Brazilian Journal of Development

Blockchain to improve security, knowledge and collaboration inter-agent communication over restrict domains of the internet infrastructure, with human interaction

Blockchain para melhorar a segurança, o conhecimento e a colaboração entre os agentes de comunicação sobre domínios restritos da infraestrutura da Internet, com interação humana

DOI:10.34117/bjdv5n7-103

Recebimento dos originais:17/06/2019
Aceitação para publicação: 05/07/2019

Juliao Braga (a.k.a.: Luiz Juliao Braga Filho)
Formação acadêmica mais alta: PhD Candidate
Instituição: Universidade Presbiteriana Mackenzie, BR & Universidade de Lisboa, INESC-ID, PT
Endereço completo: Rua Alves Redol, 10, 1000-029 Lisboa, PT
Email: juliao@braga.eti.br

Joao Nuno Silva
Formação acadêmica mais alta: PhD
Instituição: Universidade de Lisboa, INESC-ID, PT
Endereço completo: Rua Alves Redol, 10, 1000-029 Lisboa, PT
Email: joao.n.silva@inesc-id.pt

Patricia Takako Endo
Formação acadêmica mais alta: PhD
Instituição: Universidade de Pernambuco
Endereço completo: Avenida Agamenon Magalhães, S/N - Santo Amaro - Recife - PE - 50100-010
Email: patricia.endo@upe.br

Jessica Ribas
Formação acadêmica mais alta: PhD Candidate
Instituição: Universidade Presbiteriana Mackenzie
Endereço completo: Rua da Consolação, 930, Consolação, São Paulo, SP, 01302-907
Email: jessica.ribas@mackenzista.com.br

Nizam Omar
Formação acadêmica mais alta: PhD
Instituição: Universidade Presbiteriana Mackenzie
Endereço completo: Rua da Consolação, 930, Consolação, São Paulo, SP, 01302-907
Email: nizam.omar@mackenzie.br

Brazilian Journal of Development

ABSTRACT

This paper describes the development and implementation of a blockchain to improve security, knowledge and intelligence during the communication and collaboration processes between agents under restricted Internet Infrastructure domains. It is a work that proposes the application of a blockchain, independent of platform, in a particular model of agents, but that can be used in similar proposals, since the results in the specific model were satisfactory. Additionally, the model allows interaction and, also, collaboration between humans and agents.

Keyword: internet infrastructure, agentes, ai, a2rd, skau.

RESUMO

Este artigo descreve o desenvolvimento e a implementação de um blockchain para melhorar a segurança, o conhecimento e a inteligência durante os processos de comunicação e colaboração entre os agentes sob domínios restritos da Infraestrutura da Internet. É um trabalho que propõe a aplicação de um blockchain, independente da plataforma, em um modelo particular de agentes, mas que pode ser utilizado em propostas similares, uma vez que os resultados no modelo específico foram satisfatórios. Além disso, o modelo permite interação e, também, colaboração entre seres humanos e agentes.

Palavras-chave: infraestrutura de nternet, agentes, ai, a2rd, skau

1 INTRODUCTION

Autonomous System (AS) is the name given to the networks making up the Internet (Hawkinson and Bates 1996). ASes establish interconnections through a protocol called *Border Gateway Protocol* (BGP) (Rekhter et al. 2006). BGP is a complex protocol that requires a lot of knowledge from the administrators of an AS. Sometimes the human being also forgets to update information, especially those related to routing policy and that reside on important servers such as *Internet Routing Registry*[1] (IRR), for example. IRR is a distributed database of route and route-related information (Braga 2010). Sometimes the human participation during the creation and update IRR objects processes is neglected and this is the motivation of this research. We propose to create a model of agents which could replace the human interventions. So, was propose the *Autonomous Architecture Over Restricted Domains* (A2RD) into the restricted domain of an AS, applying as use case over the IRR (Braga et al. 2015). A2RD replaces the human with your agents or *Intelligent Elements* (IEs), establishing a new IRR model, named *IRR revised* (IRR revised), shown in Figure 1.

Brazilian Journal of Development

A2RD specialized agents, automatically create objects as defined by the *Route Policy Specification Language* (Alaettinoglu et al. 1999, Blunk et al. 2005). Those

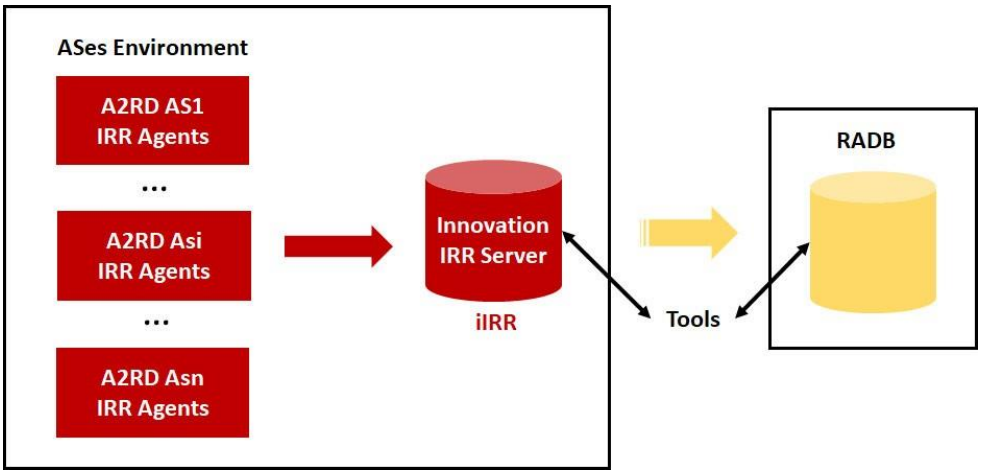


Figura 1. The IRR revised model established by A2RD implementation. Source: (Braga et al. 2019a)

