AUTHENTICATION AND VERIFICATION OF SOCIAL NETWORKING ACCOUNTS USING BLOCKCHAIN TECHNOLOGY

[1]Samer Shorman and [2]Mohammad Allaymoun

[1]Department of Computer Science, Applied Science University, Kingdom of Bahrain
[2]Administrative & Financial Sciences, AMA International University, Kingdom of Bahrain

ABSTRACT

Social networking pages authenticate by blockchain technology, through authenticating personal information and profile pages in the form of block and then distributing them with Blockchain to become a trusted reference point. To identified and verified social network accounts. This research proposed an effective and easy technical mechanism to authenticate the personal pages on social networks. Using this mechanism, anyone can authenticate any account on social networks, as well as increasing the possibility of making sure of the real individual behind social networking accounts. Moreover, this technique will show the fake accounts in order to reach a more confident and secure social network environment. Blockchain technique requires only a simple update to the characteristics of its platforms by developers, which is only a participatory mechanism between Blockchain and personal information. It is then combined with personal pages, to indicate that these pages contain the real personal information of the account holder, which is stored in an encrypted block that is difficult to modify, copy, or steal.

1. INTRODUCTION

Information technology has made tremendous progress in all areas of daily human life. Those aspects are represented in people's interactions, communication that is no longer limited to real communication through exchange of visits or making a phone call but developed to show a new concept of communication between people by technology. These are called social networking sites, which can interact with the other person at any time wherever via electronic platforms [1] [2].

Social networks are websites that provide services that enable people to express themselves and to meet other people who share the same interests [3].Social networks are virtual communities that enable users to share ideas and interests, as well as making new friends. Social networking sites have many advantages, making them different from other websites, and one of these features is the ability to create personal accounts so that the user can register access to the sites with them. The ability to create personal pages enables the user to publish personal information about themselves, such as biography, personal photos, or the latest activities, and ability to interact with other users by creating friendships, creating groups, and following other users [4, 5]. In addition, there are publications communicating the latest news and news regarding the other users of the site. As well as the possibility of publishing and modifying the contents, these may be written messages, photos, videos, etc. Users can interact with other users' posts by writing comments,

DOI: 10.5121/ijcsit.2019.11601

expressing different opinions, and showing admiration for publications [6].The challenges and threats facing users on social networks have increased. These threats include trust, the trust of users in dealing with others, the inability to ascertain the identity of people and the truth of accounts, and the absence of effective mechanisms capable of distinguishing fake or real pages [7].

The lack of confidence in dealing seriously with most users comes from the frequency of creating accounts usually for entertainment, but over time, there has been increased interest in verifying the identity of the real owners of accounts. The reason for the emergence of fake pages for users is usually to spread rumours and false news or the theft of followers [8]. It has become necessary to have a mechanism that is able to authenticate accounts on social networks. Some social networking sites have created mechanisms to limit the fake pages, or show a logo that distinguishes the real pages, enabling followers to identify the real pages of the personalities who wish to follow them. Facebook, Twitter and others have also used Blue Check, a blue sign on their personal pages. These mechanisms and procedures are specific only to specific categories (media, sports, government, etc.), which have greatly reduced the problems they were directing, reducing fake pages that spread news and rumours. In order to obtain this blue sign, a number of documentary paperwork must submitted to confirm the identity of the page owner.

Moreover, the existing method is effective only for specific categories, and its procedures are rather complex in order to verify and authenticate personal identity. Most users cannot authenticate their pages, for a number of reasons, including that the procedures for getting the blue check are somewhat complex and require time. The authentication depends on the number of followers, which prioritizes accounts with greater influence, as followed by the Twitter company. Hence, this study seeks to find a technical and free mechanism to authenticate the social networking pages, through the integration of Blockchain technology with social networks[9].
One way to improve these sites is to take advantage of Blockchain features and the tools it provides to document and verify personal information. It will help in reducing the complex procedures used in social networks, in order to authenticate accounts and confirm the real information of account holders. This verification is usually displayed as a logo shown on the personal pages as a blue check, the mark indicates that it’s a reliable page. The use of the new technique will enable users to approach social networks more confidently without concern. As a result, the code that refers to the block containing the real information will become a sign that enables followers to confirm that the personal page is real and reliable, to allow social networks to focus on the goals for which they were created, such as social communication. This research aims toward the goal that authentication pages be available to everyone without conditions or restrictions to obtain a sign of trust (code block) on social media pages. The research structure will be literature review, blockchain, proposed model, dissections and conclusion.

