

Daniel Drescher (2017). Blockchain Basics - A non-Technical Introduction in 25 Steps. Retrieved from: https://www.apress.com/gp/book/9781484226032

Ameer Rosic (2016). Smart Contracts: The Blockchain Technology That Will Replace Lawyers. Retrieved from: https://blockgeeks.com/guides/smart-contracts/

Wikipedia (2019, August 22). Timestamp. Retrieved from: https://en.wikipedia.org/wiki/Timestamp

Andreas M. Antonopoulos (2018, February 26). Blockchain Fundamentals – What is a Merkle Tree. Retrieved from: https://medium.com/byzantine-studio/blockchain-fundamentals-what-is-a-merkle-tree-d44c529391d7

Hackernoon (2018, November 22). Asymmetric Cryptography in Blockchains. Retrieved from: https://hackernoon.com/asymmetric-cryptography-in-blockchains-d1a4c1654a71

Saurabh Goyal (2015, July 1). Centralized vs Decentralized vs Distributed. Retrieved from: https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868

Andrew Tar (2017, December 02). Decentralized and Distributed Databases, Explained. Retrieved from: https://cointelegraph.com/explained/decentralized-and-distributed-databases-explained

Supply Chain 247 (2019, September 03). The Insolar Blockchain Business Network Platform. Retrieved from: https://www.supplychain247.com/paper/the_insolar_blockchain_business_network _platform

Andrew Tar (2018, January 17). Proof-of-Work, Explained. Retrieved from: https://cointelegraph.com/explained/proof-of-work-explained

EY – Bulding a better Working World (2018, August). General Data Protection Regulation (GDPR): The paradigm shift in privacy. Retrieved from: https://www.ey.com/Publication/vwLUAssets/ey-gdpr-aug-2018/$File/ey-gdpr-aug-2018.pdf

Wikipedia (2019, August 16). Sociotechnical System. Retrieved from: https://en.wikipedia.org/wiki/Sociotechnical_system

Leah May Cabugao (2016, July 12). Chapter 2 – Business and its Environment (pages 20-46). Retrieved from: https://www.slideshare.net/leah_may6/chapter-2-business-and-its-environment-63932333

Russell Lincoln Ackoff (Copyright 2017, Graham Berrisford). Ackoff's ideas- for applying system theory to management science. Retrieved from: http://grahamberrisford.com/AM%204%20System%20theory/SystemTheory/ChallengingSystemsThinkers/Ackoff%27s%20ideas.htm

Assimakopoulos Nikitas (2009, January). The Design and Control Systemic Methodology (DCSYM): a multi-agent modelling and operation platform. Retrieved from: https://www.researchgate.net/publication/247835569_The_Design_and_Control_Systemic_Methodology_DCSYM_a_multi-agent_modelling_and_operation_platform

Anthony Stafford Beer (1972). Brain of the Firm from: https://books.google.gr/books/about/Brain_of_the_firm.html?id=T_A9AAAAIAAJ&redir_esc=y