Automating Ex-Post Enforcement for Spectrum Sharing:
A new application for Block-chain technology

Amer Malki[1], Martin BH Weiss[2]

Abstract
One of the "Grand Challenges" in spectrum sharing that was identified by leading researchers was automating the enforcement of spectrum sharing [1]. In general, the automation of enforcement has numerous challenges, including the detection of events, gathering forensic evidence surrounding the event, maintaining the security and provenance of the records, and conducting adjudication that is consistent with the extant rights structure [2]. To illustrate this challenge, Shay et.al. [3] conducted a simple experiment surrounding the enforcement of traffic laws. One of the "Grand Challenges" in spectrum sharing that was identified by leading researchers was automating the enforcement of spectrum sharing. In general, the automation of enforcement has numerous challenges, including the detection of events, gathering forensic evidence surrounding the event, maintaining the security and provenance of the records, and conducting adjudication that is consistent with the extant rights structure. This work will be looking at the enforcement aspect in the spectrum sharing regime, especially on ex-post enforcement by using Block-chain technology to automate the ex-post enforcement processes. The potential usages can be divided into three applications which are ex-post enforcement using Block-chain by itself as Publicly-Distributed-Database, ex-post enforcement using Smart Contract, ex-post enforcement as Decentralized Autonomous Organization (DAO)

Keywords
Spectrum Sharing —Ex-post enforcement — Ex-ante enforcement—Spectrum Access System (*SAS*)—Block-chain

[1] *Email: asm110@pitt.edu, School of Information Sciences, University of Pittsburgh, Pittsburgh, PA*
[2] *Email: mbw@pitt.edu, School of Information Sciences, University of Pittsburgh, Pittsburgh, PA*

Contents

Introduction

Spectrum sharing policy was introduced to utilize the spectrum properly and to overcome limitations in access to radio spectrum. In a broad sense, this amounts to a reformation of rights relationships between the spectrum sharing entities. The stakeholders in the sharing arrangement include the (incumbent) Primary Users (PU) who hold the spectrum license, and the (entrant) Secondary User (s) who may use the spec-

trum temporarily or with rights that are subordinate to the license holders. A set of strategies and technologies are required to enforce rights in any management system [4] and the timing of the enforcement action (ex-ante and ex-post) plays a significant role in such a management system [5]. Ex-ante enforcement is measures are designed to prevent stakeholder rights from being violated. In most discussions, this focusses on ways of protecting a PU's signal from harmful interference caused by an SU [6, 7], while ex post mechanisms deal with addressing the consequences of interference after the fact. Practical enforcement schemes have ex-ante and ex-post enforcement that are coupled.

The analysis performed in [2] suggests that this approach is too narrow. The authors note that SUs have usage rights that deserve to be enforced as well, and that the collective action rights associated with spectrum sharing may require enforcement measures beyond interference. Collective action rights include the right to determine who may use spectrum (and when they may use it) and who may determine who is excluded. The Commerce Spectrum Management Advisory Committee (CSMAC) counsels the National Telecommunications and Information Administration (NTIA) on any matter related to spectrum policy. CSMAC's enforcement subcommittee report suggested that the emergent spectrum sharing systems to use geolocation databases (e.g., TeleVision Wight Space (TVWS) databases and Spectrum Access Systems (SAS)) to mediate spectrum access, so the enforcement of the collective action rights amounts to requiring transparency of decision making as well as audits of these systems. As we move to more intensive sharing of spectrum, the likelihood of events that are enforceable ex post increases, despite ex ante measures. The Enhancing Access to the Radio Spectrum (EARS) second workshop report [1] recognized this and set the goal of lowering the costs by automating some of the ex-post enforcement steps.

This paper will study the enforcement in Spectrum Access Systems (SAS) based spectrum sharing regimes. We focus in particular on the enforcement events that occur in the normal course of spectrum sharing (i.e., Type 1 events as described in Table 1); in doing so, we exclude treatment of "rogue" or "pirate" radios, and of interference due to equipment failures of devices and systems that are not participants in the sharing regime. These excluded events are important to address, but we hold that they require a distinct enforcement methodology that may not be amenable to automation under today's technology.

In our analysis, we consider two architectures for enforcement systems: a third party enforcer and a self-reporting approach [8]. In the third party enforcer approach, the enforcer must be trusted by all the entities of the system and must have authority to resolve enforcement violation events [9].

We will examine how these two architecture apply in the enforcement of usage as well as collective action rights. A hypothetical scenario of using the recommended ex-ante enforcement (protection zones) and the involved entities will be used to analyze ex-post enforcement steps and the enforcer role in both architectures. This hypothetical scenario concerns about the behavior of the SUs is significant / of concern if SU-mobile devices transmit near PU-base station or if they are transmitting high power signals within the protection zone. These behaviors will cause harmful interference to the PU signal and data received by the PU will be lost. For ex-post enforcement, we will follow the graduated response approach that had been suggested in [10].

The role of the enforcer in the ex-post enforcement is to prevent, detect, conduct forensic analysis, adjudicate, and control parties' behaviors. In the self-reporting approach, PU and SU would report their own activities to spectrum sharing enforcement authority (which could be SAS for this architecture) when they violated the spectrum sharing policy. Following the self-reporting approach, the detection and forensic roles will be deducted from the enforcer because parties report their violation act, in addition, reducing the risk of getting uncertain sanctions when violating the spectrum sharing policy.

This paper is divided as follows: section 2 will give a historical background. Section 3 will provide the motivation and the purpose from this work. Section 4 will explain the structure of the automated enforcement system. Section 5 will introduce the Block-chain and how does it work. Section 6 will explain the Block-chain usages and its potential applications to enforce Spectrum Sharing policy between the sharing parties. Section 7 will discuss and conclude this work.

1. Background

As spectrum sharing has moved from the laboratory into commercial systems, the efficient, effective and predicable enforcement of rights has become more critical. As shown by [11] and [2], the notion of rights becomes more complex in shared spectrum. The rights bundle that users are endowed with consist of usage rights (right to transmit, right to receive) as well as collective action rights (management rights, exclusion rights, appropriation rights). Both classes of rights deserve both definition and enforcement, even if most of the attention today is on enforcing usage rights, which involves the prevention or detection of interference between multiple users. Weiss et.al. [2] have made a case for the need to enforce collective action rights as well as interference rights in spectrum sharing systems. To date, collective action rights have been exerted through the NTIA's CSMAC process[1] and in the Federal Communication Commission (FCC) (through the Administrative Procedures Act (APA)). In spectrum sharing systems, these collective actions are codified in software-based SAS systems which will require transparency as well. Since these collective action rights are not fully recognized or understood, they are not amenable to automation at this time.

Enforceable interference events might be subdivided into four distinct types, as outlined in Table 1. Each type of interference

[1] The Commerce Spectrum Management Advisory Committee (CSMAC): https://www.ntia.doc.gov/category/csmac

Type 1	Events due to the routine operation of participants in a sharing ecosystem
Type 2	Events due to "rogue" or malicious users
Type 3	Events due to faulty equipment of authorized spectrum users
Type 4	Events when all users are in compliance with all applicable regulations

Table 1. A typology of interference events

calls for different technical, operational and legal approaches. Type 1 interference events might occur due to aggregation of similar devices, propagation anomalies, location errors, etc. In these kinds of events, we expect that the radios are compliant with applicable technical and operational regulations. We cannot say the same about Type 2 interference, which might be software radios that have temporarily been programmed to operate in a band and may not make an effort at compliance with the appropriate technical and operational requirements. These may or may not have a typical physical characteristic that would allow them to be automatically identified. Type 3 events are due to leaky cables, poor filters, etc. We would expect these to be licensed devices that fit no particular patter or lack a particular physical characteristic. Type 4 events occur when regulations or licenses are incomplete and/or poorly written or assigned.

For the purpose of this paper, we consider only Type 1 events because we believe that these are most amenable to automated enforcement. In these cases, the ex post enforcement process, consisting of detection, forensic analysis, and adjudication, is most straight-forward. Type 1 users who cause interference will not actively try to mask their identity and The characteristics of their transmitted signal is most likely understood[2], making detection easier. They will most likely cooperate with the forensics process, and they will most likely respond cooperatively to the outcomes of the adjudication process.

2. Motivation and Purpose

In the US, much of the attention on spectrum sharing is between federal users and commercial users. Thus, the Primary User (PU) or the spectrum incumbent is a federal agency and the secondary user (SU) with subordinate rights is the commercial user. Sharing agreements are worked out in the Commerce Spectrum Management Advisory Committee (CSMAC), which counsels the National Telecommunications and Information Administration (NTIA) on any matter related to spectrum policy. A part of such agreement includes the applicable enforcement regime which might be propylactic in nature (i.e. ex ante) or remunerative (ex post). The CSMAC's enforcement subcommittee report suggested that the Spectrum Access System (SAS) could play a role in implementing enforcement mechanisms for spectrum sharing. To do that, SAS expected architecture and responsibilities to manage both

[2]This is notably not true for military radars and other military signals.

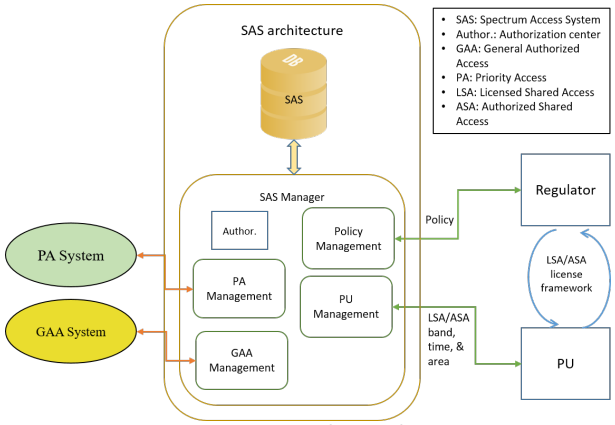

Figure 1. Prototype of SAS from [2, 12]

spectrum assignment and harmful interference were explained in [12]. Figure **??** shows SAS architecture base on a model from [2, 12]. Sohul et. al summerized SAS duties as follows [12]:

1. It would need to access PU's database to collect information about the PU spectrum utilization.
2. It would need to coordinate with the regulator to update the policy.
3. It also would need to access SU's database to get: 1) devices geolocation, 2) interference environment, 3) radio constraint, 4) and spectrum request.
4. It would the ability to:
   (a) allocate spectrum on the dynamic bases,
   (b) detect and resolve any unwanted interference event.