objects that can not be created automatically will receive support from AS administrators through a human-computer cooperation mechanism. Nothing is changed in relation to the present and future of the IRR structure that is characterized by the recommendations of the *Internet Engineering Task Force*[2] (IETF) and *Internet Research Task Force*[3] (IRTF) stakeholders, disseminated through of their formal documents (Meyer et al. 1999, Villamizar et al. 1999, Newton 2004, McPherson et al. 2015, Kisteleki and Haberman 2016). Neither does it affect the security concerns surrounding the IRR and Internet governance (Kuerbis and Mueller 2017). Similarly, tools that use IRR databases can be used without any modification. A very useful, among others, is the IRR Powertools[4].

In this paper, *blockchain* is a data structure whose components are chained, with guarantee of immutability of its contents, and consequent integrity of the chain preserved by a cryptography process, with difficult computational reversibility. This definition is much simpler but more computationally oriented than those in which blockchain is associated with crypto-economics or crypto-currencies, and often have confusing definitions, but when it is clear, blockchain is defined as a database (Nakamoto 2008, Pilkington 2015).

On the other hand, by abstracting from property of immutability, the data structure like blockchain is a well-known concept used in computer research and originated in the academic

literature of the 1980s and 1990s (Narayanan and Clark 2017). As a simple data structure, for example, in works involving *provenance*, which is used as complementary data documentation containing the description of 'how', 'when',

'where', 'why' the data were obtained and 'who' obtained it (Braga and Banon 2008). The blockchain model proposed in 2008 to meet the Bitcoin virtual currency has effectively aroused the interest of the research community mainly by the immutabi- lity property that ensures data integrity (Prusty 2017, Bashir 2017). Immutability and integrity are obtained by a hash encryption mechanism (Bakhtiari et al. 1995, Rogaway and Shrimpton 2004). The combination of these two factors and charac- teristics associated to the blockchain recommended the application in the A2RD project, with the aim of enhancing communication and collaboration among the IEs (Braga et al. 2017b). This proposal is more simpler than those application of blockchain in Internet Infrastructure with fundamentals in Bitcoin technology, based in the appropriate fact that to run, Internet use resources such as numbers and names (Hari and Lakshman 2016).

There is no study directly related to this work and there are few blockchain works related to the Internet Infrastructure (Angieri et al. 2018). Blockchain still is not a matured technology, there are challenges that need to be considered when designing a platform, to ensure security, reliability and usability. So, if there is no related works associated with Internet Infrastructure, is due to the emergent nature of the topic, the reviewed literature was not published in high-ranking journals with prolonged review cycles (Xu et al. 2016).

The main goal of this paper is to present the *Internet Infrastructure Blockchain* (IIBlockchain), a blockchain architecture to improve the security, knowledge and intelligence in inter-agent communication and collaboration over restrict domains of the *Internet Infrastructure*, developed specifically and therefore independent of any available blockchain platform. The architecture proposed for IIBlockchain admits the interaction between the human being and the agents of the A2RD model as an additional resource to increase and improve the intelligence and autonomy of these agents. The next sections of this paper will be organized as follows. In section 2 we discuss the A2RD project and the needs for inter-agents communication and cooperation. In section 3 we present the architecture of IIBlockchain and the properties inherent to the blocks, their types and the characteristics of the designed chain. In section 4 we discuss the implementation of IIBlockchain showing the

