DOI: 10.14488/BJOPM.2019.v16.n2.a9

ISSN 2237-8960
Brazilian Journal of Operations & Production Management

BLOCKCHAIN BASED MFA SOLUTION: THE USE OF HYDRO RAINDROP MFA FOR INFORMATION SECURITY ON WORDPRESS WEBSITES

João Antonio Aparecido Cardoso
joaocardoso87@hotmail.com
Federal Institute of Education, Science and Technology of São Paulo – IFSP, Bragança Paulista, São Paulo, Brazil.

Felipe Takeshi Ishizu
felipetakeshi16@gmail.com
Federal Institute of Education, Science and Technology of São Paulo – IFSP, Bragança Paulista, São Paulo, Brazil.

Jeferson Tadeu de Lima
jtlima200@gmail.com
Federal Institute of Education, Science and Technology of São Paulo – IFSP, Bragança Paulista, São Paulo, Brazil.

Jefferson de Souza Pinto
jeffsouzap@ifsp.edu.br
Department of Manufacturing Engineering and Materials. State University of Campinas – UNICAMP, Campinas, São Paulo, Brazil.
Federal Institute of Education, Science and Technology of São Paulo – IFSP, Bragança Paulista, São Paulo, Brazil.

ABSTRACT

Goal: The present work aims to present how the use of a blockchain two-factor authentication solution 2FA on a page developed on WordPress can contribute to the information security regarding user authentication.

Design/Methodology/Approach: The research method employed is characterized as an exploratory research, since all the analysis is based on the theoretical reference data available on the subject. A field research was carried out in relation to the implementation of the multi-factor authentication plugin Hydro Raindrop MFA, which uses blockchain technology offered by The Hydrogen Technology Corporation and the Project Hydro platform over the Ethereum network. Thus, this paper sought to present and conceptualize some of the technologies used, pointing out their contribution to information security.

Results: The main results showed that the use of decentralized technology, such as blockchain and the Hydro Raindrop Plugin, can contribute considerably in the process of user authentication, which may strengthen the safeguard of the information and assets of individuals and organizations by inhibiting or reducing the possibility of successful hacker attacks. This solution is at the forefront of innovation with regard to data security because it uses advanced blockchain technology. It might contribute in a satisfactory way to the preservation of critical data and information that are the core value of many organizations of the industry 4.0.

Limitations of the investigation: This research was limited to analyzing how the implementation of the Hydro Raindrop multi-factor authentication solution on a WordPress page can be beneficial to ensure information security.

Practical implications: This study's findings can contribute to entities interested in cybersecurity. As a suggestion for future works, analyses of plugins or similar solutions available on the market in distinct types of websites, or performance comparisons between them, may be relevant to contribute to scientific research.

Originality/Value: This work can contribute in an innovative way to scientific research, since it addresses a recently created solution that uses blockchain technology as its basis for a safer method of authentication.

Keywords: Authentication; 2FA; Blockchain; Information Security; Hydro Raindrop.

ABEPRO
DOI: 10.14488/BJOPM.2019.v16.n2.a9

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

1. INTRODUCTION

The recent developments in Information Technologies are fomenting the fourth industrial revolution, in which physical goods are no longer the main source of value creation, and the growing role of the digital economy makes intangible assets play a vital role in business processes and the economy altogether. For this reason, preserving the integrity of data generated by several sources in the new digital economy is a key challenge (Jeny, 2018).

With the expansion of services provided on the Internet, there is a need to implement technologies that provide users with an experience of reliability and integrity of the information sent and received while accessing Internet pages or applications. One of the most commonly used form of access to applications or websites is login and password authentication, which ensures that only properly-recognized users can access information or services. However, just as there is an evolution in the services provided, there is also an increase in malicious activity seeking to have access to sensitive information or cause the unavailability of the services (Tiwari et al., 2016).

Companies that offer online services try various ways to defend themselves against illegal access to their customers' data, but even with the use of strong passwords created in accordance with the directives required by network administrators, user data may be at risk. Data theft does not exclusively affect social network accounts or email services while using the Internet; bank accounts or confidential business data can also be targeted by cybercriminals, which forces institutions to implement tools that authenticate the login process on their systems (Wiśniewska, 2018).

To prevent attacks, according to Claessens et al. (2002) apud Vieira and Ruggiero (2007), [...] there are works that propose the use of cell phones as a token that receives SMS messages as a way to send the OTP (one-time passwords) to the client. This method is relevant due to its use of separate channels; it is therefore more difficult for an attacker to gain control. However, this represents an additional cost for each authentication. The purpose of this paper is to analyze the advantages and disadvantages of a two-factor authentication (2FA) solution based on blockchain technology, which was implemented on a test page based on WordPress to examine if this solution can be an alternative to safeguard the integrity and reliability of websites or applications.

2. THEORETICAL FRAMEWORK

Information Security

According to Ferreira (2003, p. 1), "Information is an asset that, like any other important asset, has value to the organization and, therefore, needs to be adequate and protected. Information security protects information." Personal and sensitive data, in general, should not be trusted in the hands of third-parties, where they are susceptible to attacks and misuse (Zyskind et al., 2015).

In the digital era of Industry 4.0, companies cannot afford to ignore digital trust, as digital ecosystems can only function efficiently if all parties involved can trust in the security of their data and communication, as well as the protection of their intellectual property (Geissbauer et al., 2016).

Security is one of the most important concerns in an Industry 4.0 implementation, given that vulnerabilities introduced during manufacturing (e.g. hardware Trojans and backdoors) can be difficult to detect (Lin et al., 2018).

Information security is vital for any industry that wants to protect its data, not only due to common losses, for example, misplacement of servers, but also in terms of external threats from people of different types motivations for illicit purposes (Hajdarevic et al., 2012; Corrêa, 2018).

Information Security can be defined as an area of knowledge dedicated to the protection of information assets from unauthorized access, improper alterations, or unavailability (Sêmola, 2003, p. 43). Security can be compromised by some attitudes of its users, by the environment or structure surrounding it, or by malicious individuals with the objective of stealing, destroying, or altering information (Warkentin and Willison, 2009; Corrêa, 2018).

Therefore, in order to guarantee the security of information, it is fundamental that companies that offer the most diverse types of services, mainly in the financial sector, use advanced methods of authentication and encryption.

Authentication is a process of verifying the identity that appears in a system, that is, the system verifies the credentials of who is trying to access with those that are in the database. If successful, access to the system is allowed because the credentials have been validated. Authentication is divided in two ways, the first being identification, which would be the presentation of the identity to the system as login and password, and the second as verification, which compares the given identification with the stored data (Fares, 2015).