Figure 1 shows SAS model which relies on a central authority (central-closed database, and central manager (controller)) to enforce the spectrum sharing rights among the PU and SU. On the other side, the CSMAC enforcement subcommittee report recommended NTIA to use a third party to enforce the users rights for the spectrum sharing regime. In such a centralized system with a closed-database would require the third party enforcer to go through a costly security measures to be certified. These certification costs would impact heavily on the cost of the ex-post enforcement. If the cost of the ex-post enforcement is too high, the sharing entity would prefer not to share the spectrum as a result.

Further, Shavell and Kaplow studied a model of probabilistic law enforcement to on how to control harmful behaviors [8]. They added to the model a self-reporting approach and compared it to the approach without self-reporting mechanism. The self-reporting approach is when entities can be encouraged to report their harmful actions without significantly affecting their incentives whether or not to commit the act. They found out that the enforcement system with a self-reporting approach would save the enforcement resources, and the risk of getting uncertain penalties would be reduced. In spectrum sharing, self-reporting approach is when PU and SU would report their own activities to spectrum sharing enforcement authority. Unfortunately, self-reporting approach is

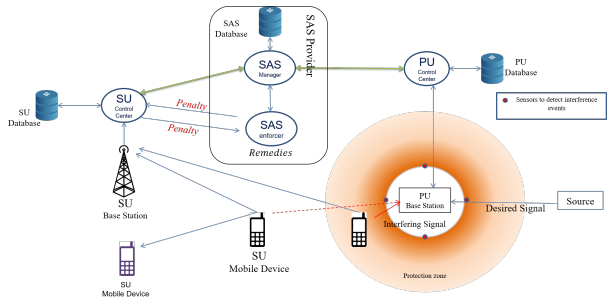

Figure 2. Spectrum Access System (SAS) with a centralized database

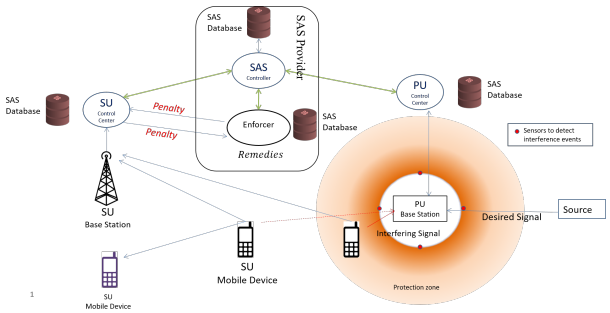

Figure 3. Spectrum Access System (SAS) with a Block-chain (publicly-distributed-database)

not applicable with such centralized-closed-database.

Figure 2 shows an example on spectrum sharing between the PU and SU when using SAS with a centralized database. The sharing entities are : 1) PU, 2) SU, 3) And CSMAC report added a SAS provider. To enforce the users rights, SAS provider would play the role of the manager, the data provider, and the enforcer. To enforce the rights of the spectrum sharing, SAS would need to access both PU and SU databases. To monitor the spectrum, sensors need to be built around the PU base stations. These sensors will have a range called protection zone to detect any harmful interference. We will be looking at the enforcement aspect in this case. SAS provider would take inputs from incumbents regarding their spectrum utilization and manage the secondary use of the available spectrum opportunities.
If a SU wishes to transmit, it requests the SAS [2]. SAS would decide whether or not to authorize the SU's transmission based on: 1) a database, 2) the license outline. The license outline should be populated and sustained mutually by the regulator and the PU. Every time there a violation spectrum sharing rights, SAS enforcer would access the database for the data to apply the remedies to the violator. With centralized database as the example on Figure 2, then the data would reside with the SAS provider. The SAS provider would have pile of potential exclusive information that is possibly vulnerable and It could be a hacking target.

2.1 SAS with a publicly-distributed-database

An alternative to the centralized management scheme when using Block-chain technology. The Block-chain technology is a publicly-distributed-database. The Block-chain technology provides an opportunity for any system to be an open reliable and democratic, such when used on the economic system. We aim to build the wireless-telecommunication industry symbolized in spectrum sharing regime that is open, reliable, and democratic. We introduce Block-chain technology to be used for Spectrum Access System (SAS) to automate the ex-post enforcement processes.

Figure 3 shows the same example of Figure 2 but with the usage of the Block-chain technology (publicly-ditributed-database). The SAS controller coordinate with the PU and SU. SAS provider would play the role of the controller, the data provide. SAS provider also might play the role of the enforcer or the role could be played by an external entity since the database is public, distributed, and stored by all the involved entities. In this example we hypothesize that enforcer is under the SAS provider responsibilities. To monitor the spectrum, sensors need to be built around the PU base stations. The Spectrum sharing database would be distributed and stored among the sharing entities. Every time there a violation for the users rights, SAS enforcer will apply the violation remedies based the publicly-distributed-database.
The example on Figure 3 shows that Block-chain technology will provide:

1. The opportunity to SAS to be open, reliable and democratic system.
2. Data is stored in every node
3. Even if a system fails the integrity of the distributed database is maintained.
4. Enable users to control their own information rather than giving it to a centralized entity

On the other side, the performance of the distributed database is always under question. And the traffic of the network would increase. Also, When using PoW as a voting tool for the Block-chain to reach consensus, the power and process consumption may also become a limitation when used with devices that had limited processors and power.

3. Brief Introduction on the Block-chain Technology

Block-chain is a promising technique that may have more usage in the near future. Block-chain technology is a a publicly-distributed-database that can be used in any system. It can be defined as a resilient, reliable, transparent and decentralized way of storing and distributing a database across all nodes of a network. The Block-chain is a database that contains digital actions, in general. These digital actions might be transactions, a registry system, an inventory system, tracking, or monitoring assets [13]. These digital actions propagate from one entity to another through the system with the help of a digital token. A digital token is a unique address specified only for a certain digital action. The Block-chain application can only decide on the representation of the digital token,

whether it is payment, a transferring of fund, or registering a property.

The main benefits when using Block-chain technology in a system are: 1) the database is stored in each node connected to the network, and 2) It is used to store and distribute any action in the network to all the nodes. The Block-chain technology provides an opportunity for the economic system to be an open, reliable, and democratic system [14]. That opportunity opens the door for researchers to try implementing this technique on other system's applications as well. We aim to build the wireless-telecommunication industry symbolized in spectrum sharing regime that is open, reliable, and democratic.

In the last two years in the United States, over $00 million has been invested in Block-chain associated technology [15]. In addition, some of the largest financial companies funded startup corporations to find Block-chain applications to be applied on Wall Street [15]. In fact, in 2015, the National Association of Securities Dealers Automated Quotations (NASDAQ) lunched the Linq platform, based on Block-chain technology, from the startup Chain to trade non-public shares [16]. IBM and Samsung are experimenting with Block-chain technology to power the Internet of Things (IoT) [17]. Swan named the Block-chain as the fifth most disruptive computing paradigm after mainframes, PCs, the internet, and mobile/social networking [13]. Andressen[3] elected the Block-chain technique as the most important invention since the internet itself [17, 18].

Block-chain is used as a supportive technique for Bitcoin [13]. Smart contract is another example of using Block-chain as a supportive technology to implement and monitor contract terms [14]. Nick Szabo proposed the idea of a smart contract [19], but was not well-known until the emergence of cryptographic currency [14]. Block-chain takes advantage of cryptographic methods to guarantee both trust and reliability of the blocks. Any Block within the Block-chain consists of digitally signed actions that are approved by the network. Each Block contains a reference to its ancestor Block to form a Block-chain. Block-chain technology can be used to support many types of applications (financial, economic, market, cash transactions, government, health, or science) [13].

The Block-chain is simply a chain of Blocks that represent a public ledger stored and distributed among all the nodes of a network. Depending on the application that it is used for, a Block records all the digital actions between the nodes of a network, which contain the date and time, and a reference to its ancestor Block [17]. Figure 4 shows how the Block-chain is interconnected from the first Block to the last one and the assembly of the Block. The Block consists of a header, Block size, digital action counter, and list of digital actions [21]. The digital action contains contributors, the date, time, and activity. In Bitcoin, the average size of the digital actions (transactions) is, at a minimum, 250 *bytes*; and the average Block holds over 500 digital actions, while the header size is fixed to 80 *bytes* [21]. The header fields of each Block are a time stamp, nonce, a hash of previous Blocks, and Merkle root [22]. The time stamp is the approximate creation time of the Block. The nonce is a counter used to ensure each digital action is only handled one time [23]. The hash of the previous Block is used to link this block to the prior one to construct the chain of Blocks. The Merkle root is the Hash of the Block (Block's fingerprint). It is a digest of all the transactions in the Block [21]. The Merkle root is used to verify the integrity of the Block. As shown in Figure 4, the Merkle root is created by repeatedly digesting pairs of digital actions until there is one root hash [21].

Next we will give a brief explanation about an important process within the Block-chain technology called mining because it may play an important role when adopting the Block-chain technology. (More in-detail information about the Block-chain technology in Appendix A).

3.1 Mining

When a new digital action needs to be validated and added to the Block-chain, the Mining procedure is used [21]. It is used to protect the Block-chain against falsified digital actions (such as double-spending in a Bitcoin network or void signatures) [21, 24]. Miners[4] authenticate new digital actions and add them to the publicly-distributed-database [21]. Digital actions are grouped into a single Block and are validated periodically[5]. However, in other cryptographic currency such Litecoin, the transactions are grouped in a single Block every 10 minutes [20]. Miners compete amongst each other to find a solution to intensive and pressing mathematical puzzles [27]. The greater the processor's power the miners put in, the greater the chance of finding the solution and wining. If a miner solves the mathematical puzzle, the miner broadcasts the Block of the digital-actions to all the nodes of the network to be approved. This approval step is called Consensus model. All the other nodes in the network check the Block to verify that the miner solved the Mathematical puzzle. If more than fifty percent of the nodes agree, that Block of digital-actions is added to the Block-chain [27].

Mining is the process of solving a challenging mathematical problem (mathematical riddle) based on the cryptographic hash algorithm. Miners participate to solve the mathematical problem by applying the Hash function to the block header frequently by changing one parameter until the outcome string of characters matches a certain goal [21]. The mining process is achieved by harnessing the computing power of the Miners to discover valid Blocks [28].

Table 2 shows several voting tools that are used in practice.