Brazilian Journal of Development

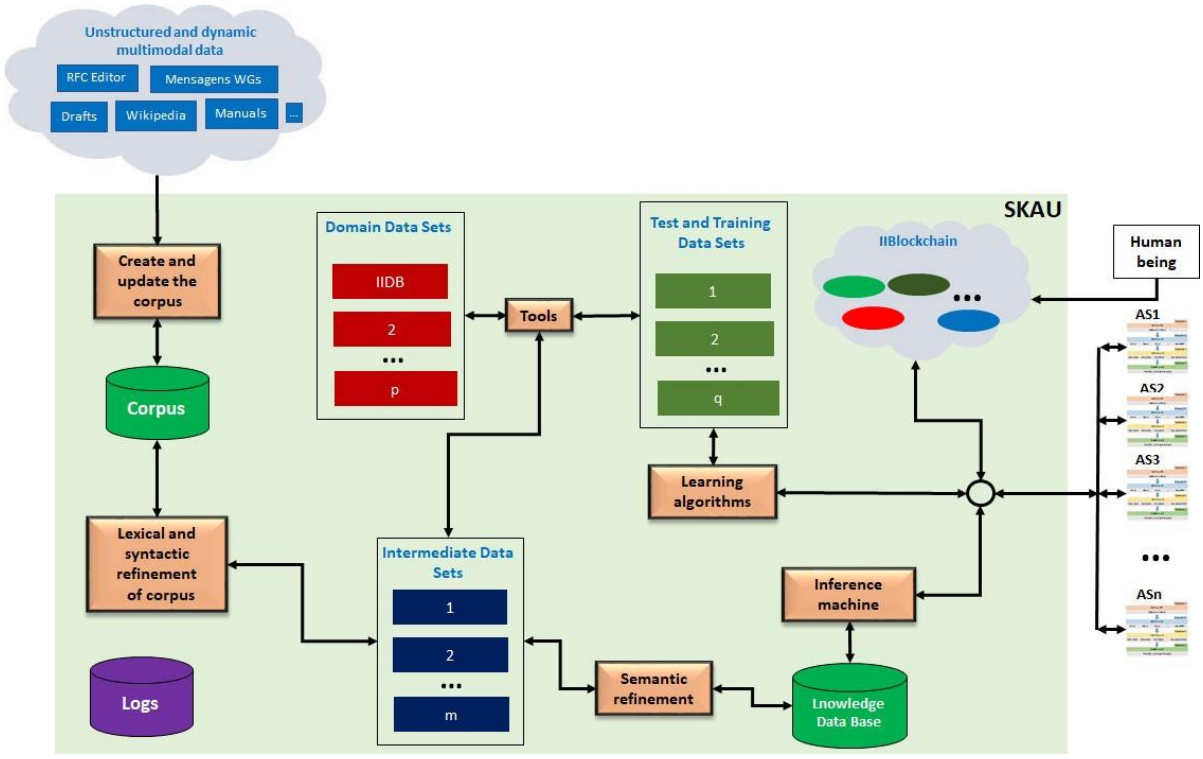
main associated properties. In section 5 we present the conclusions and in section 6 we present the proposals for future works.

2 THE A2RD PROJECT

A2RD is a project that initially proposed the creation of agents with automatic activities replacing human tasks in the environment of the AS restricted domain. The use case was the automatic process of addition and update of objects in IRR server. The application was considered useful mainly because the tasks of the AS administrator did not guarantee the accuracy in its completion nor the permanent need to update the objects, making the IRR an unreliable system from the point of view of its contents. A2RD solved this problem.

A new proposal for the A2RD environment model emerged from this experience (Braga et al. 2019b). The Figure 2 shows the environment conceptual model, named *Structure for Knowledge Acquisition, Use and Collaboration Inter A2RD Agents* (SKAU) in which each implementation of A2RD, into an AS, is represented as an agglomeration of intelligent agents scattered in a four layer model.

A2RD agents, reach their autonomy and intelligence aided by a lot of components, among which the *Knowledge Base*, the *Test and Training Data Sets*, and *Domain*



Brazilian Journal of Development

Figura 2. Structure for Knowledge Acquisition, Use and Collaboration Inter A2RD Agents (SKAU), i. e., the A2RD environment conceptual model

Data Sets. These components are obtained from non-structured databases, in particular, from the *Request for Comments* database, containing documents authored by network operators, engineers and computer scientists, documentary methods, behaviors, research, or innovations applicable to the Internet. The production of the RFCs occurs in the environment of *Work Groups* of the *Internet Engineering Task Force* (IETF) and *Internet Research Task Force* (IRTF), and maintained by RFC-Editor[5].

Each AS, of its own free will, may implement its respective A2RD, which is controlled by the special agent named *Controller*, which receives the identification *x:0*, where *x* is the *AS Number* (ASN).

A2RD agents need to communicate in order to collaborate, learn and cooperate with each other. This communication needs to be secure, that is, the respective *Controller* must recognize the origin of each pair in their information exchanges. A mechanism called *Dark Think Security* (DTS) has been proposed to ensure the desired security challenges (Braga et al. 2017a). Although preliminary implemen- tations have revealed that DTS is indeed secure, it has proved to be complex in implementation. In the search for a simpler alternative included *Pretty Good Privacy* (PGP) (Garfinkel 1995). Using PGP, an AS*x* Controller that wants to communicate with an AS*y* Controller, will use the AS*y* *public key* to encrypt the message, foR $\forall x$ *and* $\forall y$ *such that* $x \neq y$ *and* $x, y = 1, ..., n$, $n \leq$ total ASes pre- sent in the *Internet Routing Table*[6]. The AS*y* controller uses AS*x* *secret key* to decrypt the message. Thus, for this and for other reasons that we will see in the

following section, the recommended solution was a variation of blockchain imple- mentations proposed in the literature, that we named in this paper as *IIBlockchain*, which represents the component like a cloud, in Figure 2.

3 IIBLOCKCHAIN MODEL AND IMPLEMENTATION

The IIBlockchain model can be seen in Figure 3, which shows the implementation of A2RD in any two ASes (AS*x* and AS*y*).