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

Multi-Factor Authentication

Single-factor verification is the most popular way of protecting data and accounts with two simple information: log-in and password. Passwords can create a dilemma: weaker passwords are easy to remember; however, they are easy to guess. On the other hand, strong passwords can be difficult to guess, but they are also difficult to remember (Donohue, 2014).

Using passwords is still the most common way to authenticate or prove identity online, but this method offers diminishing protection, as hackers can use a variety of phishing attacks, brute-force attacks, attacks on web applications, and intrusions at points of sale to steal passwords and cause considerable damage (Mckeown, 2017).

Passwords do not provide sufficiently strong identity verification. In fact, any individual who obtains the password is able to log into that account and have access to sensitive data. In addition, account security is based solely on password strength, which in many cases is not adequately strong, since users favor simple solutions and most of the time do not like to remember a string of characters containing large, numeric, and special characters (Dacanay, 2017).

As such, users often facilitate hacker activity by choosing weak passwords, using the same password for multiple applications, and keeping the same password for extended periods of time. These practices, although helpful for them to remember their logins, invite hackers to come in through the front door (Mckeown, 2017).

In this sense, to ensure information security, it is important to use multi-factor authentication (MFA) methods, also known as: step authentication, advanced authentication, two-step verification, and two-factor authentication. These are security systems that require more than one method of authenticating credential-independent categories to verify the user's identity for a login or other transaction (Rouse, 2015).

Unlike typical single-factor authentication, MFA requires users to prove their identity by providing at least two pieces of evidence in three main categories: what users know, what users have, and what users are (Mckeown, 2017). According to Figure 1.

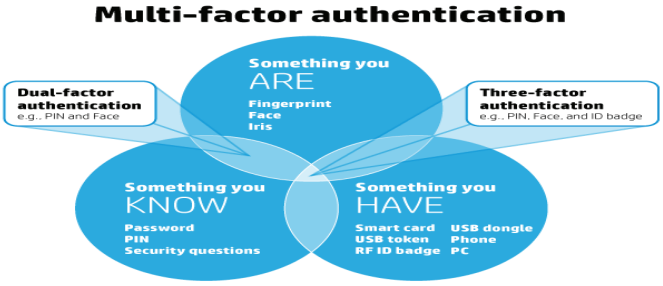

Figure 1. Multi-Factor Authentication.
Source: Adapted from Lambauer (2016).

According to Wiśniewska (2018), "the multi-factor authentication (MFA) method involves the use of at least three elements between: something the user knows, something the user is and something the user has":

"a) Something the user knows - It can be a sign or a typical PIN that must be entered in an appropriate window. The level of security of this type of factor depends on length and complexity (use of distinct types of alphanumeric characters - both 1,2,3 and XyZ).

b) Something that the user is - The ability to identify faces or read fingerprints is still not widely used and has already been partially questioned as an effective security method. As it happens that the fingerprint can be falsified, and intruders can also deceive the facial recognition tool with a mask or photograph.

c) Something that the person has - It can be a pen drive connected to a computer, a card to open doors, a telephone to receive a code via SMS, or other items that will allow users to access it." (Wiśniewska, 2018).

The multi-factor authentication method using SMS services is used by many organizations and services; however, SMS text message scans and unique codes are still susceptible to phishing attempts by hackers, as hackers can clone a telephone number and intercept the SMS authentication message, allowing unauthorized access to services (Coldewey, 2016). Unfortunately, the special passcodes generated by traditional two-factor authentication systems usually consist of a string of random numbers, which can make them easy to phish since a hacker will merely need to trick users into disclosing their special codes (Kan, 2018).

According to Rouse (2015), there are other factors that can add extra layers of security to the authentication process, such as:

"Location factors - the user's current location is generally suggested as a fourth factor for authentication. Once again,

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

the omnipresence of smartphones can help ease the burden of authentication: users typically carry their phones, and most smartphones have a GPS device, allowing reasonable confirmation of the login location. Time Factors - The current time is also sometimes considered a fourth factor for authentication or, alternatively, a fifth factor. Checking employee IDs at work times may prevent some types of user account attacks. A bank client cannot physically use their debit card in the United States, for example, and then in Russia 15 minutes later. These kinds of logical locks can prevent many cases of online banking fraud". (Rouse, 2015)

The principle of the MFA is that each factor compensates for the weakness of the others. For example, authentication factors about "something the user knows" such as passwords and PIN codes may be susceptible to brute force (hackers forcing logins) or social engineering attacks. Thus, administrators can complement the security of their assets by adding a self-stressing factor that is not as easy to guess as "something the user has" by authenticating users through their mobile devices or "something they are," such as a biometric fingerprint factor, iris or voice. Unless the hacker has all the factors required by the system, they will not be able to access the account (Dacanay, 2017).

When a company requires its employees to provide more than one factor for authentication in order to grant access to their data, it becomes more difficult for a criminal to impersonate an employee. A password theft alone is no longer enough to access data and services, and without the additional physical element needed, a cybercriminal will encounter more challenges to succeed in his attack (Ghiorzoe, 2014).

Thus, the purpose of multi-factor authentication is to create an extra layer of defense and decrease the feasibility that an unauthorized person will be able to access a target, such as a physical location, a computing device, network, or database (Rouse, 2015). If one of the factors is compromised by a hacker or unauthorized user, the chances of another factor also being compromised are low; therefore, requiring multiple authentication factors provides a higher level of assurance on the user's identity (Dacanay, 2017).

Although traditional 2FA authentication solutions using smartphones and SMS messages can add an extra layer of security, they are not failsafe as a security researcher has released a tool that can bypass a host of two-factor authentication (2FA) schemes widely used across platforms such as Gmail and Yahoo (Afifi-Sabet, 2019).

Industry 4.0 complex systems will require a more robust security solution (Lin et al., 2018). Thus, it is fundamental to have an alternative and impenetrable way of multi-factor authentication that ensure information security. One of the innovative technologies being used and studied for this matter is blockchain.

Blockchain

The term "blockchain" is used to refer to a data structure that can be defined as an ordered list of blocks, where each block contains a small (possibly empty) list of transactions, and each block in a blockchain is "chained" (Xu et al., 2017). Via this chain, each piece of data can be traced back towards its primary source. The data system itself, therefore, provides the trust (Horenberg, 2017). In this case, the blockchain cannot be deleted or altered without invalidating the hash chain (Xu et al., 2017). As can be seen in Figure 2.