2. LITERATURE REVIEW

Social networks have many advantages; they have brought about a major change in the world of technology and the world at large, including the availability of social networks to communicate with people wherever they may be; the meeting of people with shared ideas.It also made possible the creation of job opportunities. Possibility of finding, identifying and communicating with people with common interests. Fast news dissemination. They provide opportunities for corporate owners to develop their enterprises by exploiting the ease and speed of finding people who share certain interests, and this facilitates the publication of advertisements [2].Social networks are a

fun source for some people, and this is done by tracking the latest news feeds. There are many pros for social networks, but there is the dark side, which affects users directly, such as privacy violations, which usually expose them to dangers such as impersonation, forgery, extortion, spreading rumours, etc [10].Recently, competition between social networks such as Facebook, Twitter, Instagram, YouTube and others has increased. Each site offers various services and communication methods, which seek to attract the largest number of Internet users. Statistics show that the most used social media sites are Facebook and Twitter in the Middle East [11]. For this purpose, each site seeks to provide entertaining and fun interactive tools in its platforms, such as video chat, with the possibility of adding shapes and animations to personal stories.

An important observation is that social networking sites do not have an authentication mechanism and automatically verify the identity of the applicants, because these sites are not able to impose restrictions and conditions in order to verify the identity of the account holder. Which may negatively affect the number of users, so the terms and policies make it easy to set up accounts and overlook the check and verify the identity of the service applicant, resulting in an increase in the number of fake pages. Fake pages are used to exploit important categories, by using personal photos or personal information, in order to spread lies and discredit. This is illegal and threatens privacy. So, dealing with social networking sites has become a dangerous and risky thing [12, 8]. Hence, each important category seeks to have its pages on social networks distinctive and authenticated in order to attract real followers, in addition to removing all fake pages that use the name or pictures in order to mislead the followers.

The authentication mechanisms on social media accounts differ from one site to another, but they are similar in terms of the objective, which is authenticating personal pages, in addition to showing a logo that distinguishes these pages from other pages. This mechanism requires everyone to follow specific procedures to complete authentication. Hence, obtaining a trust logo is not easy, accompanied by complicated procedures that are difficult to follow by normal users, unlike the important personalities who usually have managers who maintain their daily work and accounts.

The sign of trust on Facebook is called Blue Check. This tag indicates that the page has been verified by the identity of the account holder. Blue Check usually appears on the pages that need to be distinguished from the rest of the fake pages, which need to spread news and communicate with the followers without the risk of phishing by pages that exploit the same names, pictures, and information [13].The blue check requires several things, including an effective account, compatibility with Facebook policy, as well as public interest by followers in addition to matching the page or profile with the Facebook Terms of Service. It is available in the account (cover photo, profile photo, followers, personal information, website of the account holder, or social networking account), and then a service applicant fills out a form of application that includes all personal information. They then send a copy of a government-issued personal document (e.g. passport, driver's license or national identity card) to validate an application. Then they send some additional information such as URLs associated with the personal account, which helps to clarify the extent of public interest of the service applicant, in addition to writing a recommendation explaining why the need to get this logo. For example, one may write the risks that are exposed by fake pages using their name or images to spread rumours, what is the real benefit of the appearance of the blue check on their personal pages, which help followers and friends follow the real accounts, etc. At the end of the proceedings, a notice referring to the Facebook review is received within two to five days, and it is probable that the request is rejected because the company is not satisfied with the applicant's request or lack of one of the required

pieces information. It is also noted that these procedures are lengthy and limit the number of accounts that can benefit from this service. It also targets categories (journalists, Popular Brand or Businesses, government officials, Celebrities, Media, Entertainment, Sports Companies),and it is within the power of Facebook to remove the logo in case of violation ofthe company's law and policy. Block check has helped to create a sense of safety and confidence and reduce the fake pages [14].