Brazilian Journal of Development

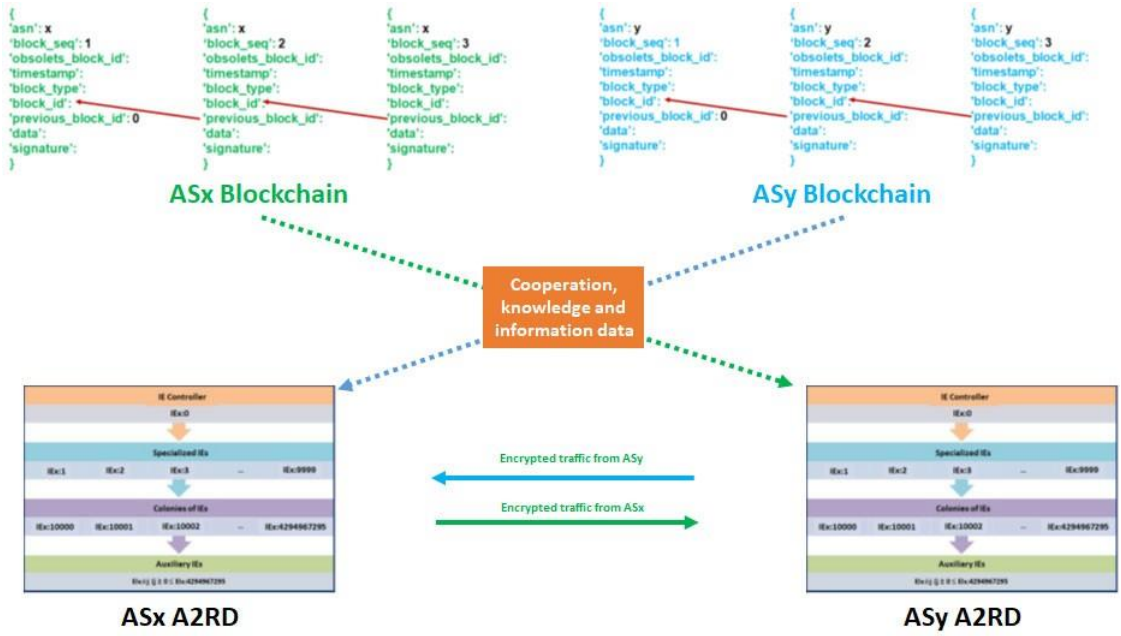


Figura 3. IIBlockchain Architecture implemented over ASx and ASy domains

This figure shows that the respective A2RD communicate through encrypted messages. Also, the A2RDs independently maintain a blockchain with properties characteristic of IIBlockchain. These chains contain, in their blocks, data inherent to each A2RD and about the environment of the AS in which they are implemented allowing the cooperation through the exchange of knowledge and information that can help in learning and maintaining the autonomy of their respective IEs. Each A2RD locally maintains a copy of IIBlockchain from each of the other ASes. There is no need to implement an A2RD for a chain to be constructed for an ASN. Specialized IEs of an ASx any guarantee that minimal information is included in chains of other ASes.

3.1. BLOCK PROPERTIES

A block of any chain type is equivalent to a dictionary structure of the Python language, whose configuration and summary description of the respective keys are shown in Figure 4.

The detail description of block keys are in Table 1.

```
{
'asn': Autonomous System Number,
'block_seq': Position into the chain,
'obsoletes_block_id': 'Block ID of the block that may have been replaced by this',
'timestamp': 'Current time the block was add to the chain',
'block_type': 'Type of the block',
'block_id': 'Hash of the entire block that will identify it',
'previous_block_id': 'Block ID of the previous block of this block',
'data': 'Data of the related with the block type',
'signature': 'Signature that ensures the owner of the data'
}
```

Figura 4. Block Structure

3.1.1. Human being blocks

Humans are agents, like any agent of the A2RD model. The difference is that they need tools to help them to build blocks. Examples of blocks that are to be constructed by humans are those that identify to the A2RD agents the respective passwords of the available equipment, in the domain and / or sub-domains of an AS.

3.2. CHAIN PROPERTIES

Any chain only exists if it has a 'Genesis' block type as its first block ('block_seq' = 1). Suppose that AS*x* wants to add in its chain, a block that will contain its *PGP public key* with which any ASN can encrypt messages that only AS*x* will understand. At this point, the AS*x* chain is empty. Suppose $x = 18782$. So, using the IIBlockchain Python class available at GitHub[7] if we add the block of type *PublicKey* we will have a two block chain as can be seen in Figure 5. It is important to note that block numbers (*block_seq*) are sequential (1 and 2, respectively).

Continuing and add a third block, now an *mntner* IRR object type (*irr_mntner*). The data is transformed into a string to be signed by the PGP, ensuring data properties to AS18782. Once this is done, the block is added to the chain as the third block. The block added can be seen in Figure 6.

To complete these example that illustrate some properties of the chain, let's assume a change in the object *irr_mntner*. A new data is signed via PGP, and included in the chain, not without first identifying in the *obsoletes _block_id*, the block that it is rendering obsolete. The new block is added as 4th block in the AS18782 IIBlockchain and your configuration is shown in Figure 7.

3.3. CHAIN TRANSFER

The chains are compressed and named as *ASxVaaaammddhhmmss.zip*. A specialized

IE will take care of this activity and follow up by compacting the chain, sending it to GitHub[8] and update the respective version in *wordIETF*. All chains are public, but the *secret keys* are not.