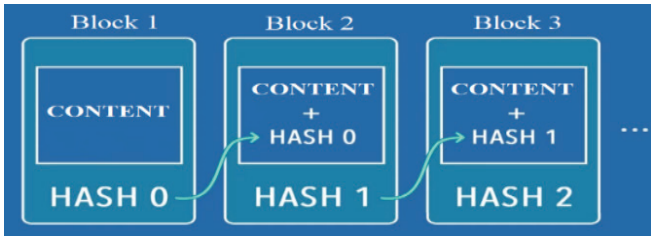

Figure 2. Blockchain.
Source: Damasco (2017).

It is an integrated construction of infrastructure in several fields, composed of six key elements: decentralization, transparency, open source, autonomy, immutability, and anonymity (Lin and Liao, 2017).

Instead of having a central administrator like traditional databases, a blockchain is a distributed ledger that exists across several locations or among multiple participants, synchronized using the Internet, and visible to anyone within the network (Arcos, 2018).

A blockchain is a distributed database that maintains a growing list of data records that are protected against tampering and revision, even by operators of the data storage nodes (Fanning and Centers, 2016). The blockchain contains a certain and verifiable record of each transaction made in its network (Crosby et al., 2016).

Thus, Pilkington (2016) apud Chicarino et al. (2017) define blockchain as:

> *"[...] a concept aimed at decentralization as a security measure. They are distributed and shared records and databases that have the function of creating a global index for all transactions that occur on a given network. It works as a ledger, only in a public, shared and universal way, which creates consensus and trust in direct commu-*

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

> *nication between two parties, that is, without the intermediary of third parties. It is constantly growing as new complete blocks are added to it by a new set of records. The blockchain can also be used for supply chain communications, smart contracts, digital identity management, and several other applications" (Pilkington, 2016).*

The idea of a distributed and resistant network to attacks and attempts of fraud and tampering is remarkably interesting for permanent and unalterable storage of data of any nature (Lucena and Henriques, 2016; Cai and Zhu 2016).

In this sense, one of the advantages of using blockchain for data storage is the confidence generated, seeing that the data contained in it cannot be erased. A zone of credibility is created on the system, which allows the transactions performed to be considered as integral and legitimate (Staples et al., 2017; Garrote and Pazos, 2018).

Applications of Blockchain Technology

Industry 4.0 technologies can offer many advantages; however, it requires effective integration of many technologies and systems, and seamless operations across all components of the chain, which creates many challenges regarding trust, traceability, and reliability. Nonetheless, several of these challenges can be addressed using blockchain (Zhou et al., 2015 apud Mohamed and Al-Jaroodi, 2019).

For the operation of a blockchain, a decentralized peer-to-peer network is crucial, since in this way all changes (additions) in it can be checked and accepted (or rejected) by most of the peers, thus preventing the insertion and consolidation of incorrect information (Swan, 2015).

Transactions are stored in blocks interconnected to one another, and each block is connected to only one block before it, resulting in a sequential chain of blocks in which before being added to the chain, each block is validated by a computational mathematical process called mining (Garay et al., 2015).

The peer-to-peer network is decentralized and relies on its users to function because their information is not stored on a central server, and each user shares pieces of information with other network users, ensuring greater scalability (availability, connectivity, and performance), adaptation to failures, acceleration of communications, and reduction of costs related to infrastructure (Pourebrahimi et al., 2005; Antunes et al., 2015).

The blockchain concept is capable of accomplishments far beyond a technological innovation seen that it can change the way of conducting business centrally to a decentralized form. It thus confers trustworthiness to the execution of transactions between distributed and mutually unreliable agents, without the necessity of an intermediate entity trusted by both (Chicarino et al., 2017; Shyamasundar and Patil, 2018).

Industry 4.0 denotes the flexibility of products and services to be shared over the Internet or other networks, and it is expected to attain the circumstance of decentralization and self-regulation offered by blockchains (Tama et al., 2017).

Blockchain technology is a catalyst for emerging use cases in the financial and nonfinancial industries such as industrial manufacturing, supply chain, and healthcare. Additionally, it can play a pivotal role in transforming the digitization of industries and applications by enabling secure trust frameworks, creating agile value chain production and tighter integration with technologies such as cloud computing and IoT (Ahram et al., 2017).

Blockchain refers to a technology rather than a particular product, and its applications are already diverse (Arcos, 2018). Some of the key information security challenges can be addressed by using the decentralized, autonomous, and trustless capabilities of blockchain (Kshetri, 2017).

This technology can be used for data management to store and ensure the privacy of enormous quantities of personal and sensitive information (Zyskind et al., 2015).

Blockchain technology can benefit businesses that deal with costly, slow, or unreliable transactions, or ones that serve markets with underdeveloped payments systems or large numbers of unbanked customers (Rabah, 2017).

The service sector is one of the major beneficiaries of the blockchain, insofar as from its use, two anonymous parties can do business with each other, through the Internet, with encryption to provide the necessary security and guarantee the inalterability of transaction, reducing the risk of third-party violation or human error (Dinh et al., 2017).

The blockchain technology has remarkable advantages related to automation, transparency, auditability, and cost-effectiveness that can contribute to saving costs and improving efficiency by allowing payments to be finished without any bank or any intermediary. Moreover, it can be used in several financial services such as digital assets, remittance, and online payments, which may represent a disruptive innovation for many varieties of contracts and business activities (Atzori, 2015).

These characteristics presented by blockchain can be beneficial to companies that deal with data authenticity

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

and can be used for the purpose of proof of identity, as it not only stores data that can be used to identify someone or something, but also provides basic security concepts for identification and authentication (Drescher, 2018).

Hydro Raindrop MFA

The Hydro platform enables organizations to utilize the capabilities of blockchain technology to ensure the security of information, transactions, confidential documents, and more. It is implemented in Ethereum's blockchain network, a public open-source blockchain platform launched in 2015.

Built on Hydro's distributed public ledger, there is a blockchain-based authentication service called Hydro Raindrop. This service provides an extra layer of security that helps verify that an access request is coming from an appropriate source. Hydro Raindrop provides a way to improve off-chain authentication protocols by incorporating blockchain mechanics as a component of a single-factor or a multiple-factor authentication process.

This novelty can create a useful security layer to help prevent system violations and data breaches because the distributed, public, decentralized nature of the Ethereum network blockchain ledger adds a new step that can make authentication more robust.

Thus, with Hydro Raindrop, authentication can leverage the power of blockchain technology and be applied as a precondition that interacts seamlessly with standard off-chain processes.

