INTERNET BANKING VS BLOCKCHAIN: WHAT TECHNOLOGY ADHERES BETTER TO ASPECTS RELATED TO INFORMATION SECURITY? A BRAZILIAN CASE STUDY

MORAIS, JULIANI PAOLA RIBEIRO

Universidade de Taubaté, Department of Informatics, Brazil.

E-mail: juliani1011@gmail.com,

MONTEIRO, RITA DE CASSIA R. V.

Universidade de Taubaté, Department of Informatics, Brazil.

E-mail: rita_rigotti@yahoo.com.br,

MONTEIRO, DIEGO VILELA

Universidade de Taubaté, Department of Informatics, Brazil.

E-mail: dvm1607@gmail.com.

ABSTRACT

For centuries civilizations have sought a way to improve the exchange of goods and services, and due to the exponential increase in new products people have adopted currency as a solution, popularly known today as money, thanks to currency getting a product has become a relatively simple process. Currency has evolved over the years. At first the money was only the exchange of goods or products among people. As the years passed precious metal and stones acquired their own value. Currently we are in the age of paper currency, in which most countries have their own currency. However, information related to the virtual currencies and the number of people who are using has grown. What was once just a code spread on the internet, is now attracting the attention of banks and specialists, gaining new market value. This article aims to compare the technologies that encompass the security of the transactions of Internet Banking and the virtual currency Bitcoin. We compared both technologies to the pillars of information security, known as CIA, confidentiality, integrity and availability. During the topics it will be possible to observe information about each of the technologies, as well as, the way of operation, the safety methods adopted and some definitions regarding technical terminology on the topic. Later, based on the collected information it will be possible to observe which technology currently adheres best to the CIA criteria in Brazil. At last a brief discussion on how the technologies can be complementary for the construction of new systems even more effective and safe.

Key words: Blockchain, Bitcoin, security, Internet Banking, confidentiality, integrity.

INTRODUCTION

Nowadays, the keyword for any system is security, it is necessary to be mindful of how the data is stored and accessed, so to find the best way to protect essential information pertaining to businesses from institutions and organizations, maintaining So the integrity and confidentiality of the data being transmitted. Based on this, this

article aims to compare the technologies that guarantee the safety of Internet Banking and the Blockchain Technology, that is behind the virtual currency Bitcoin. Furthermore, statistical data related to attack attempts suffered by Blockchain around the world and banking technologies in Brazil in 2015 shall be analyzed, to demonstrate to what extent can each technology currently overcome the problems of information security.

The idea of a decentralized money emerged in 1998 through the Cyberpunk Manifesto that was aimed at respecting the privacy of people by offering goods and services without their privacy being violated either by the government or any other source. the concept of Bitcoin as cryptocurrency was officially published in 2009, almost ten years after the manifesto, by the programmer whose pseudonym is Satoshi Nakamoto who in turn did not reveal much about his identity.

Bitcoin is a kind of virtual currency. Ramos (2012) defines virtual currency as a currency unlike any previous one, working in a completely electronic fashion. No governments or agencies regulate it, virtual currency exist through cryptography and decentralized code.

From 2009 to the present-day Bitcoin has been maintained by the community of users who use it, the source code of the currency is open, which allows several developers to further enhance the currency and their security features, each change in the code is only accomplished with the consensus of all members of the Bitcoin community. In 2017 the virtual currency Bitcoin was divided into two extra types, Bitcoin Cash and Bitcoin Gold. For the purposes of this study, we will only use Bitcoin, thus disregarding the schemes and technologies adopted by its new variations.

With the arrival of Bitcoin, one technology behind its network has woken interest from several scholars and businesses: the Blockchain. According to Filho (2016), “The Blockchain which is commonly compared to a ledger, is formed by several blocks, which contain one or more transactions stored.”

The Blockchain is the data structure representing a financial accounting entry or a record of a transaction. Each transaction is digitally signed with the purpose of ensuring its authenticity and ensuring that no one tampers with it, so that the registration itself and transactions within it are considered highly integer.

The idea of Nakamoto for the Blockchain according to Castro (2017), was based on three pillars:

i. Give a copy of the transaction history performed from the start of the digital currency to all available computers to process it;

ii. To validate each new transaction, encryption requires two keys: a public (disclosed with the order of the transaction) and another private (always kept secret), confirming the identity of the user without exposing it to the risk of stealing their coins; and

iii. Process the transactions in blocks: each new block is processed and appended to the original list as another link in the chain (hence the name ' blockchain '). Finally, all computers, working in a coordinated, but independent way, process transactions and hit the results with each other, validating by consensus the new transaction block before attaching it to the old blockchain. "

With the pillars defined by Nakamoto for the construction of the Blockchain two problems that occurred very frequently were solved:

i. Double-spending, which occurs when a same transaction is requested more than once, i.e. when the same currency is spent more than once; and

ii. The guarantee that the Data is immutable, that is, it allows the authenticity of the information, since after the data is saved in the block chains they cannot be more altered.

The Blockchain applications can be numerous, from registration of real estate, voting systems, registry offices, virtual currencies and various other areas. Lately, large banking institutions and communications firms are conducting studies for future implementations of Blockchain and virtual currency technologies in their networks. This has mainly affected the labor market and education since with the emergence of this new technologies has created the need for more skilled professionals to conduct research, studies, and new applications.