As for Twitter in obtaining the blue check, it is almost similar to the procedures followed on Facebook but differ in several points. For example, the requirement to get the logo of trust on Twitter requires a certain number of followers, and the large number of followers indicates how important the account holder is [15].This means that the account is not necessary for VIP or trademark owners to get a logo, also if the account has a good online activity and having a follower of a few thousand users, this increases the chance of getting a logo. The procedures to begin to obtain a logo include connecting a phone number on the Twitter account, and in order to confirm the phone number, the user is required to re-enter the code, and confirm the applicant's identity, and usually the code sent to the user's email. Then you must confirm the email on your Twitter account. When you add the email address to the user account on Twitter, Twitter sends a confirmation link to this mail, and the user has to access his email page and click on the link to complete his email confirmation. In addition to sending the curriculum vitae to the service applicant, it contains an account picture, cover photo, date of birth, and URL. It also requires that the account be on the status of public and not private. After these procedures, the notice of acceptance of the application takes two to five days to appear, but not all applications are accepted and may be rejected based on their terms and the conditions and policies followed by Twitter [16][17].

In fact, most social networking sites follow the same procedures, which include difficult and traditional steps to authenticate social networking pages using paper documents;the number of accounts and target categories that are able to obtain this logo are few and limited.Therefore, the social media sites are forgetting the main purpose for which they were created, such as communicating, entertaining and establishing relationships, in order to focus on the role of security and authentication purely.

Therefore, this research creates an effective technical alternative capable of authenticating the social networking pages, in order to obtain a trust logo or code that facilitates the identification of reliable pages and allow everyone to authenticate their accounts. By linking the block chain technique, it consists of blocks containing personal information that are authenticated and encrypted and arenot editable, distributed to all users. This lends a kind of double trust between the Block chain and social networks. The social network is relieved from the role of security and authentication, which is done by a third party in documenting the accounts in a technical manner.

3. BLOCKCHAIN

Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency Bitcoin[18]. The identity of Satoshi Nakamoto is unknown. The invention of the blockchain for Bitcoin made it the first digital currency to solve the double-spending problem without the need of a trusted authority or central server. The Bitcoin design has inspired other applications, and blockchain, which are readable, by the public are widely used by cryptocurrencies [19].

Blockchain is considered a type of payment rail.[20] Private blockchains have been proposed for business use. Sources such as Computer World called the marketing of such blockchains without a proper security model "snake oil." [21]

A blockchain is a growing list of records, called blocks, which are linked using cryptography to store data. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree) [22].

A blockchain is resistant to modification of the data. It is an open, distributed ledger, which can record transactions between two parties efficiently and in a verifiable and permanent way [23].It used a distributed ledger; a peer-to-peer network typically manages a blockchain. Which is collectively adhering to a protocol for inter-node communication and validating new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain [19].

Block chain contains three basic elements. The first is a distributed ledger (as in multiple versions), but it is centralized (as in one copy only), a way to record and store a personal account link on social media networks. This ledger is general, which means that anyone can read it, and is immutable, which means that no one can change what happened in the past.

The second element is the consensus algorithm, a way to make sure that all the ledger copies are the same for everyone. This is usually called mining. A crucial part of the system is that anyone can participate. They are distributed, which means that no particular node in the compatibility network should be trusted. Unless it is approved by all, and that any process must be taken by unanimous consent, which means that all operations are monitored; no modification or procedure is permitted without consensus.

The third element, encryption and distribution block, which contains the data stored, and the result is a Hash code, which indicates the location of the block and its contents, and then links the block with the rest of the chain [22, 24].