Because the ledger is in a distributed and decentralized network, transaction processing is not subject to single points of failure. This activity on blockchain provides reasonable security against failures since the transactional aspect of the Hydro Raindrop server can remain functional without relying on any trusted party. The public nature of the ledger also ensures that any party (whether a private system or a verified user) can monitor authentication attempts from anywhere in the world in real time. Blockchain technology offers transparency through the value chain (Arcos, 2018). Such a level of transparency is a substantial advantage, particularly when it comes to authentication systems that house sensitive and expensive data.

3. METHOD AND STUDY OBJECT

A qualitative research is exploratory, and researchers use it to explore a topic with the purpose of familiarizing themselves with a subject that is to be further examined (Creswell, 2009; Cooper and Schindler, 2013). Thus, this study consists of an exploratory research in which the authors acquainted themselves with a topic that needs to be investigated. This research seeks to deepen knowledge about information security and multi-factor authentication technology. In addition, this study has a qualitative approach where researchers collect data themselves through examining documents, observing behavior, or interviewing participants. They may use an instrument for data collection, but the researchers are the ones who gather the information without the need of using or relying on questionnaires or instruments developed by other researchers (Creswell, 2009).

Regarding the means of investigation, the field research, according to Vergara (2009, p. 43), is an: "empirical investigation carried out in the place where a phenomenon occurs or occurred or that has elements to explain it. It may include interviewing, questionnaire application, testing and participant observation or not." The data for this analysis was therefore obtained in a field research in which the researches implemented a multi-factor authentication plugin based on the blockchain technology offered by The Hydrogen Technology Corporation and Project Hydro platform on a WordPress website. It is also based on the documentation available regarding the Hydro Raindrop authentication plugin, data encryption, blockchain technology, and information security.

For the purpose of this study, a template webpage was created by the researchers using the WordPress website builder, and the page was hosted for free on the hosting service offered by 000webhost.com. The website object of this study can be accessed through the URL "ssiifsp.000webhostapp.com."

This method of research allowed a confrontation between theoretical knowledge guided by bibliographic references that exposed the positioning of authors who deal with studied subjects from different perspectives and the facts of reality, which were examined by the researchers while performing the implementation of the Hydro Raindrop authentication plugin on the test website.

According to the Merriam-Webster Dictionary (2019), empirical means "based on observation or experience." Therefore, this study's data was analyzed based on the researchers' empirical experience during the use of the authentication tool. The researchers have examined different documents regarding information security, blockchain technology, and the Hydro Raindrop MFA plugin. Moreover, performance tests were carried out on the plugin along with internal group discussions to evaluate their findings and observed experience with respect to the use of the Hydro Raindrop MFA plugin as an authentication tool.

This work aimed to compare the theoretical framework

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

regarding information security and to use empirical experience to analyze the possible advantages and disadvantages of using the blockchain based plugin Hydro Raindrop MFA as a multi-factor authentication solution to guarantee the safeguard of information during user-authentication proceedings.

4. HYDRO RAINDROP CONFIGURATION

The Hydro MFA plugin adds another layer of security to websites or apps using the blockchain-based authentication layer. It is designed to work immediately, providing unmatched security standards for sites and their users. To activate the Hydro Raindrop MFA plugin from the administrator side of a website or application, some configuration steps are necessary.

First, the administrator must create an account on Hydrogen's website "hydrogenplatform.com" and then request access to the production APIs. After access is approved by Hydrogen, the administrator must generate a Client ID, Client Secret, and Application ID, as can be seen in Figure 3.

In the WordPress dashboard, the administrator must go to the plugin tab, perform a search for the Hydro Raindrop MFA plugin, and install it. After installing the plugin, the administrator must navigate to Hydro Raindrop MFA Plugin Set-

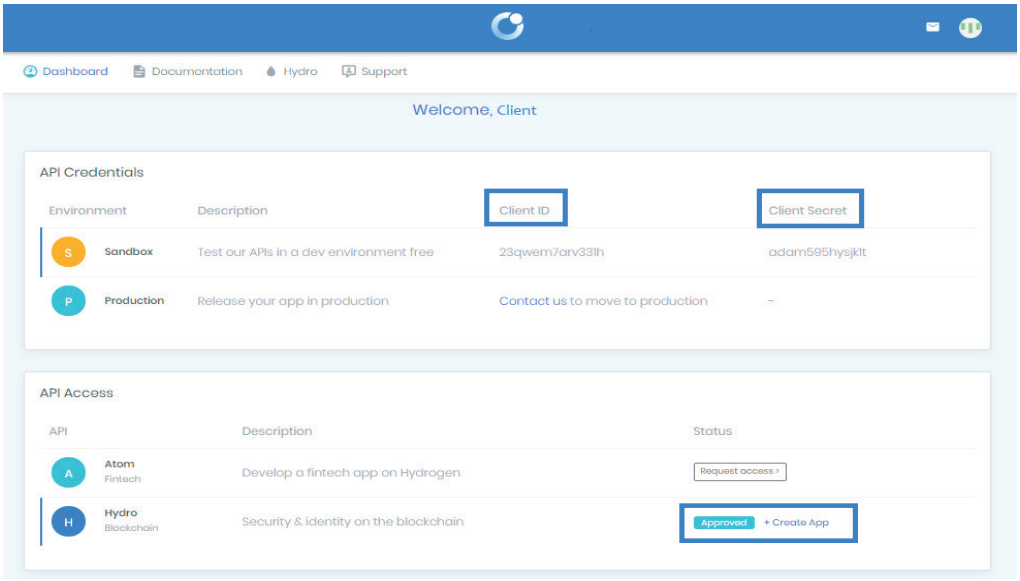

Figure 3. Hydrogen Dashboard.
Source: Hydrogen Technology Corporation (2018).