[3] Marc Andressen is an American entrepreneur and founder of Netscape.

[4] Miners is a generalized term and they are equivalent the Bitcoin Miners.

[5] In the Bitcoin network, the transactions are grouped in single Blocks every ten minutes on average [25]. Ten minutes is the average time to find a Block. The ten minutes was Nakamoto's choice as a trade-off between first confirmation time and the amount of work wasted due to chain split [26]. However, in other cryptographic currencys, such Litecoin, the transactions are grouped in a single Block every two minutes [20]

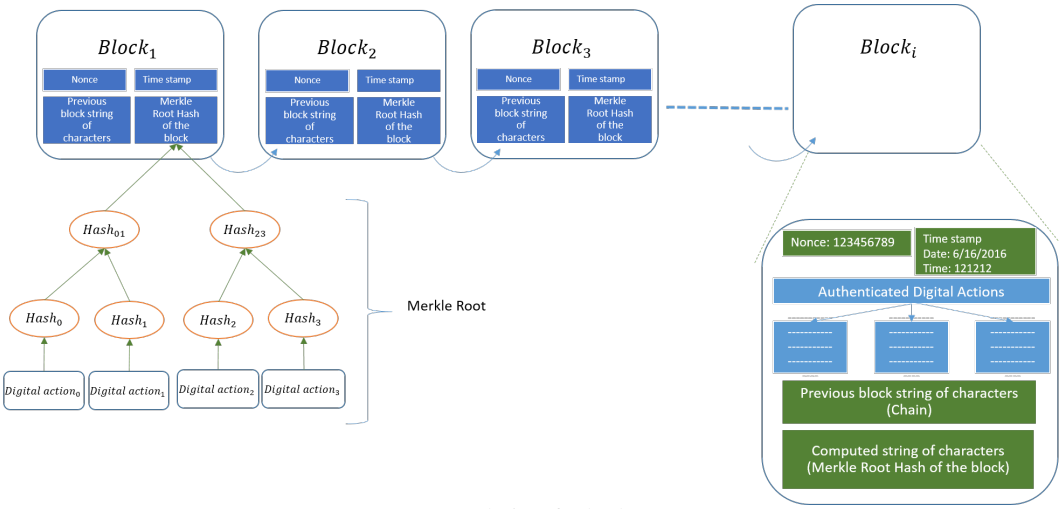

Figure 4. chain of Blocks [20]

Voting tool	Advantages	Disadvantages	Resource	Model
Proof-of-Work (PoW)	-Decentralized control.	-Power and process consumption.	Solving the mathematical puzzle→ processor power → energy consumption	Bitcoin
Proof-of-Stake (PoS)	-Decentralized control. -Low latency. -Ease of rule.	-Lack of flexible trust.	Certificate of Deposit (CD)	NXT (registry, asset exchange, secure messaging, and stake allocation)
Stellar Consensus Protocol (SCP)	-Decentralized control. -Low latency. -Flexible trust	-Manual broadcasting for the root token	Quorum vote (peer standing)	Vumi (Under development)
Ripple consensus algorithm	-Decentralized control.	-Network monitoring	Exceptional node list based on peer reputation	Ripple

Table 2. Shows several voting tools or consensus protocols adopted from [29]

The voting tool is run by a mining software in order to reach consensus among the mining nodes in a network to solve a mathematical puzzle (problem). The most common voting tool is Proof of Work (PoW); it is used in the Bitcoin network and was introduced in 2002 [30]. To validate a Block using PoW, a certain cryptographic hash, including the Block's component, is formed, and must be below a threshold value (miners need to complete a brute-force exploration for a partial hash collision) [31]. This is to guarantee that a Block cannot be altered without doing all the work associated with finding the hash collision [31]. There are other types of voting tools, such Proof of Stack (PoS) [32] and Stellar Consensus Protocol (SCP) [33]. Peercoin is a cryptographic currency that uses PoW as a voting tool and, in addition, can use PoS as an alternative voting tool as well [32]. Vumi is a mobile messaging application, currently under development, that will be built using SCP as its voting tool [34]. Explaining voting tools is beyond the scope of this work and will be left for future work.

Depending on the application of the Block-chain, Miners receive rewards for using their computational power to solve the mathematical problem. For example, in the Bitcoin network the rewards are coins for every new block, in addition to transaction fees from all the transactions within the Block [21]. These rewards motivate the Miners to secure the network, while at the same time executing the distributed monetary system.

4. Enforcement Architecture System

Last section gave an introduction about the Block-chain tecnology. This section will discuss the enforcement architecture in detailed example.

In the past, the FCC assigned static spectrum bands to each user. Using this approach it was possible to prevent most of the interference between users. With the revolution in the

telecommunications industry in the last two decades and the lack of new dedicated spectrum bands, the federal government proposed certain bands to be shared [6, 35, 36]. As discussed elsewhere [2] sharing leads to a reconfiguration of rights relationships among stakeholders, which require enforcement if they are to be viable.

Any rights system requires a set of strategies and technologies to enforce the rights [37] and the timing of the enforcement action (ex-ante and ex-post) plays a significant role [38]. The general characteristics of the enforcement of rights were applied to spectrum sharing in [39]. These characteristics are [37, 39]: 1) enforcement timing action (ex-ante or ex-post); 2) form of the sanctions; and 3) party (ies) carrying out the enforcement.

Shavell [38] argues that the timing of the enforcement action plays an important role in any enforcement regime. Enforcement actions can take place before (potential) interference events (**ex-ante enforcement**), or afterward (**ex-post enforcement**). The spectrum sharing approaches that have been proposed by the NTIA emphasize ex-ante actions, which are designed to prevent a PU's signal from harmful interference that could occur by the SU [6, 39]. A comprehensive enforcement framework would include protecting the rights of the SU as well, in addition to having an ex post component that can efficiently and effectively adjudicate claims of interference. The practical enforcement schemes have ex-ante and ex-post enforcement that are linked together. Thus, the enforcement system would consist of: 1) ex-ante enforcement; 2) ex-post enforcement; 3) and an enforcer. The enforcer could be a third party enforcer or self-reporting enforcement system.

This work considers two architectures for enforcement systems: a third party enforcer and a self-reporting approach [8]. Third party enforcer approach, the enforcer must be trusted by all the entities of the system and must have authority to resolve enforcement violation events [9]. We will examine how these two architecture apply in the enforcement of usage as well as collective action rights. A hypothetical scenario of using the recommended ex-ante enforcement (protection zones) and the involved entities will be used to analyze ex-post enforcement steps and the enforcer role in both architectures. This hypothetical scenario concerns about the behavior of the SUs is significant / of concern if SU-mobile devices transmit near PU-base station or if they are transmitting high power signals within the protection zone. These behaviors will cause harmful interference to the PU signal and data received by the PU will be lost. For the ex-post enforcement, we will follow the graduated-response approach as an ex-post enforcement measure that had been suggested in [10].

4.1 Ex-ante Enforcement

The ex-ante enforcement procedures consist of prevention mechanisms that shape the activity before the harmful interference occurs. Examples of ex-ante enforcement are exclusion zones, protection zones and Signal Interference to Noise Ratio (SINR) limitations. Regulators prefer using an exclusion zone to prevent harmful interference because this is less complicated than other ex-ante enforcement mechanisms. A protection zone is another ex-ante enforcement mechanism, but costs more because it requires coordination between the sharing entities when transmitting within the zone.
The CSMAC-enforcement subcommittee recommended that the NTIA along with the FCC identify the ex-ante measures of the operational and technical guidelines governing the spectrum sharing of federal government bands. These guidelines include interference mitigation and enforcement procedures to provide ample precision for PUs and prospective SUs [40]. The CSMAC-enforcement subcommittee recommended the ex-ante enforcement measures to be applied when sharing the spectrum which are 1) protection zones; 2) SINR limitation to establish the interference threshold.

4.2 Ex-post Enforcement

The ex-post enforcement mechanisms consist of corrective measures after a violation event has occurred. The corrective measures may include penalties (such as fines, product recall, or revocation of licenses) or modifications of rights between parties or other kinds of sanctions (e.g., power penalties, transmission moratoriums, etc.) such as in [41, 42]. In the US, ex-post enforcement measures in spectrum sharing cases are different because the spectrum is going to be shared between Federal/non-federal and commercial usage. And each type of these agencies has a different entity to govern the spectrum usage. Those entities each have different ex-post measures. The entity that governs the Federal spectrum users is the NTIA but has no authority over non-federal users. Conversely, the FCC governs non-federal uses but has no authority over federal spectrum users [40]. That is why we see differences in ex-post enforcement measures between NTIA and the FCC. The CSMAC-enforcement subcommittee report recognized the differences and difficulty of relying on one entity (NTIA or FCC) to govern if a harmful interference event occurred between PU and SUs [40]. It recommended that NTIA and the FCC enter into a new central Memorandum of Understanding (MOU) to govern spectrum sharing rights between federal and non-federal users. By central-MOU, federal and non-federal entities would rely on both the FCC and NTIA to take necessary actions in the event there is a breach of a sharing agreement.

The CSMAC-enforcement subcommittee recommendation related to ex-post enforcement measures were discussed in [10]. It was found that the specific-MOU would framework enforcement rights and proper penalties of the sharing parties. This recommendation will not be an ideal solution because it would be under the umbrella of the Communications Act of 1934[6] and the Forfeiture Proceedings guidelines[7].

[6] Communications Act of 1934 (last visited 9/9/16): https://transition.fcc.gov/Reports/1934new.pdf

[7] Forfeiture Proceedings guidelines(last visited 9/9/16):

4.3 Enforcer

The role of the enforcer would be to detect, adjudicate, and control parties' behaviors. The enforcer must be trusted by all the entities of the system and must have authority to resolve enforcement violation events[9]. The parties could elect the enforcer to resolve both the acceptability of a hypothetical violation event and its costs [9].

In the US, telecommunications agencies can be divided into two types: federal agencies and non-federal commercial agencies. Each type of agency has a different enforcer (entity) to govern spectrum usage. NTIA has authority over federal spectrum users (which are the PU of the spectrum) but has no authority over non-federal users (which are the SU of the spectrum). Conversely, the FCC governs non-federal spectrum use but has no authority over federal spectrum users [40]. As a result, a legal framework for implementing an enforcement function must be developed. The enforcer would govern PU and SU behaviors to 1) guarantee spectrum sharing rights are enforced; 2) and assure that PU will not receive any harmful interference signals from the SU.