The evolution of currency has made its use and storage change through the years. Currently, Internet Banking and Mobile Banking are growing, according to data acquired from FREBABAN (2017), presented in Figure 1, in 2016 digital media represented around 57% of all transactions. As this number grows there is also an increase in the number of attacks directed at users, especially with the use of fake pages.

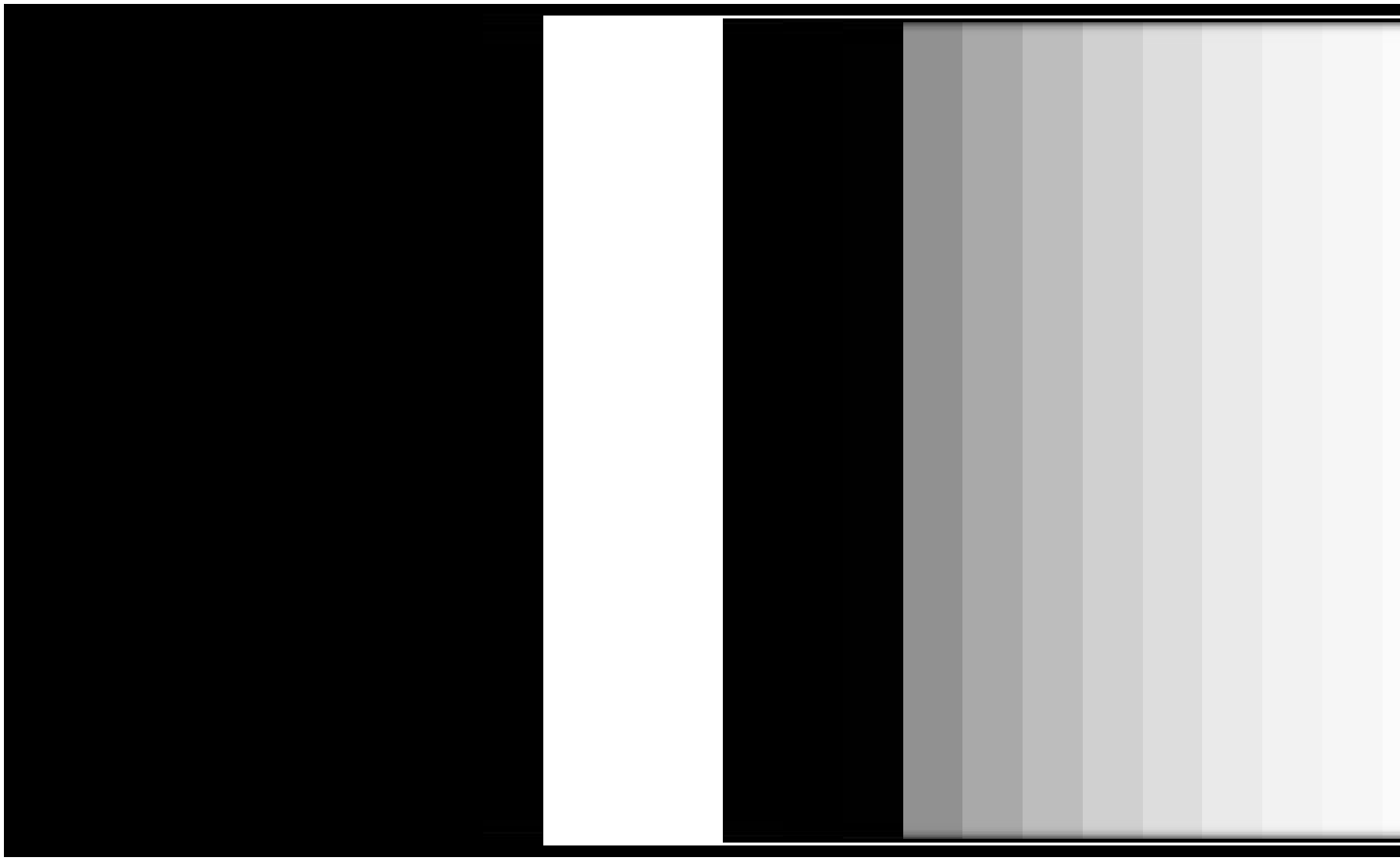

Figure 1: Increased transactions by digital channels. Digital media is represented by green colored stripes Source: FEBRABAN (2017).

Matos (2013), says that “the origin of internet banking dates to the last century 80’s when the attempt of entities to offer electronically processed service to their clients was registered. However, only in October 1994 the first sketch of what is currently named Internet Banking emerged. In a groundbreaking movement of the American bank Stanford Federal Credit Union, the Californian financial institution that took

advantage of the expansion of network telecommunications and the World Wide Web to break the barriers of distance and enable the accomplishment of various online operations, about 13 months after the start of the testing period of virtual transactions. "

Adachi (2004), defined that “A bank's website generally has two types of content: open, which publishes institutional information, dissemination of products and services, in addition to communicating promotional campaigns and closed content, when enables customers to access their personal data and bank transactions”.

Objectives

This article aims to compare the technologies of the virtual currency Bitcoin, the Blockchain and the technology used by the network Internet Banking.