4 IIBLOCKCHAIN IMPLEMENTATION

In this section we make considerations on important topics that deserved special attention during implementation.

Tabela 1. Description of block dictionary keys

Key	Description
asn	ASnumber: Identifies the owner number of the string. For same string, the value of this key is always the same. If the identifier has the letters HU, that is, HUnumber, the block was produced by a human, usually the AS administrator.
block_seq	Identifies the position of the block within the chain. If block i preceding or immediately preceding block j than $i < j$ and not necessarily $j = i + 1$. This is due to the fact that a block can be removed, from an *ASN* chain, if it becomes obsolete. Upon removal, the block is added to the *obsolete* chain. The immutability and integrity of this *ASN* chain must be restored.
obsoletes_block_id	If the value of this key is not empty, so this references the **block_id** that will be obsoletes
timestamp	Time moment the block was add in the chain
block_type	Type of the block: block types are not necessarily predefined. IEs can create different types of blocks through agreements between them during their normal activities. Important blocks are, however, predefined. For example, the *Genesis* block, which is necessarily the first block of any chain. Blocks that represent IRR objects always prefix the usual object name with *irr_*. Blocks added by humans are necessarily prefixed with *hu_*.
block_id	Hash that will identify the block, obtained on the whole block, after it is completely filled
previous_block_id	**block_id** of the previous block of this block
data	Data of the related with the block type
signature	Signature that ensures the owner of the data

4.1. SPACE ANALYSIS

Table 2 displays some data about storage values, considering the chain created for the example in this paper.

Tabela 2. Storage Costs Parameters

#	Discrimination	Value
1	Block 1	1,300
2	Block 2	1,365

Brazilian Journal of Development

3	Block 3	3,451
4	Block 4	3,571
5	Total	9,687
6	ASes in routing table (27/06/2019)	64,831
7	IRR objects number (ARIN)	10
8	Number of protocols in TCP/IP	51

We used the *sys.getsizeof* function to determine the amount of bytes occupied by the Python dictionary structure, chosen to represent IIBlockchain. The result is


```
{
'asn': 18782,
'block_seq': 1,
'obsoletes_block_id': '',
'timestamp': 'Wed, 31 Jan 2018 10:57:19 +0000',
'block_type': 'Genesis',
'block_id': 'b663e678b4a96432e66ad45018680a93f3345b87490b6c49a0b791df61b3932a',
'previous_block_id': '0',
'data': '',
'signature': ''
}

{
'asn': 18782,
'block_seq': 2,
'obsoletes_block_id': '',
'timestamp': 'Wed, 31 Jan 2018 10:57:19 +0000',
'block_type': 'PublicKey',
'block_id': 'c18c6625f918b75b6292c62ee2949f83d53d5d8207174673bd08b8d4c7635657',
'previous_block_id':
'b663e678b4a96432e66ad45018680a93f3345b87490b6c49a0b791df61b3932a',
'data':
['-----BEGIN PGP PUBLIC KEY BLOCK-----',
'Version: GnuPG v1',
'',
'mI0EWnGhDwEEAKyP9NkCL3Fjs5x2FOtgrpJOC35U12JQI6MsudUYGA5vrMsvkq1L',
'W8oATQMUDzcPr2r6N+Y/PJKCDs9D81UlbtZJrUDgCBWnMpgxnngfSmEzgCZVrCev',
'QLQusEQBSwAaHxkDYnvK7vYznLkxd0v59qGwream5Byq3hvu5uGio7A9ABEBAAG0',
'LkFTMTg3ODIgKFVzZWQgaW4gQTJSRCBtb2RlbCkgPEFTMTg3ODJAYTJyZC5wdD6l',
'uAQTAQIAIgUCWnGhDwIbLwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQfpNr',
'HVGA5oRR9gQAn94XRaAzAUZqiVVK48FVDzRP1Zf+73BABGNGXx9SfMLM5xQ7w8Pq',
'YREtJJGu0Ax8nBBK1crRC1RBSIXGWyWx6xqZCM2NsNCViDFVOVyxp3sR5kVrcLwW',
'0PW2V0kepdzN+jPjNwJTirzqQu4STl9iALcv4bURiB9Kd2Zzuv/Hv/8=',
'=MLP4',
'-----END PGP PUBLIC KEY BLOCK-----',
''],
'signature': ''
}
```


Figura 5. Initial chain that, necessarily, has the block type 'Genesis'

not very good and so we evaluated two alternatives versions. The preferred version was that of larger result values[9] (lines 1-4 on the table). Suppose each block of the string to be constructed occupies twice as many bytes as the largest block in our example (line 4). So our block occupies **7,124 bytes**. *American Registry for Internet Numbers*[10] (ARIN) identifies ten objects to populate its IRR (line 7). Thus, only with IRR objects, the IIBlockchain of an AS spends $7,124 \times 10 =$ **71,124 bytes ~70 Kbytes**. So, the total bytes to represent the IRR objects for all ASn are: $64,831 \times 70$ Kbytes $= 4,647,086,080 \sim$ **4,4 Gbytes**. Now, let us assume that for each TCP/IP protocol[11] (line 8) we will need 20 blocks with the largest