The enforcer would need to monitor and detect the interference events that affect the PU's received signal and are caused by the SU's. A sensing system would need to be built around the PU's receiver. The sensor network should be able to detect the aggregate signal energy attributable to the SU's transmitted signal. The sensor antennas would have a range equal to the protection zone ranges depending on the specific sites. If the signal energy is below noise level, it would not be detectable. If the signal energy reaches the noise level, interference would be detected and the enforcer would apply the ex-post enforcement measures recommended by the specific-MOU, such as penalizing the SU.

4.3.1 Third party enforcement system

Third party enforcement system means that the enforcement system would be consist of ex-ante enforcement, ex-post enforcement and enforcer would be a third party. The role of the third party would be to administer the behavior of the sharing entities by policing and enforcing user's rights in the spectrum sharing regime. This governing role means that the third party would prevent, detect, adjudicate to enforce the spectrum sharing policy among the PU and SU to guarantee the users rights. To be able of preventing and detecting and responding to any harmful interference event, the third party would need to:

1. Build a sensor network around the PU antenna. The sensor antennas would have a range equal to the protection zone ranges depending on the specific site. If the signal energy is below noise threshold level, it would not be detectable. If the signal energy reaches the noise level, interference would be detected.
2. Have access to SAS to monitor the spectrum. The access would offer required evidence of interference that might be required for the adjudication, forensic and enforcement steps [40].
3. Trusted by the sharing entity. The enforcer should be able to access the PU and SU communication systems and databases to identify and allocate the violator to collect the proper evidence to help in the adjudication process.

CSMAC-enforcement subcommittee report recommended the NTIA to consider a third party as an enforcer [40]. The third party should pass an appropriate security clearance to govern the spectrum sharing. The main purpose of this recommendation is to reduce the time and capitals required to settle harmful interference event. Additionally, if the interference event occurs and following this recommendation, the NTIA and FCC would not have to detect, forensic, and adjudicate any interference event unless the issue is escalated by the violator.

Currently, the Wireless-Telecommunication system in the US relies on a central authority to manage the spectrum policy. The central authority is dependent on a closed-database that is used to register and approve any end-user. If SAS is built on the same concept as the current management system that has been used in -current Wireless-Telecommunication system, it would be dependent on a central authority to enforce spectrum sharing rights (centralized system); and the same concept of closed-database usages would be repeated and used in the spectrum sharing regime. Such a centralized system with a closed-database would require the third party enforcer to go through a costly security measures to be certified. These certification costs would impact heavily on the cost of the ex-post enforcement. If the cost of the ex-post enforcement is too high, the sharing entity would prefer not to share the spectrum as a result.

4.3.2 Self-reporting enforcement system

Self-reporting approach, PU and SU would report their own activities to spectrum sharing enforcement authority (which could be SAS for this architecture) when they violated the spectrum sharing policy. Following the self-reporting approach, the detection and forensic roles will be deducted from the enforcer because parties report their violation act, in addition, reducing the risk of getting uncertain sanctions when violating the spectrum sharing policy.

CSMAC-enforcement subcommittee report recommended the NTIA to consider voluntary policing where the sharing entities settle the issue without upgrading it to the NTIA or FCC [40]. This recommendation would deduct the detection and forensic roles from the enforcer because parties report their violation act which would reduce the cost of ex-post enforcement as a result comparing to the cost of the ex-post enforcement without the self-reporting approach. In addition, following this recommendation would reduce the risk of getting uncertain sanctions when violating the spectrum sharing policy.

Unfortunately, the recommendation of using a third party

http://www.ecfr.gov/cgi-bin/text-idxSID=6c4588fbf26be630b7d3ce1862fbee3e&mc=true&node=se47.1.1_180&rgn=div8

only as an enforcer is costly comparing to the self-reporting enforcement. The CSMAC-enforcement subcommittee recommended to combine the two approaches (self-reporting enforcement and third party enforcer) as an ideal solution to resolve any interference event [40]. Following this recommendation by combining the self-reporting enforcement and third party enforcer, would not ultimately reduce the cost of the ex-post enforcement because the enforcement system (which is SAS) would be built on a centralized scheme with a closed-database. In addition, it would not reduce the the adjudication process costs too.
There is an alternative and better solution equivalent to the combination approach between the third party enforcer and self-reporting enforcement. The approach is by automating enforcement system in the spectrum sharing regime. Automated enforcement system would reduce the cost of the adjudication process [7]. In the past, the ways of automating the enforcement system were costly and not feasible. The following section will discuss the structure of the automated enforcement systems and its requirements.

5. Toward The Structure of Automated Enforcement Systems

The design of an automated enforcement system must begin with the end goal: reliable evidence to support a predicable and well defined adjudication process. Evidence in support of a claim might include the documentation of an interference event, which could include the location, time and date where the event was detected, locations of the transmitters and receivers that are affected by the event, the transmission history of the transmitters in the area, other parameters, such as antenna type and height, etc. For spectrum sharing systems that use a database driven spectrum management system, such as a Spectrum Access System (SAS), the transaction history of the SAS is also critical. ***Reliable*** evidence means that all parties are satisfied with the provenance of the information that enters the adjudication process. The rest of the paper will discuss a current technology that if used in the spectrum sharing regime, it would be possible to automate the enforcement system that is encountered with feasible proper costs. This technology is called a Block-chain.

6. Block-chain Potential Applications to Spectrum Sharing Systems

According to Adam Ludwin[8][43]:
"A blockchain is a database ... but it is different from a traditional database in two critical ways. First of all it is shared, so in other words it is distributed to every participant ... in the network. ... [T]he critical difference ... is that in a blockchain, the assets are controlled by the owners of the assets, whereas in a traditional database, the assets are controlled by whoever owns the database. So, it's a system whereby the asset owners retain control all the time over their assets even as we're using a data model in a network to transact."
In this context, let us consider spectrum sharing systems. At a high level, users transact to acquire transmission rights at some price. In most cases, the users construct infrastructure to use the transmission rights for some kind of information transfer application. Spectrum as an economic good has the property of being instantly renewable, which is also the property that makes interference such a significant issue. In this part, we will discuss the implication and limitation of employing the Block-chain to the spectrum sharing regime

6.1 Ex-post Enforcement using Block-chain as Publicly-Distributed-Database

As mentioned, the Spectrum Access System (SAS) be responsible for enforcement mechanisms on the spectrum sharing policy. The Block-chain technology is publicly-distributed-database that could be used for Spectrum Access System (SAS). If the Block-chain is used as the publicly-distributed-database for SAS, it will enable the requirement of enforcing the collective action rights or the interference rights in spectrum sharing systems. If the Block-chain technology is deployed in the spectrum sharing regime to enforce the user's rights, it would serve as a publicly-distributed-database. The Block-chain is empowered by cryptographic methods that will: 1) allow it to function without any central authority, 2) guarantee trust and reliability of the digital actions within the database.
The Block-chain would expedite some of the ex-post enforcement processes. Because the database would be distributed and stores around all the participated nodes (PU, SU, and the enforcer). As an example, the enforcer would not find difficulties to gather the evidence because the data resides and distributed among all the entities. Additionally, self-reporting approach would be applicable when using the Block-chain technology. And the sharing entities could avoid any uncertain sanctions by following this approach.

6.2 Ex-post Enforcement using Smart Contract

Further, the smart contract application is another decentralized application that can be used in the suggested spectrum sharing regime. A Time Limited Lease (TLL) was proposed to be used in the spectrum sharing regime to enforce the rights between the sharing entities [44]. The idea is similar to a smart contract, but different in the implementation. Where the TLL relies on a hardware to be self-executed, while the smart contract relies on a software application to be self-executed.
The smart contract application took the Block-chain implementation further than using a digital action as simple trades. As such, the digital action could contain more embedded information when used in the smart contract. It would become much easier to record, confirm, and execute the smart contract when using the Block-chain technique under the smart contract application. If the smart contract is used in the suggested spectrum sharing regime, it can substitute any third party provision of, such as lawyers to set up contracts, or

[8] Adam Ludwin is the co-founder of Chain enterprise

financial institutions to guarantee payment, or enforcers to apply the ex-post measures against the violators. The role of the ex-post enforcement was examined and evaluated in a cooperative spectrum sharing scheme [45, 10]. It was shown that the cost of the ex-post enforcement plays a significant role since sharing the spectrum will without doubt result in interference events. The cost elements of the ex-post enforcement may play an important role to effect on sharing parties' decision [45]. If the smart contract is used in the spectrum sharing regime, it might have significant impact on the cost of the ex-post enforcement. Part of the ex-post enforcement cost is the changeable enforcement cost. This changeable enforcement cost ranges from attributing interference to the appropriate party and penalizing the interferer, to collecting the penalties. Employing the smart contract to execute the ex-post enforcement mechanisms automatically would expedite, and ease the process of the ex-post enforcement which would lower the changeable enforcement costs to be almost negligible. The implication on the ex-post enforcement would generate an economic incentive for the entities to share the spectrum.

6.3 Ex-post Enforcement as DAO

The most efficient approach to deploy the ex-post enforcement in the spectrum sharing regime is by automating the adjudication [46]. The full-automated-nodes or the automatic scheme can be achieved by integrating two decentralized applications, such as smart contract and cryptographic currency. The automatic scheme might have major impact on the spectrum sharing regime if it is used to enforce the spectrum sharing rights between the sharing entities. Combining those two applications may facilitate the automation of Machine-2-Machine (M2M) communication and interaction without the need of the human intervention. If this approach is used in the spectrum sharing regime between the PU and SU, it would be the most efficient approach for automating the adjudication in the spectrum sharing that has been suggested [46]. Also, it would guarantee the income stream for the PU, and expedite, and ease the process of the ex-post enforcement when the spectrum sharing rights are violated [45]. This method of automatization would have incentives from many perspectives, such as resource benefits and economic incentives. However, the economic incentives will not be applicable if the spectrum sharing policy is not supporting it [10]. The automatization method would be a further step to show the spectrum sharing policymaker the economic, and resource incentives to share the spectrum.

One of the challenges for the Block-chain technology that is lacks of standardized processes in the Block-chain's implementations. This makes it difficult for the technology to be adopted into the market. Additionally, because the Block-chain technology is still in the research development stage, it is hard to explain and even more difficult to specify how it can be used in a system as publicly-distributed-database unless the concept of the system is well explained. When using PoW as a voting tool, the power and process consumption may also become a limitation when used with devices that had limited processors and power. This limitation can be avoided if another voting tool, such PoS is used.