COMPARISON OF THE TECHNOLOGIES REGARDING CIA

Maintaining data and secure information in an increasingly digital world has been challenging for technology professionals, within the scope of information security Three pillars are defined to analyze whether a system is safe, these pillars are called CIA, and are defined by Maia (2013), as follows:

i. "Confidentiality, unlike being a secret or something inaccessible, is a concept in which access to information should be granted to those who are entitled, i.e. only to entities authorized by the owner or owner of the information.

ii. The concept of integrity is linked to the property of maintaining the information stored with all its original features established by the information owner, taking attention to its lifecycle (creation, maintenance, and disposal).

iii. And finally, the concept of availability must ensure that information is always available for use when authorized users need. "

Based on the pillars of information security and the definitions of Maia (2013), the following topics compare the characteristic of each technology with the previously mentioned criteria.

Confidentiality

To compare the security of the two technologies we consulted the data of the Center for response and treatment of security incidents in Brazil (CERT.BR), responsible for dealing with data security incidents on computers connected to the Internet in their country, statistics show that in 2015 about 722,205 attacks were reported, from those 168,775 correspond to fraud, within these figures the total number of frauds with financial goals involving the use of counterfeit pages was 40.23%. Banks do not disclose official data about the attacks they have suffered to protect their image, however, it is estimated that most of the data reported by the CERT.BR are linked to attacked banks.

One of the most common attacks to Internet Banking in Brazil (see Figure 2) is the use of fake webpages (hereafter webpages will be referred as pages) that are identical to real bank pages. This attack targets unsuspecting users who believe they are doing

some kind of update on their personal information or are receiving a prize, and thus willingly input all their information. With these information con artists can perform several kinds of bank transactions, causing great financial damage.

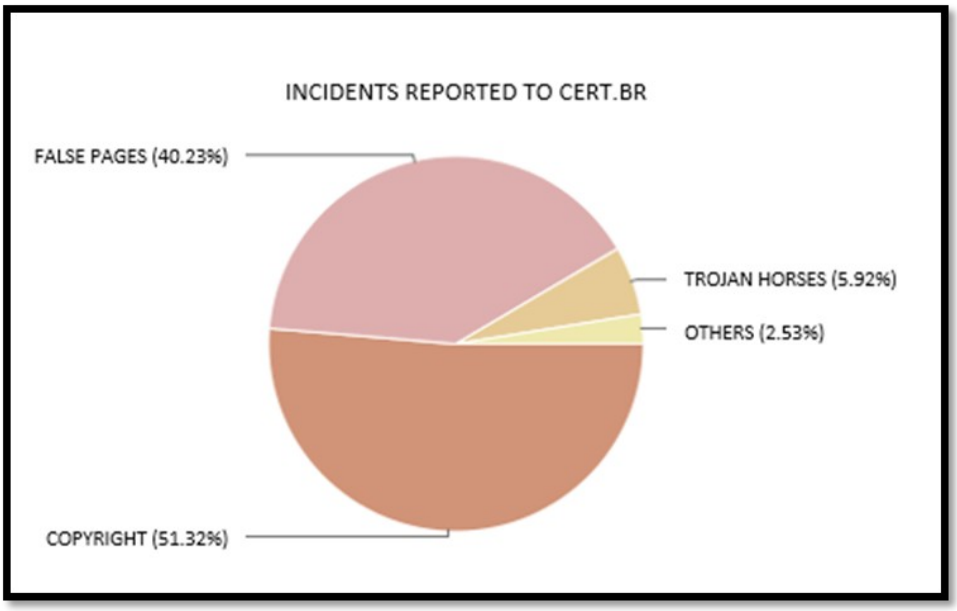

Figure 2: Incidents reported by CERT.BR.

Since its creation in 2009, Blockchain has suffered no potential damage to its network, all the actions that offered threads to the network or the integrity of users have been blocked and corrected before transactions were completed, as can be observed in the open and available data at blockchain.info The organ responsible for registering Bitcoin data and statistics.

The exchanges, brokerages responsible for facilitating the trade of virtual currency to the market, have suffered some attacks on their web pages, but, these types of attacks do not affect the Blockchain system, since each exchange itself maintains a system for purchasing and selling currency, and these systems have no direct connection to the Blockchain.

Another aspect analyzed in this article is the way the two technologies work, the network Internet Banking is integrated into banks and has a centralized system that analyses their transactions, Blockchain works with a decentralized system where several people, called "miners", are responsible for generating new blocks in the network and primarily validating users' transactions in exchange for rewards for their service. Another relevant feature regarding transactions is that since Blockchain works with a peer-to-peer system, international transactions can be accomplished faster than with Internet Banking. Because Internet Banking needs to perform currency exchange to carry out transactions which can result in high service charges. Figure 3 illustrates how both transactions work.