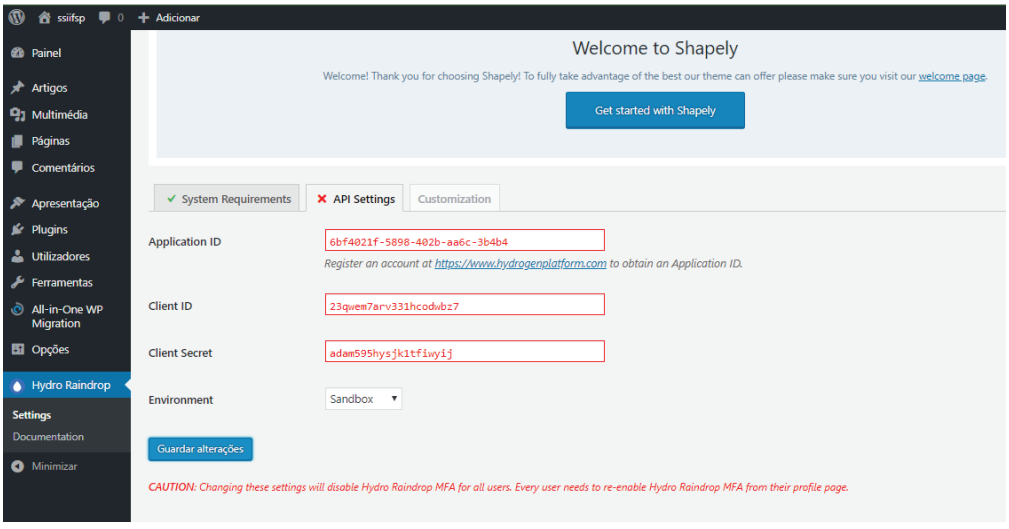

Figure 4. Hydro Raindrop plugin configuration on WordPress.
Source: The authors (2018).

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

tings and enter the data obtained in the Hydrogen account dashboard regarding its use: Application ID, Client ID, Client Secret, and the plugin is ready for use, as shown in Figure 4. However, for the plugin to work properly, the webpage or application on which the plugin is being configured must have SSL (HTTPS) enabled and PHP 7.0 or higher.

Setting up Hydro Raindrop on a Smartphone.

For the activation of the Hydro Raindrop MFA plugin on the user side, some configuration steps are mandatory. Users of the website or application on which the multi-factor authentication plugin is to be implemented need to download the Hydro application from any app store. The Hydro application is free and available for Android and iOS smartphone users.

To connect the Hydro application to the service in which the authentication plugin was configured, users must authenticate to the website with their "login and password" credentials as usual. However, after they have logged in, the Hydro Raindrop MFA plugin configuration page should be displayed so that users who wish to configure this plugin as an extra layer of security can inform the unique identification data generated in the Hydro application. In the Hydro ID profile field displayed on the page, users need to enter the Hydro ID generated on their mobile application Hydro App, as seen in Figure 5.

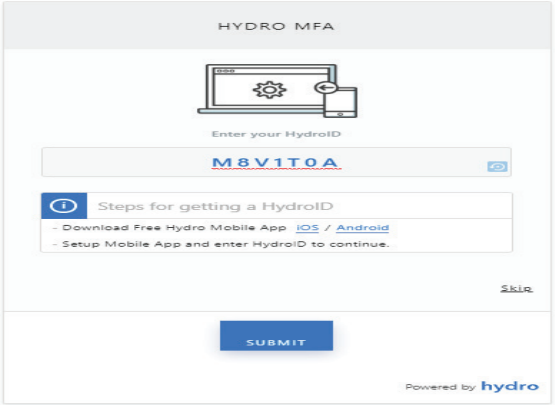

Figure 5. Setting up the Hydro Raindrop plugin on WordPress.
Source: The authors (2018).

After the submission of the Hydro ID in the requested field, the website will display a 6-digit code, as Figure 6 displays.

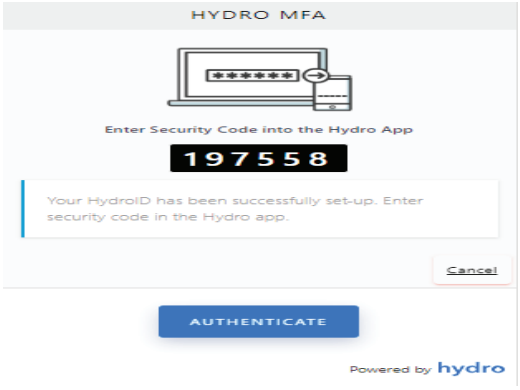

Figure 6. Token generated.
Source: The authors (2018).

After that step, users must enter the 6 digits displayed on the website into the Hydro App on their mobile devices, as shown in Figure 7, thus establishing a secure connection and connecting the smartphone device to the website plugin.

Figure 7. Application screen on which to insert the token.
Source: The authors (2018).

As a result, the token will be validated by the app through a process of consulting the Hydro blockchain, and the website or application on which the authentication plugin is being configured will be enabled to support multi-factor authentication based on blockchain. That can be seen in Figure 8.

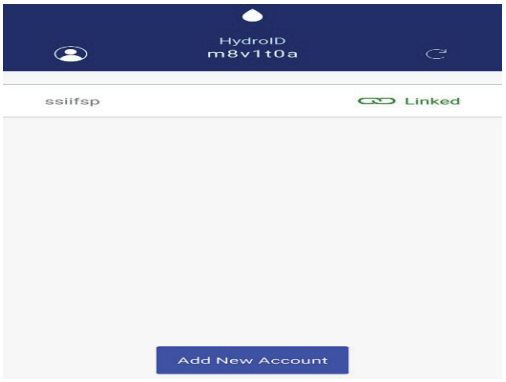

Figure 8. Validated Token.
Source: The authors (2018).

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

After this configuration process is finished, on any occasion that a user wants to log into the website on which the process was carried out, it will not only require username and password as usual, but also the user will need to enter into the Hydro App a randomly generated security code. That code is displayed on the page after their username and password are accepted. This method consequently provides an extra layer of protection.

5. RESULTS

After examining the documents related to the Hydro Raindrop MFA plugin and the theoretical references related to information security and blockchain technology, along with performance tests on the plugin and group discussions, the researchers concluded that Hydro Raindrop enables new and existing private systems to seamlessly integrate. Furthermore, it leverages the immutable and transparent dynamics of a public blockchain, using cutting-edge encryption to protect user accounts, documents, applications, transactions, payments, and more.

The Hydro Raindrop MFA Plugin showed to be an innovative solution using blockchain technology, which is in the vanguard of data security solutions and might subsidize the protection of vital data and information that have essential value for countless organizations of the industry 4.0.

Some advantages of the Hydro Raindrop multi-factor authentication plugin that could be verified during testing is that it provides an extra layer of security for users employing secure blockchain technology encryption. That is due to the fact that the data used to validate the users' access is stored in a public and decentralized database, thus guaranteeing its functionality and reducing the possibility of the service being down. That is on account of the fact that the information is saved in a decentralized way without a single point of failure, which is positive for information security according to Antunes et al. (2015).