7. Conclusion

Interference rights and collective action rights enforcement are necessity in spectrum sharing regime. Spectrum Access System (SAS) was suggested by the CSMAC to facilitate the enforcement mechanisms of these rights. Also, the collective action rights require transparency. If SAS is built on the same concept as the current management system that has been used in Telecommunications, it will be dependent on a central authority to enforce spectrum sharing rights (centralized system); and the same concept of closed-database usages will be repeated and used in the spectrum sharing regime.

As we move to more intensive sharing of spectrum, the likelihood of events that are enforceable ex post increases, despite ex ante measures. The Enhancing Access to the Radio Spectrum (EARS) second workshop report [1] recognized this and set the goal of lowering the costs by automating some of the ex-post enforcement steps.

We introduced the Block-chain technology to be used for SAS to facilitate the requirement of enforcing the collective action rights as well as the interference rights in spectrum sharing systems. Block-chain is a technology is a publicly-distributed-database that can be used in any system. It can be defined as a resilient, reliable, transparent and decentralized way of storing and distributing a database across all nodes of a network.

Block-chain technology to automate the ex-post enforcement processes. The potential usages can be divided into three applications: 1)ex-post Enforcement using Block-chain as Publicly-Distributed-Database, 2) ex-post Enforcement using Smart Contract, 3) and ex-post Enforcement as Decentralized Autonomous Organization (DAO). If Block-chain technology is used for SAS as publicly-distributed-database, it would create the opportunity of spectrum sharing regime to be open, reliable, and democratic.

The spectrum sharing policymaker could decide to use further decentralized application that benefits from using the Block-chain technology, such as a smart contract application. It becomes much easier to record, confirm, and execute the sharing rights between the PU and SU's. This would create economic incentives for the entities to share the spectrum.

Further, The spectrum sharing policymaker could decide to use further decentralized application that benefits from using the Block-chain technology, such as a smart contract application. Doing that, It would be easier to record, confirm, and execute the sharing rights between the PU and SU's. This would create economic incentives for the entities to share the spectrum. The possibility of automating the ex-post enforcement by deploying the M2M approach was discussed. The automatization method will be a further step to gain more economic incentives, and resource benefits.

Exploring how Block-chain could support other functional

groups of Spectrum Access System (SAS) and looking at SAS architecture will be on future work.

References

[1] EARS committee members. Final report: The second enhancing access to the radio spectrum workshop. Technical report, A National Science Foundation, 19-20 October 2015.

[2] M. B. H. Weiss, W. H. Lehr, A. Acker, and M. M. Gomez. Socio-technical considerations for spectrum access system (sas) design. In *Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on*, pages 35–46, Sept 2015.

[3] Lisa Shay, Woodrow Hartzog, John Nelson, and Gergory Conti. Do robots dream of electric laws: An experiment in the law as algorithm. In *Stanford Law Conferences: We Robot, Getting Down to Business*.

[4] Harold Demsetz. The exchange and enforcement of property rights. *Journal of Law and Economics*, 1964.

[5] Steven Shavell. The optimal structure of law enforcement. *Journal of Law and Economics*, 36(1):255–287, 1993.

[6] Gary Locke, LE Strickling, and A Secretary. An assessment of the near-term viability of accommodating wireless broadband systems in the 1675-1710 mhz, 1755-1780 mhz, 3500-3650 mhz, and 4200-4220 mhz, 4380-4400 mhz bands. *U. S. Department of Commerce, Washington, DC, October*, 1, 2010.

[7] Mohammed Altamimi, Martin B.H. Weiss, and Mark McHenry. Enforcement and spectrum sharing: Case studies of federal-commercial sharing. In *Telecommunications Policy Research Conference*, September 2013.

[8] Louis Kaplow and Steven Shavell. Optimal law enforcement with self-reporting of behavior. *Journal of Political Economy*, 102(3):583–606, 1994.

[9] Coleman Bazelon. The economic basis of spectrum value: Pairing aws-3 with the 1755 mhz band is more valuable than pairing it with frequencies from the 1690 mhz band. *The Brattle Group, Washington DC*, 2011.

[10] Amer Malki and Martin BH Weiss. Ex-post enforcement in cooperative spectrum sharing: A case study of the 1695-1710 mhz band. In *Telecommunication Policy Research Conference (TPRC43)*. TPRC, 2015.

[11] Liu Cui, Marcela M Gomez, and Martin BH Weiss. Dimensions of cooperative spectrum sharing: Rights and enforcement. In *New Frontiers in Dynamic Spectrum Access Networks*. IEEE, April 2014.

[12] Munawwar M. Sohul, Miao Yao, Taeyoung Yang, and Jeffrey H. Reed. Spectrum access system for the citizen broadband radio service. *IEEE Communications Magazine*, 53(7):22–28, 2015.

[13] Melanie Swan. *Blockchain: Blueprint for a New Economy*. " O'Reilly Media, Inc.", 2015.

[14] Nachiappan Pradhan Pattanayak Sanjeev Verma Crosby, Michael and Vignesh Kalyanaraman. Blockchain technology beyond bitcoin. Technical report, Sutardja Center for Entrepreneurship Technology Technical Report. UC Berkeley, 16 October 2015. Accessed: 05-31-2016.

[15] Saad Hirani. World's largest banks and corporations back blockchain. `http://scet.berkeley.edu`, 22 February 2016. Accessed: 5-31-2016.

[16] Pete Rizzo. Chain issues investor shares on nasdaq blockchain platform - coindesk. `http://www.coindesk.com`, 2015. Accessed: 6-16-2016.

[17] Jacob Stenum Czepluch, Nikolaj Zangenberg Lollike, and Simon Oliver Malone. The use of block chain technology in different application domains. 2015.

[18] Aaron Wright and Primavera De Filippi. Decentralized blockchain technology and the rise of lex cryptographia. *Available at SSRN 2580664*, 2015.

[19] Nick Szabo. Formalizing and securing relationships on public networks. *First Monday*, 2(9), 1997.

[20] Richard Caetano. *Learning Bitcoin: embrace the new world of fiance by leveraging the power of cryptocurrencies using Bitcoin and the Blockchain*. Packt Publishing, Birmingham, 2015.

[21] Andreas M Antonopoulos. *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.", 2014.

[22] Sean Pearl. Distributed public key infrastructure via the blockchain. 2015.

[23] Vitalik Buterin. A next-generation smart contract and decentralized application platform. *White Paper*, 2014.

[24] Michael Miller. *The ultimate guide to Bitcoin*. Pearson Education, Indianapolis, Indiana, first edition, 2014.

[25] George Foroglou and Anna-Lali Tsilidou. Further applications of the blockchain.

[26] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[27] Lorne Lantz. New kids on the blockchain. `https://www.youtube.com/watch?v=A1Vbrxkqjwc`, 2016. 6-15-2016.

[28] Virtual currency schemes. `https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf`, October 2012. Accessed: 5-25-2016.

[29] Juri Mattila. The blockchain phenomenon. *Berkeley Roundtable on the International Economy (BRIE)*, 2016.

[30] Adam Back et al. Hashcash-a denial of service countermeasure, 2002.

[31] Daniel Kraft. Difficulty control for blockchain-based consensus systems. *Peer-to-Peer Networking and Applications*, pages 1–17, 2015.

[32] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, 19, 2012.

[33] David Mazieres. The stellar consensus protocol: A federated model for internet-level consensus. *Draft, Stellar Development Foundation, 15th May, available at: https://www. stellar. org/papers/stellarconsensus-protocol. pdf (Accessed 3rd June, 2016)*, 2015.

[34] Vumi for developers. `http://vumi.org/developers/`. Accessed: 6-17-2016.

[35] Paul Kolodzy and Interference Avoidance. Spectrum policy task force. *Federal Commun. Comm., Washington, DC, Rep. ET Docket*, (02-135), 2002.

[36] US Federal Communications Commission et al. Promoting efficient use of spectrum through elimination of barriers to the development of secondary markets, report and order and further notice of proposed rulemaking, wt docket no. 00-230, oct 2003.

[37] Harold Demsetz. The exchange and enforcement of property rights. *Journal of law and economics*, pages 11–26, 1964.

[38] Steven Shavell. The optimal structure of law enforcement. *Journal of Law and Economics*, pages 255–287, 1993.

[39] Mohammed Altamimi, Martin BH Weiss, and Mark McHenry. Enforcement and spectrum sharing: Case studies of federal-commercial sharing. *Available at SSRN 2310883*, 2013.

[40] Commerce Spectrum Management Advisory Committee (CSMAC). Enforcement subcommittee report. Technical report, NTIA, 12 May 2015.

[41] Kate Harrison and Anant Sahai. Potential collapse of whitespaces and the prospect for a universal power rule. In *New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2011 IEEE Symposium on*, pages 316–327. IEEE, 2011.

[42] Kristen Ann Woyach, Anant Sahai, George Atia, and Venkatesh Saligrama. Crime and punishment for cognitive radios. In *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pages 236–243. IEEE, 2008.

[43] Private Interview with Adam Ludwin. a16z podcast: Blockchain vs./and bitcoin. `https://a16z.com/2015/11/11/blockchain-bitcoin-fintech`, 11-11-2015. Accessed: 5-6-2016.

[44] John M Chapin and William H Lehr. Time-limited leases for innovative radios. In *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, pages 606–619. IEEE, 2007.

[45] Amer Malki and Martin BH Weiss. Ex-post enforcement in spectrum sharing. In *Telecommunication Policy Research Conference (TPRC42)*. TPRC, 2014.

[46] Mohammed Altamimi, Martin BH Weiss, and Mark McHenry. Enforcement and spectrum sharing: Case studies of federal-commercial sharing. *Available at SSRN 2310883*, 2013.

[47] Best bitcoin congressional hearing - bitcoin in washington - digital currency talks. `https://www.youtube.com/watch?v=buFpCvTNqvg`, 2013. Accessed: 5-20-2016.

[48] Matthew Ponsford. A comparative analysis of bitcoin and other decentralized virtual currencies: Legal regulation in the people's republic of china, canada, and the united states. *Canada, and the United States (January 22, 2015)*, 2015.

[49] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks*, pages 197–223. Springer, 2013.

[50] L Jean Camp, Marvin A Sirbu, and J Doug Tygar. Token and notational money in electronic commerce. In *Usenix Workshop on Electronic Commerce*, 1995.