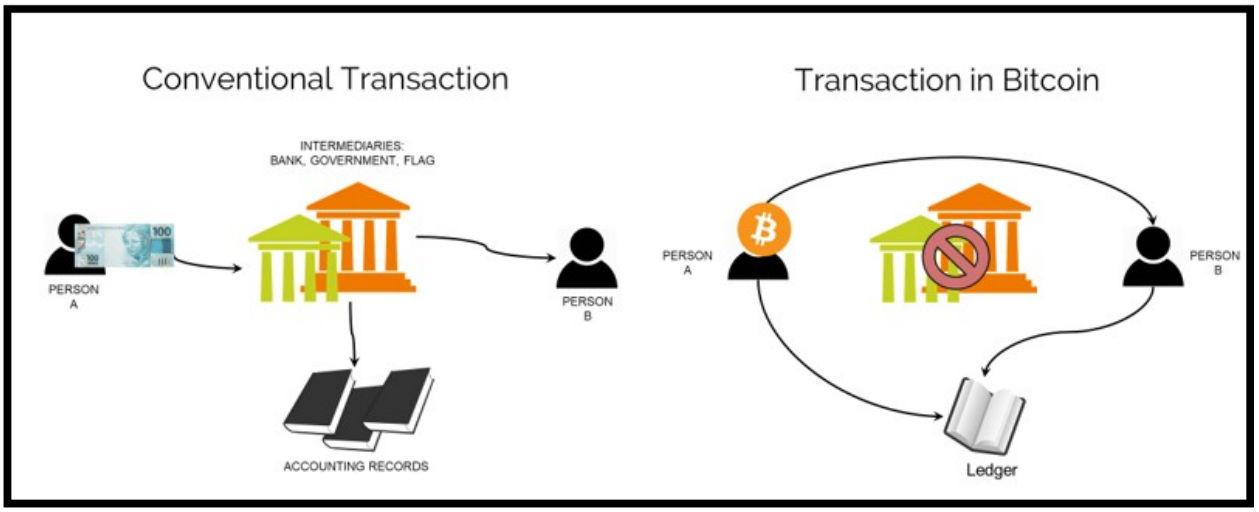

Figure 3: Example of transactions. Source: The author himself.

There are thousands of miners scattered around the world to ensure security against mistakes and fraud, miners are constantly doing double checks on each other's work. When a Bitcoin is sent to miners to confirm the transaction, they write the details in a public ledger called Block and are rewarded with fractions of newly mined Bitcoins for the service provided, while recording transactions. The miners also “play” a kind of lottery with the encryption of the blocks, the prizes are new Bitcoins. They are rewarded to the first miner that solves the encryption, that means to calculate the number that deciphers the block and send the response to the network, Figure 4 illustrates how the lottery works and the rewards for validating transactions.

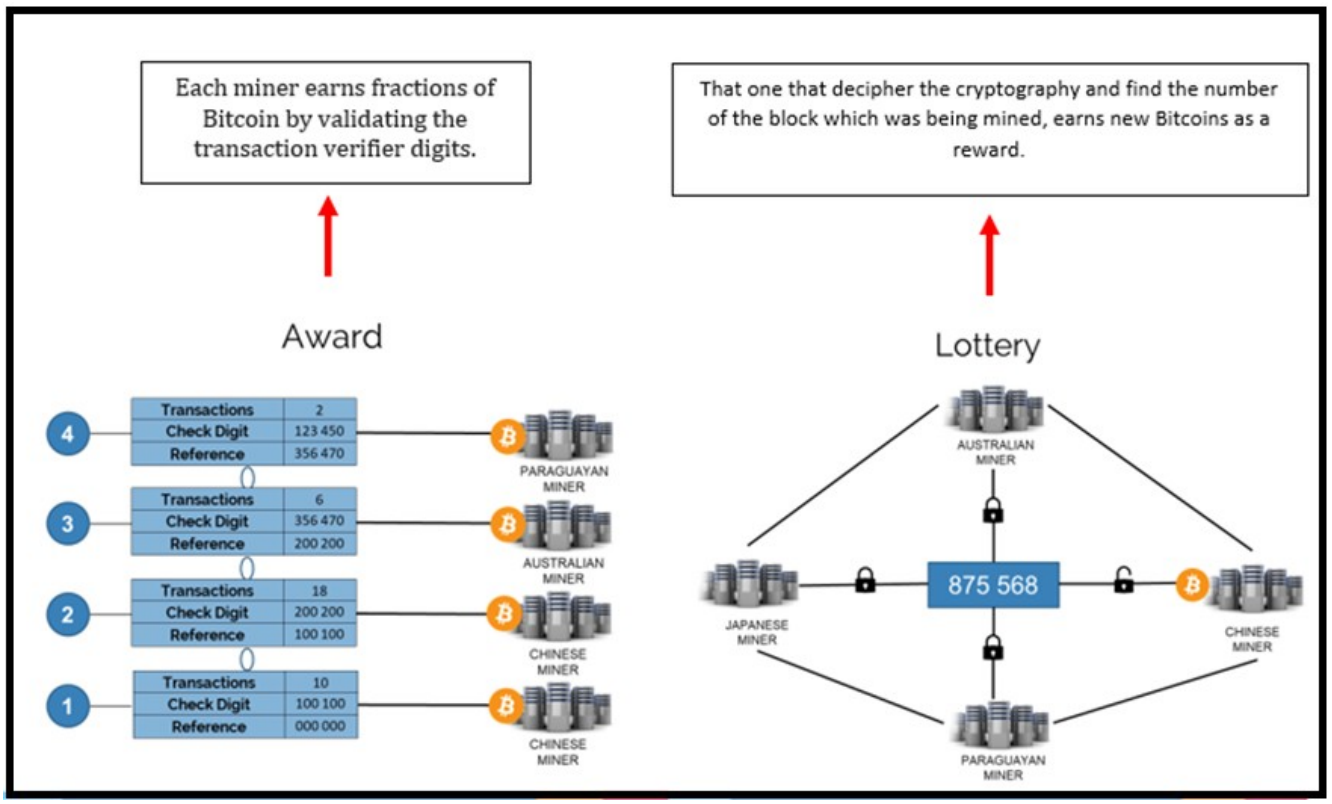

Figure 4: Prize and lottery of Blockchain. Source: The author himself.