Brazilian Journal of Development

known double size (knowledge information, for example): $20 \times 7,124$ *bytes* = **139 Kbytes**, value that corresponds to **0.003%** of the space spent by IRR objects. Certainly there are other types of blocks that IEs will produce. But the largest number of them are obsolete blocks. Very difficult to measure the space to be occupied by obsolete blocks. Only an inaccurate estimate would be possible. One estimate is that 25% of the blocks will be obsolete. So the total estimated storage space for the IIBlockchain is **5 Gbytes**. Any operation on IIBlockchain do not require additional space. There fore the space complexity is **O(1) ~ O(n)** (Costa 2015).


```
{
'asn': 18782,
'block_seq': 3,
'obsoletes_block_id': '',
'timestamp': 'Wed, 31 Jan 2018 10:57:24 +0000',
'block_type': 'irr_mntner',
'block_id': '5cc58ab3650c8ea443efddd1a4f748381e80e2c7ed325421750ec3f36f9b20ea',
'previous_block_id': 'c18c6625f918b75b6292c62ee2949f83d53d5d8207174673bd08b8d4c7635657',
'data':
{
'mntner': 'MAINT-AS18782',
'descr': 'Pegasus',
'admin-c': 'Juliao Braga',
'tech-c': 'Juliao Braga',
'upd-to': 'jb@pegasus.com.br',
'mnt-nfy': 'jb@pegasus.com.br',
'auth': 'CRYPT-PW ZocCkOH/zCkQw',
'mnt-by': 'MAINT-AS18782',
'changed': 'jb@pegasus.com.br 20090302'
},
'signature':
'-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1\n

{
"mntner": "MAINT-AS18782", "descr": "Pegasus", "admin-c": "Juliao Braga",
"tech-c": "Juliao Braga", "upd-to": "jb@pegasus.com.br",
"mnt-nfy": "jb@pegasus.com.br", "auth": "CRYPT-PW ZocCkOH/zCkQw",
"mnt-by": "MAINT-AS18782", "changed": jb@pegasus.com.br 20090302
}
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQEcBAEBAgAGBQJacaEUAAoJEIH4EAKGjl9ZzUUIAJ7q5ilUob8w0cvTKhNF8vq/
wzEh+lw3SF85nvV5GvplXql2dmgtddZD+aQVCXeRxENlO0ClbTPR0pAIlcyAG4O0
7IYxjF3nVYK2p44aCIJLYu5siUVRYexeyUVRVLVQj4qLV6p4S3VxsoTROa9avXoF
Cqa64wmDRJOepVSZMeclhjKeQRprSemOGf9SfwjZZDs8TZHFKVvAUQlgkOfuAjLn
vf6ehTfD+WM+zm+nNpXAbWx+ql+uYua/wacA5G4p0R81GVEQpmuF19Z9/BFi5gKP
qLd+modeEx0UlWr1DZle6kDAMqJFC5Q4telmTsnWKqNFvFEf6pwcR+Xzy6RD9N8=
=FLpY
-----END PGP SIGNATURE-----'

}
```


Figura 6. Block 3: Adding an IRR object

4.2. TIME COMPLEXITY

The heaviest algorithm we have in operations on IIBlockchain is to search linearly over an array or eventually over a linked list. Then, in the worst case, the complexity of time is O(n) (Costa 2015).

4.3. SECURITY

Brazilian Journal of Development

IIBlockchain is public. The security that matters to IIBlockchain will only be verified when a non obsolete block needs to be used. In two stages this is necessary: (a) the integrity of the block and (b) the reliability of the information contained in the block. Stage (a) consists of checking the validity of the hash that identifies the *block_id*. Stage (b) is the verification that the signature guarantees ownership of the information by the respective AS. If any of the above stages fails, an alert is sent to all implementations of A2RD. Immediately look for the block in the previous version and use it. The existence of the block in the previous version can be verified by the parameter *timestamp* and the name of the version. Meanwhile, specialized IEs will analyze the chain, in order to identify the cause of the breach of trust in the block.