[51] Danny Yuxing Huang. Profit-driven abuses of virtual currencies. *University of California, San Diego*, 2013.

[52] Axel Hauduc. A diagnosis of bitcoin and its future. *Medium*, 05 May 2014.

[53] David S Evans. Economic aspects of bitcoin and other decentralized public-ledger currency platforms. *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper*, (685), 2014.

[54] Björn Segendorf. What is bitcoin. *Sveriges Riksbank Economic Review*, 2:71–87, 2014.

[55] P. Baran. On distributed communications networks. *IEEE Transactions on Communications Systems*, 12(1):1–9, March 1964.

[56] Ingrid Lunden. Ibm raises its blockchain game with secure cloud services and docker integration. `http://techcrunch.com/2016/04/29/ibm-blockchain/`, 29 Apr. 2016. 5-02-2016.

[57] Paul JM Havinga, Gerard JM Smit, and Arne Helme. *Survey of electronic payment methods and systems*. 1996.

[58] What is bitcoin? introductory video and current price. `https://www.weusecoins.com/`. Accessed: 5-20-2016.

[59] Ping Wah Wong. A public key watermark for image verification and authentication. In *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*, volume 1, pages 455–459 vol.1, Oct 1998.

[60] Zulfikar Ramzan. Bitcoin - proof of work. `https://www.youtube.com/watch?v=9V1bipPkCTU&`

list=PLQb8htRul9xAz70xZUmqxX_oPe3_rz-PJ&index=7, 5-01-2013. Accessed: 6-16-2016.

[61] Contract, law.com legal dictionary. http://dictionary.law.com/default.aspx?selected=337. Accessed: 6-18-2016.

[62] Bill Maurer. Bitcoin transaction details - part 1. https://www.youtube.com/watch?v=Em8nJN8IEes, 06 July 2014. Accessed: 6-17-2016.

Appendix A

Block-chain Technology

After the internet become available to the public in the 1990s, money itself, and the methods of transferring it, converted to electronic form. Cryptographic currency was introduced as a new electronic[9] form of money, which represented the cash equivalent of transferring physical currency between hands. Cryptographic currency (equivalent to cash) can be issued, or produced, based on either centralized or decentralized currency systems, such as Bitcoin, Ripple, Litecoin, WebMoney or Dogecoin. Cryptographic currency is preferable to users for the following reasons [47]:

1. Enables the user to stay relatively anonymous
2. Easy to navigate
3. May have low fees
4. Is accessible across the globe with a simple internet connection
5. Can be used to store and make international transfer value
6. Does not typically have transaction limits
7. Generally secure
8. Features irreversible transactions

There are 500 selections of decentralized cryptographic currencies[10] available on the internet [48]. Bitcoin is one of the most popular and famous cryptographic currencies, and it is produced based on a decentralized currency system. It was introduced by Satochi Nakamoto (pseudonym) in 2008 [26]. Bitcoin is a digital coin[11] that operates on a peer-to-peer network [49, 50, 51, 48, 52, 53]. This means that every node that runs a Bitcoin client is in charge of keeping track of all the transactions, regulating the money supply, and supplying currency. Bitcoin transactions are based on cryptographic proof, instead of trust, by permitting any two agreeable nodes to transact openly with each other without needing a trusted third party. It is not dependent on a central entity (such as a central bank) to be produced, stored, or distributed. Bitcoin not only acts as cash and payment, but can also symbolize countless kinds of property.

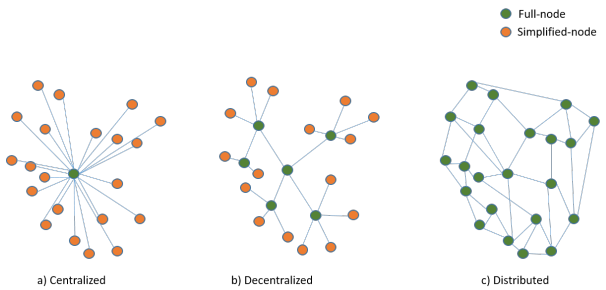

Figure 5. Centralized, decentralized, and distributed database concepts that is adopted from Paul Baran communication network classification [55].

Bitcoin was introduced as a cryptographic currency that takes advantage of encryption methods to generate currency units and approve transactions. It does not represent anything other than a number [54]. A person can get a Bitcoin by: 1) exchanging physical currency (for example, $ US dollar, or Euro), or 2) by using his computer to mine and be rewarded. Mining is the process of using the computational processing work of a person's computer to solve a mathematical problem. Bitcoin practices an exceptional and innovative strategy for keeping and allocating its operation record [20]. To generate a distributed database of operations that is both robust and clear, it allocates all operations through all network's nodes [20]. The distributed-database is called Block-chain. The reason for using the Block-chain technique in Bitcoin was to avoid double spending [26]. The importance of Block-chain came from the concept of a decentralized system to replace the absolute centralized ones (and the middlemen) [56].

The concept of a distributed scheme is related to computer engineering, and differs from centralized and decentralized systems (see Figure 5) [55]. When we say distributed database, we follow the concept in Figure 1-c that means that all the nodes have the same authority and privileges. And when a system is called decentralized, as in Figure 1-b, it means some of the nodes have all the privileges, and some are simple nodes that have no authority. In general, Block-chain is a distributed system, but the applications are used for decentralized systems, such Bitcoin and smart contracts. This is because the applications are designed to run on power and space constrained devices where the new era of devices, such smartphones, tablets, or embedded systems, lack these features [21]. A copy of the publicly-distributed-database is maintained and shared in every node on the Bitcoin network and is agreed upon by means of a proof-of-work system. Block-chain technique relies on a digital signature to provide a public history of transactions to prevent double-transactions [26]. Block-chain

[9] The idea "electronic money" is an electronically deposited money value that symbolizes a right on the developer (the value it equals is no more than the amount it was paid for), and is accepted by parties other than the developer [28]. The cryptographic currency, to date, is accepted within a specific digital world, unregulated, the supply of money varies, not guaranteed for cashing the fund, unsupervised, and has many types of risk. That means the cryptographic currency scheme can be considered a specific type of electronic money that is the cash equivalent of transferring electronic money.

[10] "Digital currency", "virtual currency", "Crypto currency", and "cryptographic currency" are all terms used for the cash equivalent of transferring electronic money. In this paper, we use the term Cryptographic currency.

[11] Digital coin or digital token are both general terms for a Bitcoin unit. In this paper, we will use the term digital token. The digital token is nothing other than a unique number that cannot be replicated and is generated using the cryptographic method.

is the database in Bitcoin, and is responsible for storing and distributing all Bitcoin's transaction ledgers to all the nodes in the Bitcoin network [49, 50, 51, 48, 57]. This database is [58]: 1) open, 2) has decentralized authority, 3) is public, and 4) is accessible in one digital record through the network. The Block-chain records all transactions that contain a date, time and participants, and stores the value of each transaction [58]. The idea of Bitcoin's Block-chain could be generalized because the Block-chain does not care whether the digital token (Bitcoin unit) represents currency, value, or property. The application can only decide on the representation of the digital token [58]. For example, smart contracts use the same framework as Bitcoin by generalizing Block-chains to build its application [23].

The Block-chain technique uses cryptographic techniques to improve its reliability and functionality without the need for a central trusted authority [20]. The Block-chain technique was used in the late 1990s for different applications such as in "A public key watermark for image verification and authentication" [59], but it started to get famous and stood out when it was introduced to support the Bitcoin [17]. The Block-chain technology replaced the central authority, such banks by a scattered consensus model. Block-chain uses a scattered consensus model where a minimum number of nodes within the network should approve the transaction (digital action). To authenticate any transaction, there is a minimum number of nodes needed to practice the authentication procedures and ensure transaction is right. The involved nodes in the authentication process are called Bitcoin Miners. Any suspicious transaction will be rejected by the Bitcoin Miners if they do not authenticate it.

Block-chain is a promising technology that can be used as a publicly-distributed-database in any network [43], and it may have more usage in the near future [17]. When using Block-chain technology, the database is stored in each node connected to the network [13]. It is used to store and distribute any action in the network to all the nodes. Depending on the action or application that it is needed for, Block-chain can be used as a technology by itself or can be used to support other technologies.

In the last two years in the United States, over $00 million has been invested in Block-chain associated technology [15]. In addition, some of the largest financial companies funded startup corporations to find Block-chain applications to be applied on Wall Street [15]. In fact, in 2015, the National Association of Securities Dealers Automated Quotations (NASDAQ) lunched the Linq platform, based on Block-chain technology, from the startup Chain to trade non-public shares [16]. IBM and Samsung are experimenting with Block-chain technology to power the Internet of Things (IoT) [17]. Swan named the Block-chain as the fifth most disruptive computing paradigm after mainframes, PCs, the internet, and mobile/social networking [13]. Andressen[12] elected the Block-chain technique as the most important invention since the internet itself [17, 18].

Block-chain is used as a supportive technique for Bitcoin [13]. Smart contract is another example of using Block-chain as a supportive technology to implement and monitor contract terms [14]. Nick Szabo proposed the idea of a smart contract [19], but was not well-known until the emergence of cryptographic currency [14]. Block-chain takes advantage of cryptographic methods to guarantee both trust and reliability of the blocks. The Block consists of digitally signed actions that are approved by the network. Each Block contains a reference to its ancestor Block to form a Block-chain. Block-chain technology can be used to support many types of applications (financial, economic, market, cash transactions, government, health, or science) [13].

How does Block-chain work?

Caetano [20] identified the Block-chain as a data structure or a chain of blocks interconnected to form a public file that records all digital action for a system. The digital actions are clustered into blocks, broadcast to all nodes of a network, and authenticated by a network of nodes. The acceptance of the block would be determined based on the consensus of the network of nodes. Crosby et al. [14] described the general idea of a Block-chain. They did so by showing that the steps of conducting a transaction in the Bitcoin network connected the Block-chain to the Bitcoin (see Figure 6). In the Bitcoin network, the approved transactions use cryptographic evidence as a substitute for a trusted central authority (such as a bank) to complete the transaction through the network. The transaction is guarded by a digital signature using the $Private_{key}$ of the sender and can be confirmed using the $Public_{key}$ of the sender. The transaction is broadcast to all nodes on the Bitcoin network. The mining nodes (Miners) approve the transaction by [14]: 1) confirming the digital signature of the sender, which verifies the sender owns the cryptographic currency, 2) inspecting each transaction that has been conducted by the sender through the publicly-distributed-database to verify the sender has sufficient funds in his account. After that, the Miners record the transaction on the Block-chain (publicly-distributed-database).