The solved block is added to the Blockchain, which lists each Bitcoin transaction already made in history, the more computational power miners have the faster they can work to calculate the right number and submit the number to the network, the difficulty of getting the right number increases based on the speed that miners complete the Blocks. The difficulty is adjusted to each 2016 mined block so that no matter how many miners exist, each new block is mined by the network in about 10 minutes, figure 05 shows how the blocks are chained and stored in the Blockchain. According to Marco Agner (2016), each block "has an 80 bytes header containing metadata to be stored in the ledger transactions, a transaction counter that varies from 1 to 9 bytes and all transactions performed within that block."

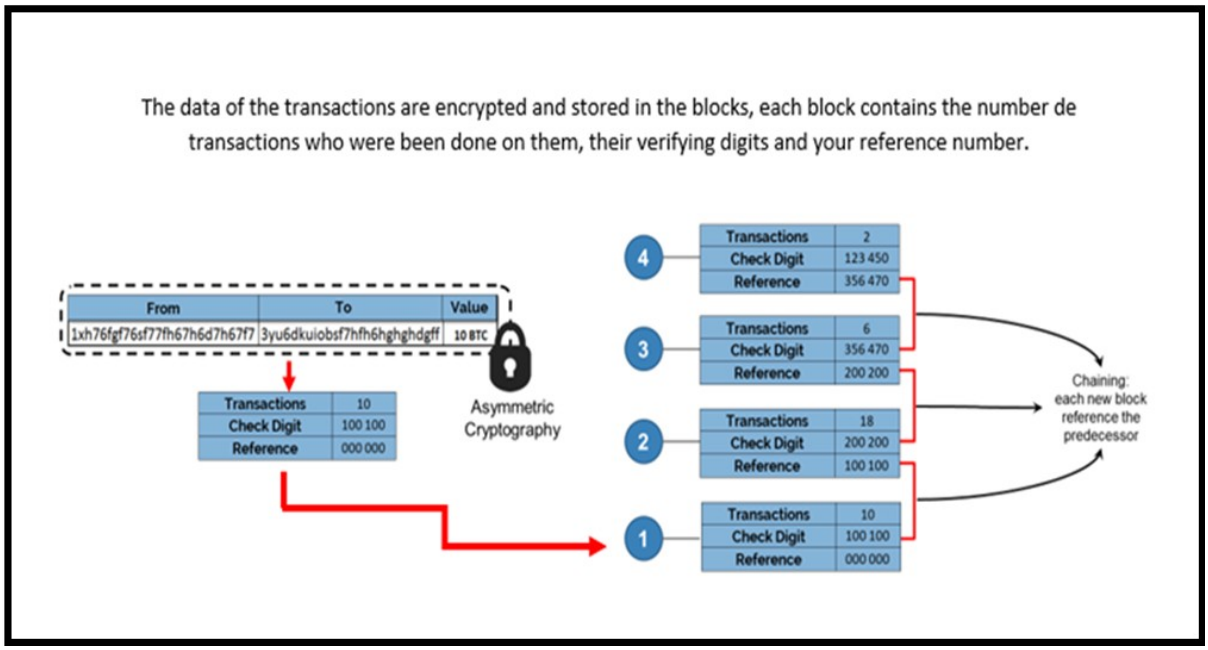

Figure 5: Chaining and storing the blocks. Source: The author himself.

The greater the complexity, the greater the computational power needed to be mined, on the other hand, the higher the number of miners and computational power involved working in the network, the greater the difficulty rate for mining and consequently the difficulty in performing network attacks increases. For this reason, the individual who wishes to invade that system would have to have at least 50% of the network and a computational power greater than that of all other miners. Figure 6 shows the current mining difficulty and a forecast for up to December 2017.