The application generates a unique ID, which is saved in a public blockchain. Once the information has been permanently saved in the blockchain, when the user wants to authenticate or log into a site, the Hydro Raindrop application queries this data in the blockchain. If the information is true, the application validates the access. This consultation process has no costs, which has a positive impact for businesses as it is important to secure data and also to reduce authentication costs, which was a matter also discussed by Claessens et al. (2002) and Antunes et al. (2015). There is only one cost when the user sets up the application for the first time on the device and their ID is recorded in the Ethereum blockchain. Nevertheless, this cost to record the information in the blockchain is borne by the company Hydrogen. It does not incur costs to the users of the authentication platform, nor to the administrators of the services that use the plugin. This is one of the main advantages relating to the use of smart contracts and the blockchain technology, as they have the potential to significantly reduce transaction costs, which are key factors to the New Institutional Economy (Gomes, 2018).

The application has proven to be secure because in the traditional 2FA authentication process users are required to inform the unique access codes (OTPs) generated on their smartphone devices, web pages, or applications, thus allowing this data to be collected by hackers. However, the authentication process through the Hydro Raindrop application differs from the most common 2FA authentication methods available on the market, since once the user has entered their access credentials on the website or service that they wish to access, a unique OTP number sequence will be displayed on the access page. This sequence must be informed by the user on his mobile application Hydro App. This process therefore reduces the possibility of unauthorized access and data leaks because even if users enter their access credentials on a fake page in a phishing attempt, the website will not have the Hydro Raindrop plugin configured, and access will not be accomplished.

In this way, as the authentication process using the Hydro application occurs differently, it ensures that login information is exchanged over a secure connection to an official website or application. Unauthorized access by hackers or their attempt to capture information login through the use of phishing pages, which would circumvent the risks of automated phishing attacks highlighted by Kan (2018) and Afifi-Sabet (2019), is inhibited.

As the configuration of this solution occurred by installing preconfigured plugins, the time elapsed for the installation and configuration process was inferior to 10 minutes. Moreover, it was simple and fast, requiring no prior knowledge of any programming language or development skills.

In addition to plugins for WordPress pages, the Project Hydro and the Hydrogen company offer plugins for other platforms such as Joomla, Drupal, Shopify, Salesforce, Magento, and others. The company ensures that the installation of this solution in any website or application takes less than an hour, which facilitates the implementation of this extra layer of security in several platforms.

The Hydro Raindrop application demonstrates having some characteristics as a backup of the access data, where in case of damage, change, or loss of the smartphone device, the user can retrieve the authentication codes referring to the websites and applications in which Hydro Raindrop is synchronized as means of multi-factor authentication. Addi-

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

tionally, the application has Face ID and PIN protection, and the application is implementing other identity and security features such as identity management, document signing, electronic payments, and more. These features are not presented by other well-known applications available on the market, such as Google Authenticator and Authy.

6. CONCLUSION

In the digital era, huge volumes of information are collected, stored, and analyzed daily by companies; it is clear that information is an important asset in the fourth industrial revolution. For this reason, modern businesses need to have their data protected to keep their capacity to make informed decisions and to keep the safeguard of tangible assets like money, digital currencies, patents, documents, and more.

Information security and user authentication through multi-factor methods are broad topics. The most widely used authentication methods (logins and passwords) may be susceptible to various attacks, and it is imperative that information systems administrators become aware of these threats and take steps to avoid the possibility of attacks on data security and organization resources.

This paper examined a MFA multi-factor authentication method that uses blockchain technology to protect access to websites and applications over the Internet. The results of the analysis of the implementation of the Hydro Raindrop multi-factor authentication plugin on a test page created on WordPress show that the proposed solution provides an extra layer of security to control access to pages created with WordPress. Moreover, it shows that this solution can be advantageous if implemented on many other websites and applications of several types. This authentication solution is at the forefront of cybersecurity and offers the fundamentals and advantages of an inexpensive implement that can be a competitive tool for numerous organizations in the new digital economy. The use of this plugin can bring many benefits considering its use has proved simple, its implementation does not entail costs for its users or system administrators, and it eliminates the need to use additional hardware for the security of information assets. In this way, the solution can ensure information security by avoiding most of the vulnerabilities found in authentication methods available on the Internet.

The discoveries of this study can contribute to entities concerned about information security and lead to further studies of other plugins or similar solutions available on the market on other types of websites along with performance tests and comparisons between those solutions. These may be useful as a suggestion for future works to contribute to cybersecurity and scientific research.

The use of decentralized technologies such as blockchain and the Hydro Raindrop Plugin can be helpful in the process of user authentication, which can fortify the protection of information and assets of individuals and organizations by impeding or reducing the chances of a cybercriminal attack to be effective.

It should be noted that there are no fully secure and vulnerability-free environments. Thus, it is imperative that technology and information security professionals use security solutions in organizations in the process of user authentication, as multiple factors of security policies that must be followed and monitored constantly.

Information security starts with user authentication. One method involves traditional login methods demanding user and password, such as using multiple authentication factors as authentication through specific hardware using tokens, smart cards, and smartphone devices to validate users' access. Another method is through biometrics, which uses a person's physical or behavioral characteristics as a way of identifying them uniquely. In addition, other security measures can be implemented, such as location and time factors, making it impossible to access systems and data in case of attempts of access at unusual times and from uncommon locations.

Although today's authentication systems are constantly improving, thus becoming more modern and secure, a relevant element to be considered in relation to information security is the human factor. Even with strict security policies and systems, the human factor might still be the less secure point in an information security system, as humans can be affected by social hacking techniques. In these cases, individuals with malicious intentions attempt to gain access to restricted information or to physical spaces without proper permission. Therefore, it is imperative that information technology managers constantly inform employees of organizations through training and communication, elucidating the reasons for using these extra authentication factors. This education ought to happen in order for the ultimate goal to be achieved, which is to enable the authentication of users with security and preserve the integrity of information and resources of companies and individuals.

REFERENCES

Afifi-Sabet, K. (2019), "The reverse proxy 'Modlishka' tool is designed to make phishing attacks as effective as possible", available from: https://www.itpro.co.uk/two-factor-authentication-2fa/32689/phishing-tool-that-bypasses-gmail-2fa-released-on-github (access 15 Mar. 2019).

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. (2017), "Blockchain technology innovations", In 2017 IEEE Technology & Engineering Management Conference (TEMSCON), IEEE, pp. 137-141.

Antunes, F. S.; Ferreira, N. A.; Boff, S. (2015), "O Bitcoin - inovações, impactos no campo jurídico e regulação para evitar crimes na internet", In 3º Congresso Internacional de Direito e Contemporaneidade, Santa Maria.