However, following these steps does not prevent the double-spending problem because the transactions do not propagate through the network and reach the destination in the order in which they are made. In other words, there was a necessity to develop a technique to make sure that the whole network agrees on the order of the transactions. The technique that was developed is the Block-chain technique that was introduced to support Bitcoin transactions and prevent double spending issues [14].

The transactions that happen at around the same time are grouped in a Block [14]. Each block is interconnected to the former one by referencing the former block's hash. Hash is a function that uses a cryptographic algorithm that can produce a fingerprint (small unique string of characters) for a file (see Figure 7) [20]. If any changes happen to the file, the fingerprint will be changed. In a Block-chain, the finger-

[12]Marc Andressen is an American entrepreneur and founder of Netscape.

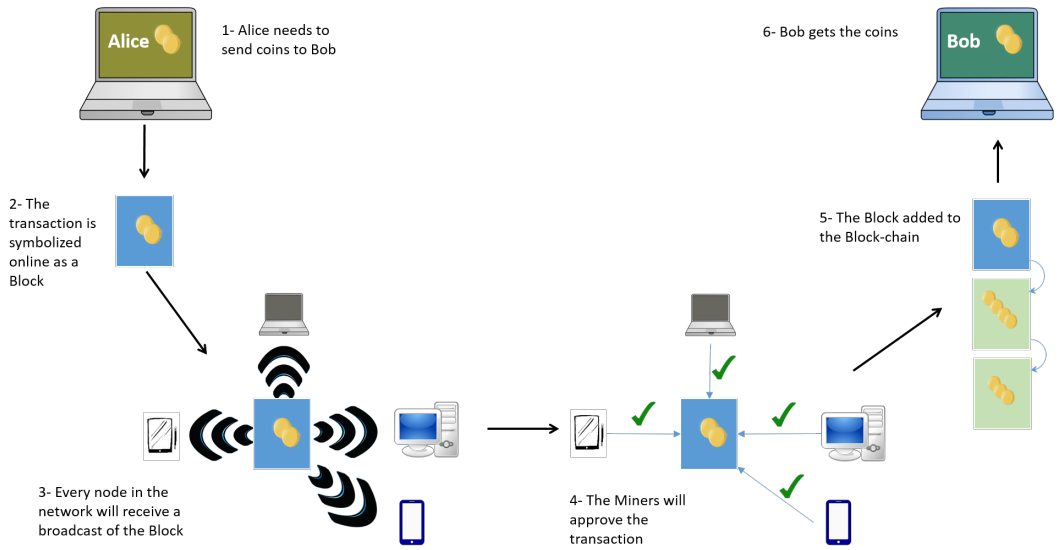

Figure 6. How the Block-chain works in the Bitcoin network [14]

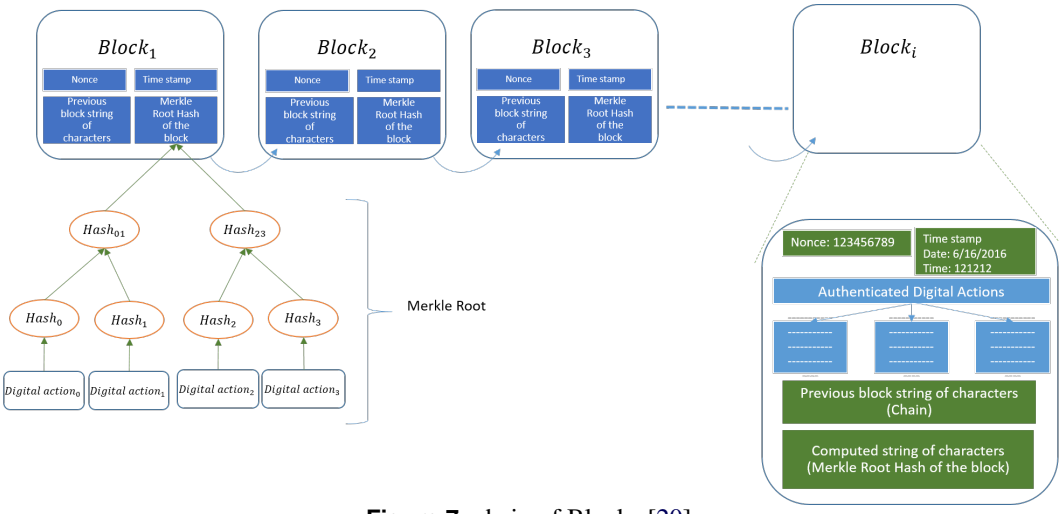

Figure 7. chain of Blocks [20]

print is added to the block and its transactions, along with the fingerprint of the previous block. The fingerprints are then used to provide authorization of the block. The outcome is a distributed and cryptographically protected database of digital actions.

The Block-chain is simply a chain of Blocks that represent a public ledger stored and distributed among all the nodes of a network. Depending on the application that it is used for, a Block records all the digital actions between the nodes of a network, which contain the date and time, and a reference to its ancestor Block [17]. Figure 7 shows how the Block-chain is interconnected from the first Block to the last one and the assembly of the Block. The Block consists of a header, Block size, digital action counter, and list of digital actions [21]. The digital action contains contributors, the date, time, and activity. In Bitcoin, the average size of the digital actions (transactions) is, at a minimum, 250 *bytes*; and the average Block holds over 500 digital actions, while the header size is fixed to 80 *bytes* [21]. The header fields of each Block are a time stamp, nonce, a hash of previous Blocks, and Merkle root [22]. The time stamp is the approximate creation time of the Block. The nonce is a counter used to ensure each digital action is only handled one time [23]. The hash of the previous Block is used to link this block to the prior one to construct the chain of Blocks. The Merkle root is the Hash of the Block (Block's fingerprint). It is a digest of all the transactions in the Block [21]. The Merkle root is used to verify the integrity of the Block. As shown in Figure 7, the Merkle root is created by repeatedly digesting pairs of digital actions until there is one root hash [21].

Mining and Consensus

In the previous subsection, we covered how the Block-chain works and why it was introduced to overcome the problem of double-spending. However, there is another issue, which is

as follows: any node in the network can collect unconfirmed digital actions, create a Block, and announce it to the rest of the network to be eligible to be added to the Block-chain [14]. This raises some concerns, notably: 1) which Block would be succeeding in the Block-chain and how would a network agree on it? 2) The Block could come in different sequences through different nodes in the network leading to a loss of reliability of the Block-chain sequence. 3) The Blocks could be created at the same time. To overcome these matters, mining mechanisms and consensus models between the network's nodes was introduced.

Mining

When a new digital action needs to be validated and added to the Block-chain, the Mining procedure is used [21]. It is used to protect the Block-chain against falsified digital actions (such as double-spending in a Bitcoin network or void signatures) [21, 24]. Miners[13] authenticate new digital actions and add them to the publicly-distributed-database [21]. Digital actions are grouped into a single Block and are validated periodically[14]. However, in other cryptographic currency such Litecoin, the transactions are grouped in a single Block every 10 minutes [20]. Miners compete amongst each other to find a solution to intensive and pressing mathematical puzzles [27]. The greater the processor's power the miners put in, the greater the chance of finding the solution and wining. If a miner solves the mathematical puzzle, the miner broadcasts the Block of the digital-actions to all the nodes of the network to be approved. This approval step is called Consensus model. All the other nodes in the network check the Block to verify that the miner solved the Mathematical puzzle. If more than fifty percent of the nodes agree, that Block of digital-actions is added to the Block-chain [27].

Mining is the process of solving a challenging mathematical problem (mathematical riddle) based on the cryptographic hash algorithm. Miners participate to solve the mathematical problem by applying the Hash function to the block header frequently by changing one parameter until the outcome string of characters matches a certain goal [21]. The mining process is achieved by harnessing the computing power of the Miners to discover valid Blocks [28].

To solve the mathematical problem, mining software runs the voting tool in order to reach consensus between the nodes. The most common voting tool is Proof of Work (PoW); it is used in the Bitcoin network and was introduced in 2002 [30]. To validate a Block using PoW, a certain cryptographic hash, including the Block's component, is formed, and must be below a threshold value (miners need to complete a brute-force exploration for a partial hash collision) [31]. This is to guarantee that a Block cannot be altered without doing all the work associated with finding the hash collision [31]. There are other types of voting tools, such Proof of Stack (PoS) [32] and Stellar Consensus Protocol (SCP) [33]. Peercoin is a cryptographic currency that uses PoW as a voting tool and, in addition, can use PoS as an alternative voting tool as well [32]. Vumi is a mobile messaging application, currently under development, that will be built using SCP as its voting tool [34]. This paper will use PoW as the voting tool and will explain it in greater detail (see section 5.2.3). Explaining other voting tools is beyond the scope of this work and will be left for future work.

Depending on the application of the Block-chain, Miners receive rewards for using their computational power to solve the mathematical problem. For example, in the Bitcoin network the rewards are coins for every new block, in addition to transaction fees from all the transactions within the Block [21]. These rewards motivate the Miners to secure the network, while at the same time executing the distributed monetary system.

Consensus model

Caetano mentioned that, by nature, any network can be made up of good or bad nodes [20]. The good nodes only agree to take valid digital actions and refuse unacceptable digital signatures (such as double-transactions in a Bitcoin network). The bad nodes can be defined as a node that agrees to take corrupted digital actions or chooses to refuse other digital actions. The consensus among the nodes of the network is used to separate and discard the bad nodes. Also, the consensus among the nodes of the network controls a Block's acceptance. If the network's nodes do not reach an agreement on a Block, this Block is corrupted and will be counted as an orphan. A fork in the Block-chain is a result of finding a corrupted Block.

The Block-chain consensus model requires all nodes in the network to come to an agreement on adding a new block of the digital actions, since there is no central authority that can make the choice [17]. The Consensus model is a democratic agreement process used between the Miners to authenticate or reject the digital actions. The digital actions are authenticated by a network of nodes called Miners using cryptographic techniques to: 1) sustain the record book, and 2) ensure that the Miners agree on the recent state of the public record and every digital action in it [58]. Miners are the nodes that validate new digital actions by using computational power to solve a mathematical riddle. Whenever a solution is found, a new Block is validated and attached to the Block-chain [31]. The Miners will reject any suspicious activity if they do not get approval from all the participating nodes. The Democratic consensus process (Consensus model) between the Miners can be compared to the notarization process, which means there is a notary for every transaction [58]. This is why Block-chain is trusted; there is a guarantee that a Block cannot be altered without redoing all the work involved in finding the hash collision.