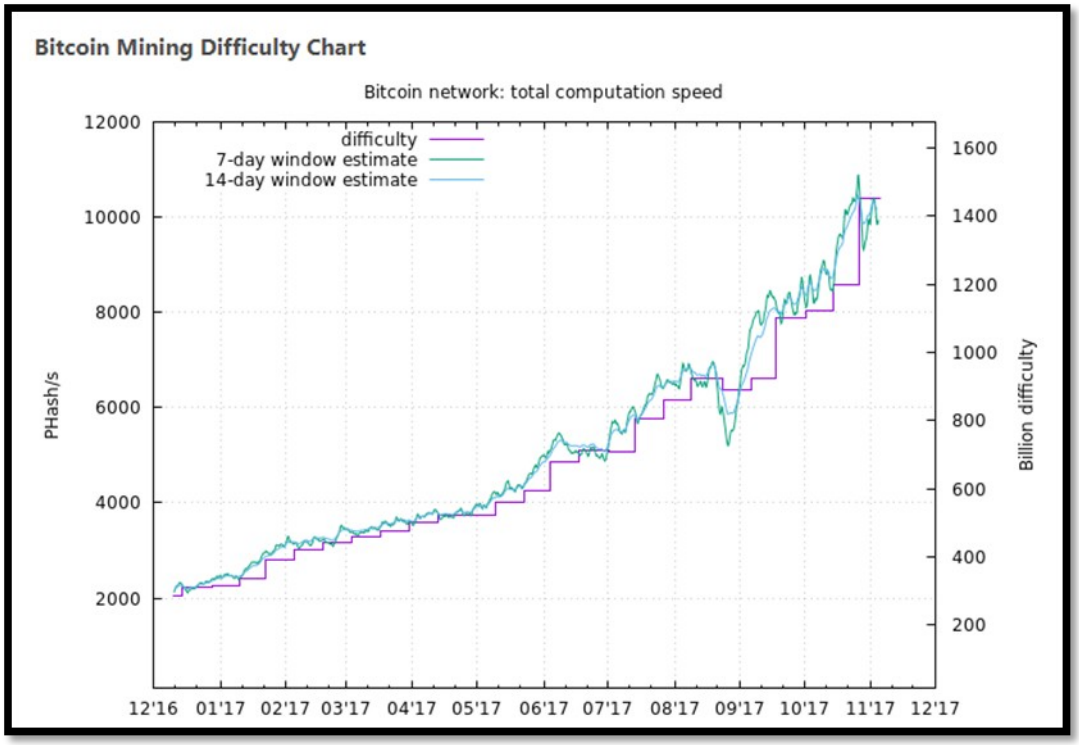

Figure 6: Degree of difficulty in mining new blocks. Source: EOBOT (2017).

Concerning disclosure of the users' identities, that is, the confidentiality of the data, the network Internet Banking saves in its system all the data from the users who performed the transactions in its accounting storage system. This data contains personal information about its users, such as: names, account numbers, transferred amounts, etc.

In this regard, Blockchain differs greatly from Internet Banking, within the network no user data is revealed, and transactions are carried out in a peer-to-peer fashion. Only the public keys and amounts are stored in the ledger. Since Blockchain protects its users' anonymity, ill-intentioned people can easily make use of it. Tracking transactions might become possible in the future, but so far, no tracking technique identifies precisely location or user.

Integrity

Regarding security, technologies also differ considerably. Blockchain in addition to passwords, Tokens and security keys, also uses asymmetric encryption and the Hash rate, defined by Steller and Cerqueira (2017), as, "A kind of unique signature that prevents information from being altered".

Hash is what differentiates the Blockchain network from others. Hashes meet within the headers of each block, together the hashes form the Merkle tree, ie, together they work as a kind of digital signature, thus making it an encryption present in the Blockchain. Something with a high degree of safety.

According to Marco Agner (2016), "to form the root of this binary tree with transactions, each transaction has its ID (the hash of the transaction) concatenated to the ID of the neighboring transaction in the tree, and is subjected to a double round Verification, by the hash function SHA-256, Successively until it reaches the root. For this, all transactions must be placed on the same level as in Figure 6, and form pairs to successively create the above levels. If a Block does not have a pair of transactions, the last transaction is repeated, for a better understanding figure 7 illustrates an example of the Merkle tree in a block with 16 transactions performed on the Blockchain network, in which it proves that transaction M is included in the block.

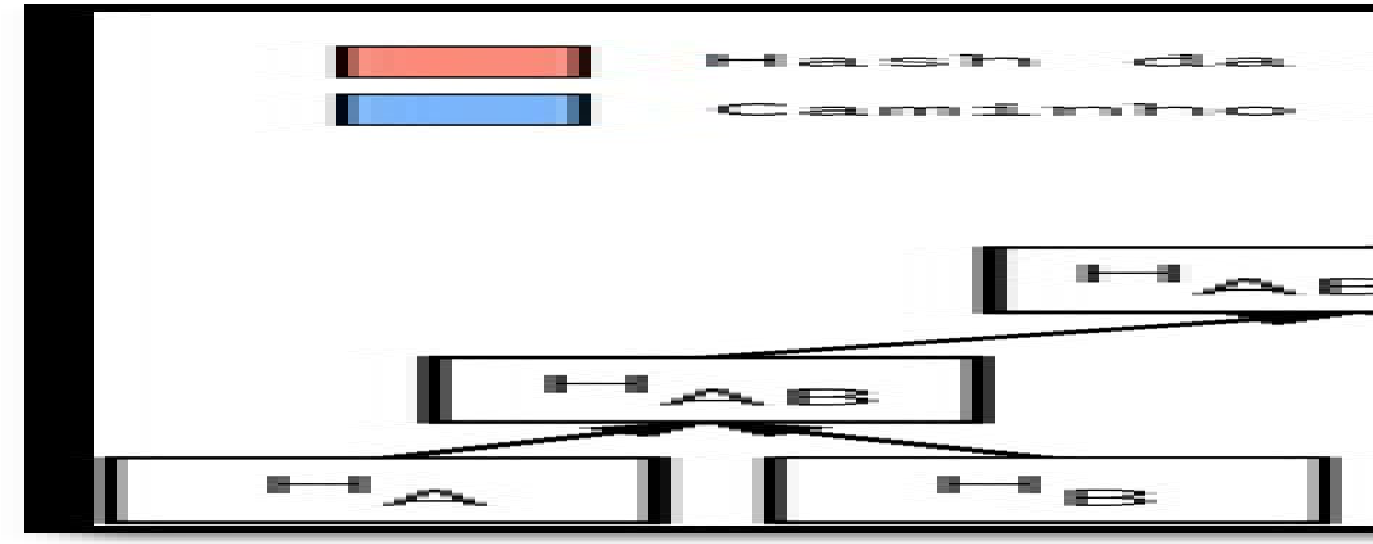

Figure 7: Merkle tree. SOURCE Marco Agner (2016).