Arcos, L. C. (2018), "The blockchain technology on the music industry", Brazilian Journal of Operations & Production Management, Vol. 15, No. 3, pp. 439-443, available from: https://bjopm.emnuvens.com.br/bjopm/article/view/449 (access 11 Mar. 2019).

Atzori, M. (2015), "Blockchain Technology and Decentralized Governance: is the state still necessary?", available from: https://ssrn.com/abstract=2709713 (access 03 Apr. 2019).

Cai, Y.; Zhu, D. (2016), "Fraud detections for online businesses: a perspective from blockchain technology", Financial Innovation, Vol. 2, No. 1, p. 20, available from: https://jfin-swufe.springeropen.com/articles/10.1186/s40854-016-0039-4 (access 16 Abr. 2019).

Chicarino, V. R.; Jesus, E. F.; Albuquerque, C. V. N.; Aragão Rocha, A. A. (2017), "Uso de Blockchain para Privacidade e Segurança em Internet das Coisas", In Livro de Minicursos do VII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Brasília: SBC.

Claessens, J.; Preneel, B.; Vandewalle, J. (2002), "Combining world wide web and wireless security", In De Decker B., Piessens F., Smits J., Van Herreweghen E. (Eds) Advances in Network and Distributed Systems Security. IFIP International Federation for Information Processing, Vol. 78, Springer, Boston, MA, pp. 153-171.

Coldewey, D. (2016), "NIST declares the age of SMS-based 2-factor authentication over", available from: https://techcrunch.com/2016/07/25/nist-declares-the-age-of-sms-based-2-factor-authentication-over (access 15 Nov. 2018).

Cooper, D. R.; Schindler, P. S. (2013), Business Research Methods, 12th ed., McGraw-Hill Education, New York.

Corrêa, R. C. V. (2018), Segurança da informação: banco de dados dos servidores do sindicato dos trabalhadores das instituições federais de ensino superior no estado do Pará, Trabalho de Conclusão de Curso (Graduação) – Faculdade de Biblioteconomia, Instituto de Ciências Sociais Aplicadas, Universidade Federal do Pará, Belém.

Creswell, J. W. (2009), Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 3rd ed., SAGE Publications, Thousand Oaks, CA.

Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. (2016), Blockchain Technology: Beyond Bitcoin. Applied Innovation, Vol. 2, pp. 6-10.

Dacanay, M. (2017), "Benefits of Implementing Multi-Factor Authentication", available from: https://www.globalsign.com/en/blog/benefits-of-multi-factor-authentication (access 15 Nov. 2018).

Damasco, R. (2017), "Blockchain: conceitos básicos e aplicações da tecnologia", In Conferência Web.br, W3C Brasil, São Paulo.

Dinh, T. T. A.; Wang, J.; Chen, G.; Liu, R.; Ooi, B. C.; Tan, K. L. (2017), "Blockbench: A framework for analyzing private blockchains", In Proceedings of the 2017 ACM International Conference on Management of Data, ACM, pp. 1085-1100.

Donohue, B. (2014), "What is Two-Factor Authentication? Where Should You Use It?", available from: https://www.kaspersky.com/blog/what_is_two_factor_authentication/5036 (access 10 Nov. 2018).

Drescher, D. (2018), Blockchain Básico: uma introdução não técnica em 25 passos, Novatec Editora, São Paulo.

Fanning, K.; Centers, D. P. (2016), "Blockchain and its Coming Impact on Financial Services", Journal of Corporate Accounting & Finance, Vol. 27, No. 5, pp. 53-57, available from: https://onlinelibrary.wiley.com/doi/full/10.1002/jcaf.22179 (access 5 Nov. 2018).

Fares, M. (2015), "Fatores de Autenticação", available from: https://www.tiespecialistas.com.br/fatores-de-autenticacao (access 5 Nov. 2018).

Ferreira, F. N. F. (2003), Segurança da informação. Rio de Janeiro; Ciência Moderna.

Garay, J.; Kiayias, A.; Leonardos, N. (2015), "The Bitcoin Backbone Protocol: Analysis and applications", In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, Berlin, Heidelberg, pp. 281-310.

Garrote, C. G. D.; Pazos, J. D. (2018), "O que é Blockchain? Como podemos aplicá-la na propriedade intelectual?", available from: https://www.demarest.com.br/pt-br/publicacoes/o-que-%C3%A9-blockchain-como-podemos-aplic%C3%A1-la-na-propriedade-intelectual (access 3 Nov. 2018).

Geissbauer, R.; Vedso, J.; Schrauf, S. (2016), "Industry 4.0: Building the digital enterprise", available from: https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf (access 20 Apr. 2019).

Ghiorzoe, T. Z. (2014), "Cibercrime, proteção de dados e autenticação de múltiplos fatores (MFA)", available from: https://blogs.technet.microsoft.com/risco/2014/09/18/cibercrime-proteo-de-dados-e-autenticao-de-mltiplos-fatores-mfa (access 2 Nov. 2018).

Gomes, S. S. (2018), "Smart Contracts: legal frontiers and insertion into the Creative Economy", Brazilian Journal of

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

Operations & Production Management, Vol. 15, No. 3, pp. 376-385, available from: https://bjopm.emnuvens.com.br/bjopm/article/view/378 (access 11 Mar. 2018).

Hajdarevic, K.; Pattinson, C.; Kozaric, K.; Hadzic, A. (2012), "Information security measurement infrastructure for KPI visualization", In 2012 Proceedings of the 35th International Convention MIPRO, IEEE, pp. 1543-1548.

Horenberg, D. (2017), "Applications within Logistics 4.0: A research conducted on the visions of 3PL service providers", In 9th IBA Bachelor Thesis Conference, Enschede, The Netherlands, 5 de Jul. 2017.

Hydrogen Technology Corporation. (2018), "Introducing Hydro the FinTech Blockchain", available from: www.hydrogenplatform.com/hydro (access 1 Nov. 2018).

Jeny, A. (2018), "On accounting, digital economy and intangible assets' recognition", available from: http://knowledge.essec.edu/en/economy-finance/accounting-digital-economy-and-intangible-assets.html (access 15 Apr. 2019).

Kan, M. (2018), "Hackers beat 2-factor protection with automated phishing attacks", available from: https://mashable.com/article/hackers-beat-two-factor-authentication-2fa-phishing/#rftPYUAHSOqg (access 12 Mar. 2019).

Kshetri, N. (2017), "Blockchain's roles in strengthening cybersecurity and protecting privacy", Telecommunications policy, Vol. 41, No. 10, pp. 1027-1038, available from: https://www.sciencedirect.com/science/article/abs/pii/S0308596117302483 (access 14 Abr. 2019).