5 CONCLUSIONS

The authors consider that the objective of allowing a mechanism of relation ship between IEs of the various A2RD implementations was achieved. Also, Blockchain is effective in ensuring co-operation and distribution of knowledge that can be shared


```
{
'asn': 18782,
'block_seq': 4,
'obsolets_block_id': '5cc58ab3650c8ea443efddd1a4f748381e80e2c7ed325421750ec3f36f9b20ea',
'timestamp': 'Wed, 31 Jan 2018 10:57:49 +0000',
'block_type': 'irr_mntner',
'block_id': 'b65ab41ee6e8675a5a75e5be5d3eb99a335b1c1073e0617a4d92cc4e6650350d',
'previous_block'_id: '5cc58ab3650c8ea443efddd1a4f748381e80e2c7ed325421750ec3f36f9b20ea',
'data':
{
'mntner': 'MAINT-AS18782',
'descr': 'Pegasus',
'admin-c': 'Juliao Braga',
'tech-c': 'Juliao Braga',
'upd-to': 'info@a2rd.pt',
'mnt-nfy': 'jb@pegasus.com.br',
'auth': 'CRYPT-PW ZocCkOH/zCkQw',
'mnt-by': 'MAINT-AS18782',
'changed': 'jb@pegasus.com.br 20180203'
},
'signature':
'-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

{
"mntner": "MAINT-AS18782", "descr": "Pegasus", "admin-c": "Juliao Braga", "tech-c": "Juliao Braga", "upd-to": "info@a2rd.pt",
"mnt-nfy": "jb@pegasus.com.br", "auth": "CRYPT-PW ZocCkOH/zCkQw", "mnt-by": "MAINT-AS18782",
"changed": jb@pegasus.com.br 20180203
}
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQEcBAEBAgAGBQJacaEtAAoJEEtF6Eiepna407UH/jh4Y5TEr2A72ROOEihrCUZf
TtXe69kAxbM4rFEOu5YyNKuVn/nosiOgRC46XowymC1Oben0Wwy2VVnt7jPjulmg
08vQYVrIBSYEConCiRSlAi9O1k0qBt8JjFoX1kySNwrg2TwWHu/ggQ7fwu+Bt73o
17w9/ZUBWBZyfXiPIt6PokQW000Aw/DAPQ5xUfRsDE6xHfZUz/7mrQUtDBQNAWmp
5YP84Gzyjfv6BLuFCpHetq2pzXDpDDOt13cGWGKMreR0TgAS7jpZlGXtdFjBcOUx
pisjnQc4EyQdNSUyNWMWOm7CBEGdwhvPDb1FYjPxI+SaecYrr3pwJIIIOr9H7uU=
=+/Yx
-----END PGP SIGNATURE-----'
}
```


Figura 7. Block 4: Makes block 3 obsolete

among IEs in the various domains of ASes. It is a simple, easy-to-understand, and implementation-oriented design with no additional effort required in any programming language. The IIBlockchain has both public and private characteristics and has no inherent concerns or additional difficulties, for this reason. Also, it is worth remembering that IIBlockchain is oriented to the application of Blockchain by agents and not by humans, which certainly decreases complexity.

6 FUTURE WORKS

At this point, it is not possible to determine how the presence of obsolete blocks will influence the operations on an IIBlockchain of some ASN. Implementations in programming languages like Python and others one, does not seem to be a big problem, because dictionaries are indexed and obsolete blocks can be ignored. However, it is necessary to evaluate the possibility of creating a new type of chain: the chain of obsolete blocks, that is to say, the chain consisting of blocks that become obsolete in each ASN chain.

At some point, one A2RD IE may checking the state of the chain and remove obsolete blocks, passing it to the obsolete chain considering:

- The chain from which the block was removed will be reconstituted to maintain the immutability and integrity. This is achieved by having the next block point to the previous block removed, and a new hash is calculated to identify

  the next block and successively to the blocks thereof until the end of the chain.

- The block removed will be inserted in the *obsolete chain* pointed to the last block of this chain. The block's block number ('block_seq') should be concatenated by a hyphen and another sequence number to the number of the last block of the *obsolete chain*. After this a new hash will be determined to identify this block and the block can be inserted in the *obsolete chain*

Complementary, the IIBlockchain design is simple enough for applications in several other networking areas or not. New versions of the implementation will seek to establish independence from block structure and coding.

ACKNOWLEDGEMENTS

This work is supported by CAPES – Brazilian Federal Agency for Support and Eva-luation of Graduate Education within the Brazil's Ministry of Education, by national funds through FCT with reference UID/CEC/50021/2019 and by MackPesquisa.

REFERÊNCIAS

Alaettinoglu et al. 1999 Alaettinoglu, C., Villamizar, C., Gerich, E., Kessens, D., Meyer, D., Bates, T., Karrenberg, D., and Terpstra, M. (June 1999). Routing Policy Specification Language (RPSL). Technical report, RFC Editor. RFC2622. (DOI: 10.17487/RFC2622). Acessado em 03/06/2019.

Angieri et al. 2018 Angieri, S., García-Martínez, A., Liu, B., Yan, Z., Wang, C., and Bagnulo, M. (2018). An experiment in distributed internet address management using blockchains. *arXiv preprint arXiv:1807.10528*.

Bakhtiari et al. 1995 Bakhtiari, S., Safavi-Naini, R., Pieprzyk, J., et al. (1995). Cryptographic hash functions: A survey. *Centre for Computer Security Research, Department of Computer Science, University of Wollongong, Australie*.

Bashir 2017 Bashir, I. (2017). *Mastering Blockchain*. Packt Publishing Ltd.

Blunk et al. 2005 Blunk, L., Damas, J., Parent, F., and Robachevsky, A. (March2005). Routing Policy Specification Language next generation (RPSLng). Technical report, RFC Editor. RFC4012. (DOI: 10.17487/RFC4012). Acessado em 15/06/2019.

Braga 2010 Braga, J. (2010). Políticas de roteamentos: como resolver a impossibilidade de implementação na tecnologia *hop-by-hop* e o futuro. *GTER 29*. Disponível em <ftp://ftp.registro.br/pub/gter/gter29/01-PoliticasRoteamento.pdf>. Acessado em 25/05/2010.

Braga et al. 2017a Braga, J., de Amorim Silva, R., Endo, P. T., and Omar, N. (2017a). Dark Think Security: Enhancing the Security for the Autonomous Architecture over a Restricted Domain. In *Proceeding of CSBC 2017*, page 8, Mackenzie Presbiterian University.