According to Nobre (2014), "with the evolution of cryptography over the years, nowadays there are safe and efficient mechanisms, such as Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES), which are the base algorithms for the used protocols. Currently, the two most commonly used protocols for data protection on the Internet, Secure Sockets Layer (SSL), and Transport Layer Security (TLS) use symmetric encryption to protect data transmitted and stored. However, symmetric encryption has an important challenge and that it is impossible to resolve, with this paradigm in question a new type of encryption has emerged, the asymmetric, in which two distinct keys are used, but which complement to store the "Information."

Internet Banking uses on most systems the SSL protocol and digital certificates to ensure the Users safety when accessing their Network, beyond this Protocols virtual keyboard are also used. This technology makes possible to ensure that password input within the system cannot be captured by ill-intentioned third parties. Other features of the Internet Banking In relation to security is defined

by the Adachi (2004), as follows: "The system has basically three points: the bank that is the supplier of Services and transactions, the electronic channel user and the communication network which is the provider of access to the Internet, Therefore, in this technology the security depends on the three points and the way it is used by your users".

Availability

Recently with the advancement of smartphones in addition to the technologies cited above, it has become possible to make use of biometrics and tokens to access and carry out transactions through Mobile Banking which facilitates further people’s access to that system. Now we enter another topic to be discussed in this article: Availability.

A common feature of both systems is that they are available virtually 24h a day and can be accessed from anywhere by their users both via Mobile applications or Internet pages. This is primarily due to the fast advancement of Smartphones and operators, which through their network enable users to connect to the Internet from various locations, for example, users just have a mobile device or a Tablet to be connected, unlike some years ago when Internet usage was limited only to Desktop's and notebooks.

Recently, Internet Banking systems have also been adapted for Mobile Banking providing its users with easier to access Interfaces and mechanisms. It is worth pointing out that due to its youth Blockchain doesn’t have a widespread mobile applications system. However, its cryptographic characteristics allow transactions to be performed using QR codes in cell phones, which facilitate peer-to-peer transactions.

Regarding users ' identity confidentiality, i.e. data confidentiality. Internet Banking saves on its system all the data from the transactions. This data brings several personal information about its users, such as names, account numbers, transferred values, transactions conducted among other data.

In this aspect, Blockchain differs greatly from the Internet Banking, within the network data from users and transactions are not revealed and are conducted in a Peer-to-peer way. Blockchain transactions are made anonymously and, in the ledger, only the public keys of those who held the transaction and the value transferred are registered. Because Blockchain watches over the anonymity of its users, it makes it easier for people with dubious intentions to take advantage of this anonymity. Recently, techniques for tracing the transactions were proposed, but nothing shows the exact location or user of a transaction.

RESULTS AND DISCUSSION

Comparing the two technologies, it is possible to observe great differences in how their systems work. To say nowadays that one is more secure than the other is something extremely risky. However, considering the historical data and the security features, we can suppose that Blockchain is the most reliable technology now.

We believe that this reliability lies on the Blockchain peer-to-peer transaction fashion. What, in our conception, might discourage frauds. However, further research is still necessary to be able to confirm such statement. We find important to emphasize a few characteristics of Blockchain that make it save according to our research. The transactions are independently checked, in a decentralized system, by various miners. All the transactions have a hash, a digital signature, and asymmetric cryptography.

Internet Banking, despite its current growth in its security system, still needs some improvement, mainly to prevent malicious people from making use of fake pages copies to deceive users, another factor that hinders security is the fact that banks have large amounts of centralized data and this makes it easier for those who invade the network to gather a lot of information. We also find important to highlight that internet banking seems to be superior when we consider how easy it is to access it, especially with the addition of mobile banking that implements protections such as biometric verification.

Table 1 shows more details of the performed comparison. The characteristics quoted are the ones that fit CIA the most, and the results were divided as follows:

- The first comparison shows whether the feature is present in the system, since they have large differences in the way they work;
- The second comparison was performed at levels and punctuated as follows:
  - Low equals to 1 point, it was assigned to those characteristics that influence directly the entire system (or most of it), and can cause major failures in confidentiality, integrity or lack of availability;
  - Medium equals to 2 points, it was assigned to those characteristics directly related to availability of information and data transference;
  - High equals to 3 points, it was assigned to those characteristics that have a high degree of confidentiality, integrity and availability;
- At the end we total the scores of the characteristic to evaluate which one is higher.

Table 1 – The characteristics of the Internet Banking and Blockchain.