The consensus model occurs from the interaction of the fol-

[13] Miners is a generalized term and they are equivalent the Bitcoin Miners.

[14] In the Bitcoin network, the transactions are grouped in single Blocks every ten minutes on average [25]. Ten minutes is the average time to find a Block. The ten minutes was Nakamoto's choice as a trade-off between first confirmation time and the amount of work wasted due to chain split [26]. However, in other cryptographic currencys, such Litecoin, the transactions are grouped in a single Block every two minutes [20]

lowing practices [21]:

1. Each node verifies each transaction independently. This verification occurs when a list of measures are met.
2. Miners combine the new transactions independently plus proof-of-work which is a solution to the PoW algorithm.
3. Nodes verify the new Blocks independently and then add it to the Block-chain.
4. Each node selects independently a chain with the maximum increasing computation confirmed through PoW

7.0.1 Proof-of-Work (PoW)

A Proof-of-Work algorithm shows that the miners involved a significant amount of computational energy and, on the other side, it can be easily verified [60]. Proof-of-Work uses SHA-256 to generate a unique hash value for each block in the Block-chain [26]. By linking the hash of a new block to the hash of the prior block in the chain through all the previous baths to the hash of the origin block, then the connectivity of the Block-chain is succeeded.

As mentioned, *SHA-256* takes variable size input-data and generates 64 hexadecimal digit number which is called a fingerprint for the input-data. If a number is added to the input-data, a different fingerprint would be generated (see Figure 8) [21]. Figure 8 shows that each phrase generates totally different fingerprints, but anyone can produce the exact outcome from any computer when using the same hashing algorithm. The variable number that is used in Figure 8 is called a nonce [21]. The usage of the nonce is to change the output of the hashing algorithm which changes the fingerprint. If we set a random goal of finding an expression that generates a fingerprint that begins with number (0) in hexadecimal, it will create a challenge in the hashing algorithm.

The output of the PoW algorithm should have a mathematical property, that property requires that when an input message is concatenated with a nonce and make them the input to the hashing algorithm, the resulting fingerprint have to have a large prefix of $0's$ [60].

The length of the output string from the *SHA-256* algorithm is 256 bits no matter what the input. If the miner is looking for a fingerprint that contains 50 consecutive 0's in it, that would require him to perform 2^{50}operations of the hashing algorithm to find that string of characters [60]. In the example in Figure 8, it was looking for the first four consecutive zero bits (first zero in hexadecimal) and the wining nonce was 7, which can be verified by any person autonomously. If he added nonce 7 to the phrase "Block-chain input-data" and ran the *SHA-256* algorithm, he will get the same output string of characters. That successful result is also proof-of-work that proves the miner did the work to find that nonce number. Despite the fact that it took one run of the hash algorithm to be proven yet took 7 runs of the hashing algorithm to find a nonce that satisfies the conditions.

Block-chain's PoW algorithm is similar to the example above [21]. The miner creates a nominee Block packed with digital-actions. Then, the Miner computes the fingerprint of this Block's header to see if it less than the current target, which is the current number of sequential $0's$ of the prefix of the fingerprint. If the hash is greater than the target, the Miner needs to update the nonce by increasing the nonce by one and computing the fingerprint again.

Smart Contract

The traditional contract is an agreement with precise terms among two or more entities promising to conduct and act or prohibit it in exchange for something else [61]. To satisfy an entity's responsibility, each entity should trust the other entity [14]. Smart contract covers the same concept of the traditional contract of doing or not doing the act with a revocation of the trust condition. The smart contract terms are defined and enforced automatically by computer code. The smart contract is autonomous, decentralized, and a self-sufficient application [14].

The idea of the smart contract was introduced that had been introduced by Nick Szabo [19]. The concept of the smart contract can be defined as encrypted containers. These containers enclose values and only expose when assured situations are happened [23]. In other words, the idea of a smart contract is that contract terms are enforced and executed automatically among the participating entities without the need of an enforcer or a third party. Smart contracts were not well-known until the emergence of cryptographic currency based on the Block-chain technique [14].

The smart contract application took the Block-chain implementation further than simple simple digital action, such as trades. The digital action may contain more embedded information when used in the smart contract [13]. Block-chains, when used under the smart contract application as publicly-distributed-database, will allow the participated entities to confirm a situation or event occurrence without the need for a third-party [18]. It becomes much easier to record, confirm, and execute the smart contract when using the Block-chain technique under the smart contract application [14]. The smart contract can substitute any services that are provided by a third party, such as lawyers to form contracts, transfer property under certain conditions, or financial organizations to buy/sell merchandise/services.

The smart contract may represent the deployment of an agreement between entities. The smart contract's source code will reinforce the legal requirements. Wright and Filippi recommend that before the deployment of the smart contract, to support the reliability of the source code the smart contract's entities, there needs to be a model to prototype the contract's performance [18]. The smart contract is not a replacement of traditional physical contracts, but instead complement each other. The smart contract permits mutual problems to be resolved in a way that minimizes the necessity for trust [14]. Smart contracts' entities may need to enter into the traditional physical contract to cover non-technical matters.

The smart contract usage is to enable the trade of merchandise between unrelated people on the internet without the need

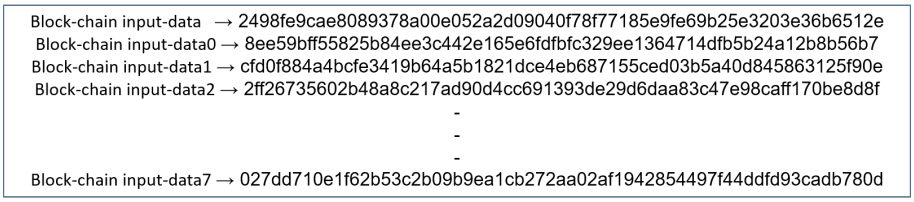

Figure 8. SHA-256 output of a characters of generating different fingerprint by iterating on a nonce. the data is generatd using free online tool called Free or matter
http://www.freeformatter.com/sha256-generator.htmlad-output

	Human interaction		Computerization	
Human establishments	✓	✓		
Automatic scheme		✓	✓	
DAO	✓			✓
System of systems			✓	✓

Table 3. The relationship between different types of automating schemes

for a central authority [18]. Recently, the smart contract was created to automatically perform derivatives, futures, swaps, and options. One usage of the smart contract is that it can be used for betting[15] by setting a programmed compensation [13]. The smart contract can be automated to release a compensation if a threshold of a definite share or exchange good is triggered. There are many applications that enable smart contract applications on top of the Block-chain technique, such Ethereum, Codius, and Ripple.
Ethereum was proposed by Vitalik Buterin in 2014 [23]. It is a platform that provides a lot of interesting programmable abilities to build and publish decentralized applications built on the top of the Block-chain technique [14]. Any entity can use Ethereum to: 1) enable smart contracts, 2) generate its own cryptographic currency (sub-cryptographic-currency), and 3) use that to execute and pay for the terms of the smart contract. Ether is the cryptographic currency for the Ethereum network, which is used to pay a fee for the provided services. Buterin categorized the usages of Ethereum to three classes which are: financial[16], partially financial[17], and non-financial[18] applications [23]. The financial applications supply customers with more dominant methods by using their cash to manage and enter into agreements. There are partially financial applications, when cash is involved, but, on the other side, there is a heavy non-financial side that is also being completed.

Cryptographic Currency

Cryptographic currencies are the earliest applications that used Block-chain technique as a publicly-distributed-database [18]. Cryptographic currency (equivalent to cash) can be issued or produced based on either centralized or decentralized currency systems. This paper is concerns specifically with decentralized cryptographic currencies that rely on the Block-chain technique. In 2008, Satochi Nakamoto (pseudonym) introduced the most well-known decentralized cryptographic currency, the Bitcoin, empowered with a distributed system known as Block-chain[26]. Bitcoin is unlike physical currencies that depend on a trusted central authority (Governments or Banks) to be produced. Instead, Bitcoin depends on a completely decentralized system because everything is based on cryptographic proof as an alternative of trust [18]. There are two ways of getting the Bitcoin. The first one is by trading physical currency (i.e., $ US dollar, or Euro). The second way is by participating in the mining process and getting rewarded. Bitcoin rewards drop whenever $210,000$ blocks are added to the Block-chain. The rewards started at 50 *Bitcoins per block* in 2009. In 2012, this rewards were reduced to 25 *Bitcoins per block* and it will be halved almost quadrennially. That is because the Bitcoin is limited to roughly $20 million$ Bitcoins in total [21]. Other cryptographic currencies, such Litecoin, have a total supply of around 84 million coins.
From the time Bitcoin was lunched, there have been 500 selections of decentralized cryptographic currencies available on the internet, such as Ripple, Litecoin, WebMoney or Dogecoin. Bitcoin does not structure the digital token that a person has. Instead it is structured as a movement of rights from a previous owner to a succeeding owner [62]. Cryptographic currency is, in general, secure. It allows us to hand over funds around the world within a couple of minutes, with no transaction limits, and with negligible fees compared to the current funds handover system that takes a couple of days, with transaction limits, and high fees to do that [18]. The cryptographic currency is accessible across the world with a computer device connected to the internet or smartphone.

Decentralized-Autonomous-Organizations (DAO)

Decentralized-Autonomous-Organizations (DAO) is a general term given to any future Block-chain application [29].

[15] In finance, it is a limit order.
[16] Sub-cryptographic-currency, derivatives, or determinations.
[17] Solving computational problem by self-enforcing donation.
[18] Voting, or decentralized governance.

DAO can represent the performance of any centralized entity in recent time. DAO can represent the performance of any centralized entity in recent time. The DAO does not mean the system is fully-automated but it is one of the automating schemes. Matilla gave a brief identification and differentiate between the automating schemes (see Table **??**).
also, Matilla argues that merging two decentralized applications that are empowered with Block-chain technology, such smart contract and cryptographic currency, makes it possible to construct fully-automated-nodes within a network [29]. Those fully-automated-nodes represent an automatic (robotic) scheme. Table 3 shows Matilla's categorization of the relationship between different types of automating schemes.