Braga et al. 2015 Braga, J., Omar, N., and Granville, L. Z. (2015). Uma proposta para o uso de elementos inteligentes em domínios restritos da infraestrutura da internet. In *Anais CSBC 2015 - WPIETFIRTF*, Recife, Pernambuco, Brasil.

Braga et al. 2017b Braga, J., Omar, N., and Thome, L. F. (2017b). Acquisition and use of knowledge over a restricted domain by intelligent agents. In *Proceedings of the SouthEast Conference*, ACM SE '17, pages 203–207, New York, NY, USA. ACM.

Braga et al. 2019a Braga, J., Silva, J. N., Endo, P., and Omar, N. (2019a). Structure for knowledge acquisition, use, learning and collaboration inter agents over internet infrastructure domains. In Arai, K., Bhatia, R., and Kapoor, S., editors, *Intelligent Computing*, pages 527–547, Cham. Springer International Publishing.

Braga et al. 2019b Braga, J., Silva, J. N., Endo, P. T., and Omar, N. (2019b). On Intelligent, Autonomous and Collaborative Agents to Manage Internet Routing Domains. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, page 1. IEEE.

Braga and Banon 2008 Braga, J. C. and Banon, G. J. F. (2008). Data provenance: Theory and application to image processing. *IEEE Latin America Transactions*, 6(2).

Costa 2015 Costa, E. (2015). *Programação em Python*. FCA, Lisboa, PT, 1 edition. Garfinkel 1995 Garfinkel, S. (1995). *PGP: pretty good privacy*. " O'Reilly Media, Inc.".

Hari and Lakshman 2016 Hari, A. and Lakshman, T. (2016). The internet blockchain: A distributed, tamper-resistant transaction framework for the internet. In *Proceedings of the 15th ACM Workshop on Hot Topics in Networks*, pages 204–210. ACM.

Hawkinson and Bates 1996 Hawkinson, J. and Bates, T. (March 1996). Report on MD5 Performance . Technical report, RFC Editor. RFC1930.

<https://tools.ietf.org/rfc/rfc1930.txt>. (Updated-By RFC6996, RFC7300) (Also BCP0006) (Status: BEST CURRENT PRACTICE) (Stream: IETF, Area: rtg, WG: idr). Acessado em 06/09/2014.

Kisteleki and Haberman 2016 Kisteleki, R. and Haberman, B. (June 2016). Securing Routing Policy Specification Language (RPSL) Objects with Resource Public Key Infrastructure (RPKI) Signatures. Technical report, RFC Editor. RFC7909. (DOI: 10.17487/RFC7909). Acessado em 03/02/2019.

Kuerbis and Mueller 2017 Kuerbis, B. and Mueller, M. (2017). Internet routing registries, data governance, and security. *Journal of Cyber Policy*, 2(1):64–81.

McPherson et al. 2015 McPherson, D., Amante, S., Osterweil, E., Blunk, L., and Mitchell, D. (December 2015). Considerations for Internet Routing Registries (IRRs) and Routing Policy Configuration . Technical report, RFC Editor. RFC7682. (DOI: 10.17487/RFC7682). Acessado em 03/02/2019.

Meyer et al. 1999 Meyer, D., Schmitz, J., Orange, C., Prior, M., and Alaettinoglu, C. (August 1999). Using RPSL in Practice. Technical report, RFC Editor. RFC2650. (DOI: 10.17487/RFC2650). Acessado em 03/02/2019.

Nakamoto 2008 Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic CashSystem.

Narayanan and Clark 2017 Narayanan, A. and Clark, J. (2017). Bitcoin's academic pedigree. *Communications of the ACM*, 60(12):36–45.

Newton 2004 Newton, A. (February 2004). Cross Registry Internet Service Protocol (CRISP) Requirements. Technical report, RFC Editor. DOI: 10.17487/RFC3707. Acessado em 03/02/2018.

Pilkington 2015 Pilkington, M. (2015). Blockchain technology: Principles and applications. In *esearch Handbook on Digital Transformations*, pages 11–39. Edward Elgar. Available at https://ssrn.com/abstract=2662660.

Prusty 2017 Prusty, N. (2017). *Building Blockchain Projects*. Packt Publishing Ltd. Rekhter et al. 2006 Rekhter, Y., Li, T., and Hares, S. (January 2006). A Border Gateway Protocol 4 (BGP-4). Technical report, RFC Editor. RFC4271. (DOI: 10.17487/RFC4271). Acessado em 03/02/2019.

Rogaway and Shrimpton 2004 Rogaway, P. and Shrimpton, T. (2004). Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In *International Workshop on Fast Software Encryption*, pages 371–388. Springer.

Villamizar et al. 1999 Villamizar, C., Alaettinoglu, C., Meyer, D., and Murphy, S. (December 1999). Routing Policy System Security. Technical report, RFC Editor. DOI: 10.17487/RFC2725. Acessado em 03/02/2019.

Xu et al. 2016 Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., and Chen, S. (2016). The blockchain as a software connector. *Proceedings - 2016 13th Working IEEE/IFIP Conference on Software Architecture, WICSA 2016*, 11(2016):182–191.