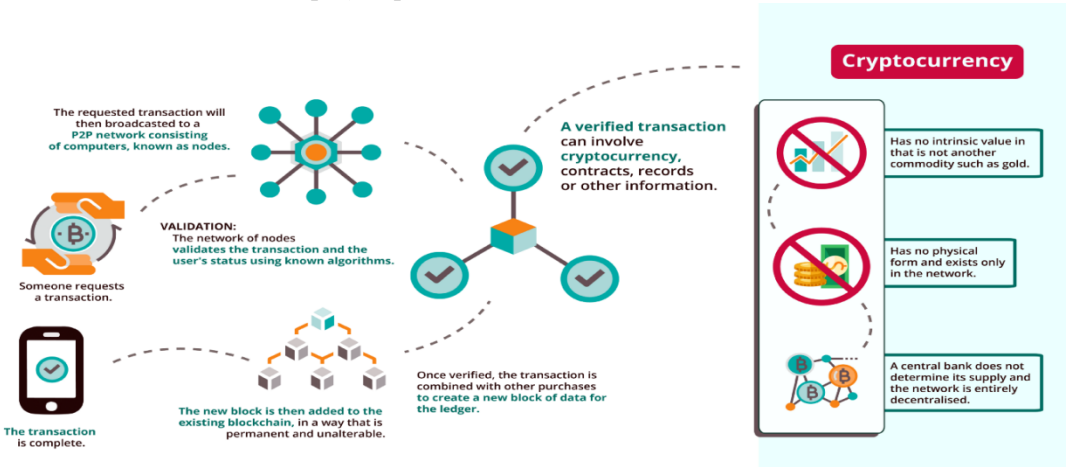

Figure 1: Blockchain mechanism [25].

Let's have a closer look at what is a block in a blockchain. Each blockchain block consists ofcertain data: the hash of the block and the hash from the previous block.The data stored inside each block depends on the type of blockchain. For instance, in the Bitcoin blockchain structure, the block maintains data about the receiver, sender, and the amount of coins. A hash is like a fingerprint (long record consisting of some digits and letters). Each block hash is generated with the help of a cryptographic hash algorithm (SHA 256). Consequently, this helps to identify each block in a blockchain structure easily. The moment a block is created, it automatically attaches a hash, while any changes made in a block affect the change of a hash too. Simply stated, hashes help to detect any changes in blocks.The final element within the block is the hash from a previous block. This creates a chain of blocks and is the main element behind blockchain architecture's security. As an example, block 45 points to block 46. The very first block in a chain is a bit special - all confirmed and validated blocks derived from the genesis block.

4. PROPOSED MODEL

In this section, the proposed model of the social media authentication mechanism is reviewed using block chain technology, as well as the benefit of block chain storing personal information in block form and distributing it to all ledgers. These blocks can be used as a reference point for information that is documented, stored and encrypted. This procedure can take advantage of a storage and distribution mechanism to be linked to social media pages to provide a technical documentation mechanism for social media account information, which does not need to follow the difficult procedures provided by Social networking sites to get a trust logo. Figure 2 shows the structure of the proposed model and as noted in the figure 2, it is necessary to have information stored in the form of a block for the service applicant to be distributed. All users of block chain, on the other hand, approved it having an effective account on the social network, and then the account is linked with the service applicant block to be a trusted reference stored in block. In other words, the information is authenticated in a participatory manner from both sides of the block and social page.