Lambauer, D. (2016), "A Multi Factor Authentication Quickstart", available from: https://dev98.de/2016/11/19/a-multi-factor-authentication-quickstart (access 12 Nov. 2018).

Lin, C.; He, D.; Huang, X.; Choo, K. K. R.; Vasilakos, A. V. (2018), "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0", Journal of Network and Computer Applications, vol. 116, pp. 42-52, available from: https://www.sciencedirect.com/science/article/pii/S1084804518301619 (access 20 Abr. 2019).

Lin, I. C.; Liao, T. C. (2017), "A Survey of Blockchain Security Issues and Challenges", IJ Network Security, Vol. 19, No. 5, pp. 653-659, available from: http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf (access 12 Nov. 2018).

Lucena, A. U.; Henriques, M. A. A. (2016), "Estudo de Arquiteturas dos Blockchains de Bitcoin e Ethereum", In IX DCA/FEEC/University of Campinas (UNICAMP) Workshop (EADCA), Campinas, SP, 29-30 de Set. 2016.

Mckeown, E. (2017), "What is Multi-Factor Authentication (MFA)?", available from: https://www.pingidentity.com/en/company/blog/posts/2017/what-is-multi-factor-authentication-mfa.html (access 11 Nov. 2018).

Merriam-Webster Dictionary (2019), "Webster's Dictionary", available from: https://www.merriam-webster.com/dictionary/empirical (access 02 Apr. 2019).

Mohamed, N.; Al-Jaroodi, J. (2019), "Applying Blockchain in Industry 4.0 Applications", In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0852-0858.

Pilkington, M. (2016), "Blockchain technology: principles and applications", Research Handbook on Digital Transformations, edited by f. Xavier Olleros and Majlinda Zhegu, available from: https://ssrn.com/abstract=2662660 (access 3 Nov. 2018).

Pourebrahimi, B.; Bertels, K.; Vassiliadis, S. (2005), "A survey of peer-to-peer networks", In Proceedings of the 16th Annual Workshop on Circuits, Systems and Signal Processing, ProRisc, Citeseer, available from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.1218 (access 15 Apr. 2019).

Rabah, K. (2017), "Overview of blockchain as the engine of the 4th industrial revolution", Mara Research Journal of Business & Management, Vol. 1, No. 1, pp. 125-135, available from: http://business.mrjournals.org/index.php/business/article/view/7 (access 20 Apr. 2019).

Rouse, M. (2015), "Multifactor authentication (MFA)", available from: https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA (access 9 Nov. 2018).

Sêmola, M. (2003), Gestão da segurança da informação: uma visão executiva, Campus, Rio de Janeiro.

Shyamasundar, R. K.; Patil, V. T. (2018), "Blockchain: The Revolution in Trust Management", In Proceedings of the Indian National Science Academy, Vol. 84, No. 2, pp. 385-407, available from: http://insajournal.in/insaojs/index.php/proceedings/article/view/551 (access 16 Abr. 2019).

Staples, M.; Chen, S.; Falamaki, S.; Ponomarev, A.; Rimba, P.; Tran, A. B.; Weber, I.; Xu, X.; Zhu, J., (2017), "Risks and opportunities for systems using blockchain and smart contracts", Data61 (CSIRO), Sydney, Australia, available from: https://www.data61.csiro.au/~/media/052789573E9342068C5735BF604E7824.ashx (access 16 Abr. 2019).

Swan, M. (2015), Blockchain: Blueprint for a New Economy, O'Reilly Media, Inc.

Tama, B. A.; Kweka, B. J.; Park, Y.; Rhee, K. H. (2017), "A critical review of blockchain and its current applications", In 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), IEEE, pp. 109-113, available from: https://ieeexplore.ieee.org/abstract/document/8167115 (access 16 Abr. 2019).

Tiwari, S.; Bhalla, A.; and Rawat, R. (2016), "Cyber Crime and Security", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 6, No. 4, available from: http://ijarcsse.com/Before_August_2017/

Brazilian Journal of Operations & Production Management
Volume 16, Número 2, 2019, pp. 281-293
DOI: 10.14488/BJOPM.2019.v16.n2.a9

docs/papers/Volume_6/4_April2016/V6I4-0201.pdf (access 9 Nov. 2018).

Vergara, S. C. (2009), Métodos de coleta de dados no campo, Atlas, São Paulo.

Vieira, G. Y. M.; Ruggiero, W. V. (2007), "Algoritmos para tokens de autenticação", In Proceedings, Conferência IADIS Ibero-Americana www/internet, Vila Real, Portugal, pp. 1-7.

Warkentin, M.; Willison, R. (2009), "Behavioral and policy issues in information systems security: the insider threat", In European Journal of Information Systems, Vol. 18, No. 2, pp. 101-105, available from: http://130.18.86.27/faculty/warkentin/BIS9613papers/EJIS_SpecialIssue/WarkentinWillison2009_EJIS18_2_ED_InsiderThreat.pdf (access 16 Abr. 2019).

Wiśniewska, M. (2018), "Password: SMS. How can a text message become an element of multi-factor authentication?", available from: https://www.smsapi.com/blog/password-sms-how-can-a-text-message-become-an-element-of--multi-factor-authentication (access 14 Nov. 2018).

Xu, X.; Weber, I.; Staples, M.; Zhu, L.; Bosch, J.; Bass, L.; Rimba, P. (2017), "A Taxonomy of Blockchain-based Systems for Architecture Design", In 2017 IEEE International Conference on Software Architecture (ICSA), Gothenburg, Sweden, pp. 243-252.

Zhou, K.; Liu, T.; Zhou, L. (2015), "Industry 4.0: Towards future industrial opportunities and challenges", In 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), IEEE, (pp. 2147-2152).

Zyskind G.; Nathan O.; Pentland A. (2015), "Decentralizing Privacy: Using Blockchain to Protect Personal Data", In Security and Privacy Workshops IEEE, pp. 180-184.

Received: 26 Feb 2019

Approved: 24 Apr 2019

DOI: 10.14488/BJOPM.2019.v16.n2.a9

How to cite: Cardoso, J. A. A.; Ishizu, F. T.; Lima, J. T. et al. (2019), "Blockchain Based MFA Solution: The Use of Hydro Raindrop MFA for Information Security on WordPress Websites", Brazilian Journal of Operations & Production Management, Vol. 16, No. 2, pp. 281-293, available from: https://bjopm.emnuvens.com.br/bjopm/article/view/791 (access year month day).