Features	Internet Banking				Blockchain			
	Present	Low	Medium	High	Present	Low	Medium	High
Centralized system	Yes	X			No	-	-	-
Decentralized system	No	-	-	-	Yes			X
Availability 24 hours a day	Yes		X		Yes		X	
Mobile availability	Yes			X	Yes	X		
Web availability	Yes			X	Yes			X
Ease in global transactions	Yes	X	-	-	Yes			X
Access tokens	Yes			X	Yes			X
security keys	Yes			X	Yes			X
Encryption protocols	Yes	X			Yes			X
Double Transactions Checks	No	-	-	-	Yes			X
Digital signatures-Hash	No	-	-	-	Yes			X
Biometrics	Yes			X	No	-	-	-
Virtual keyboard	Yes			X	No	-	-	-
Digital certificates	Yes			X	No	-	-	-
Anonymity of users	No	-	-	-	Yes		X	
	Rated							
	Subtotal	**3**	**2**	**21**	**Subtotal**	**1**	**4**	**24**
	Total	**26**			**Total**	**29**		

Comparing how the two technologies comply with the three pillars of information security we obtained as a result that regarding the CIA requirements the technology that fits these the most according to our parameters is Blockchain. In the matter of integrity and confidentiality, the system is more prominent primarily by the security measures that it adopts in its network, with double checks, encryption protocols, and digital signatures.

A great advantage that can be observed in both systems is that internet is virtually the only requirement. Beyond, Blockchain allows you to perform worldwide transfers and with fees lower than those of banks. However, in places with no or virtually no internet access, the availability of both systems is low.

CONCLUSIONS

At last this article concludes that all comparative goals were achieved and that despite Blockchain being something new, it has all the features to become a great security tool in the financial market, mainly by presenting advantages in the security aspect. Since 2009, Blockchain, used by the virtual currency Bitcoin, has never been tampered with.

According to the results and all the analyses carried out in this article, we conclude that, Blockchain is probably the better suited system concerning the characteristics of the pillars of information security, the CIA, and that it is of utmost importance that technology professionals keep an eye for future implementations that this system can integrate. Besides thinking of possible improvements to make it more available and accessible.

For Internet Banking, an alternative to solve security problems is the possible adoption of the security features present in Blockchain in their network, this has been happening in some institutions which have been conducting studies for future implementations. To ensure better security for their users and greater integrity of the circulating data.

REFERENCES

ADACHI, Tomi. **Gestão de segurança em internet banking: estudo de casos brasileiros.** Available at: <http://bibliotecadigital.fgv.br/dspace/handle/10438/2339>. Published on 15/12/2004. Acessed in: 06/05/2017.

AGNER, Marco. Bitcoin para programadores. Available at: < https://itsriodejaneiro.gitbooks.io/bitcoin-para-programadores/content/intro.html>. Published on: 02/03/2016. Acessed in: 11/08/2017.

BLOCKCHAIN.INFO **Estatísticas do Bitcoin.** Available at: <https://blockchain.info/pt/stats>. Acessed in: 20/05/2017

CASTRO, Felipe Infante. **O básico sobre o blockchain (e tudo que está em jogo)**. Available at: <http://braziljournal.com/o-basico-sobre-o-blockchain-e-tudo-que-esta-em-jogo>. Published on 01/07/2017. Acessed in 05/10/11.

CERT.BR. **Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil.** Available at: <https://www.cert.br/stats/incidentes/2015-jan-dec/fraude.html>**.** Acessed in 07/05/2017.

EOBOT. Mineração na nuvem. Available at: <https://www.eobot.com/fee>. Published on 2017. Acessed in 05/10/2017.

Febraban. **Pesquisa FEBRABAN de tecnologia 2017.** Available at: <https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%C3%A1ria%202017.pdf > Acessed in 06/10/2017.

FILHO, Márcio Barbosa de Oliveira. **Utilizando o protocolo bitcoin para condução de computações multilaterais seguras e justas.** Available at: <http://repositorio.ufpe.br/handle/123456789/17143?show=full>. Published on 22/06/2016. Acessed in 07/05/2017.

MAIA, Marco Aurélio. **O que é a segurança da informação.** Available at: <http://segurancadainformacao.modulo.com.br/seguranca-da-informacao>. Published on 19/08/2013. Acessed in10/05/2010.

MATOS, Mário. **Internet Banking**. Available at: <http://bancario.pt/internet-banking-e-banking/#ixzz4qKRz4aTo>. Published in 28/02/2013. Acessed in 20/08/2017

NOBRE, Erick Pedretti. **Criptografia, você deveria conhecer**. Available at: <https://canaltech.com.br/seguranca/Criptografia-voce-deveria-conhecer>. Published in 11/05/2014.

PALMA, Fernando. **CID: Confidencialidade, Integridade e Disponibilidade.** Available at: <https://www.portalgsti.com.br/2016/11/cid-confidencialidade-integridade-e-disponibilidade.html>. Acessed in 20/08/2017.

RAMOS. R, **Moedas Virtuais**, Available at: <http://www.infoescola.com/economia/moedas-virtuais>. Acessed in 15/0/2017

STELLER, Fernando W.; CERQUEIRA, Aurimar H. **Cinco princípios básicos da Blockchain**. Available at: <http://cio.com.br/tecnologia/2017/03/06/cinco-principios-basicos-do-blockchain/>. Published on 06/03/2017. Acessed in 20/05/2017.