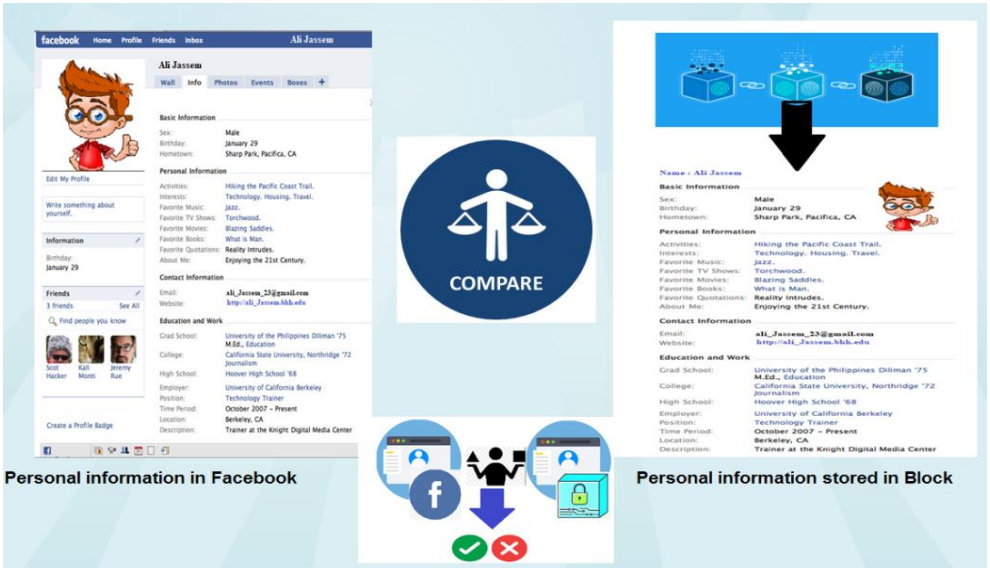

Figure 2: Personal information (Facebook,Block).

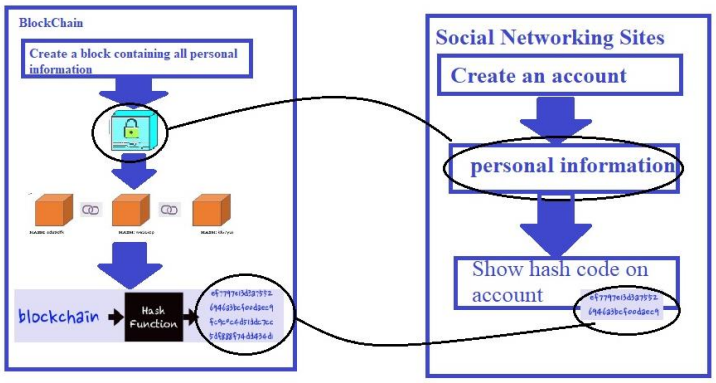

Figure 3: sequence of operations

Figure 3 illustrates the sequence of operations, and it shows the steps required to complete the authentication from both sides of block chain and social networking pages. The following steps are required for account authentication: Create an account on the social network, complete the registration of all personal information, create a block in block chain which contains all the personal information of the service applicant (personal photos, documents, links. etc). The fourth step is to add the personal account link in the block, distribute the block chain on ledgers and receive the block receipt notice, get a hash code in the block that contains all the personal information, which is the reference number, through which it becomes the address where the personal information is matched with the account. The seventh step is to add the hash code to the personal page on the social networking page and the appearances of block chain logo and the hyperlink to the block containing the documented information.

At the end, the page containing the block chain logo and the hyperlink becomes reliable based on the information stored in the block distributed to everyone. Hence, the aim is to give confidence to the social media pages based on information previously stored in the block and distributed on the ledger. This authentication is difficult to falsify, modify or violate because any process carried out on block notifies everyone in the books to get approval for any action.

One account and one block only, in other words, and this research deals with the possibility of linking one account with one block. In the future we may add additional options or the possibility of linking more than one account in a block.

5. DISCUSSION

This section reviews some scenarios for the authentication process of social networking pages by block chain. Figure 4 illustrates the sequence of the authentication process by block chain, starting from the creation of a block containing all personal information and ending with the Hash code and the logo appearing on a personal account. The steps are easy, and the mechanism only needs to create a block and link it with the personal account. Then get the trust logo immediately without having to wait, and there is no chance to reject the application for the trust logo, unless there is an attempt to modify the personal information in the block or use hash code for more than one account.

If the hash code is used in more than one account, the rest of the followers in the block chain refuse the operation, and they report a violation, so that the followers themselves are able to detect the manipulation and knowledge of the fake pages.

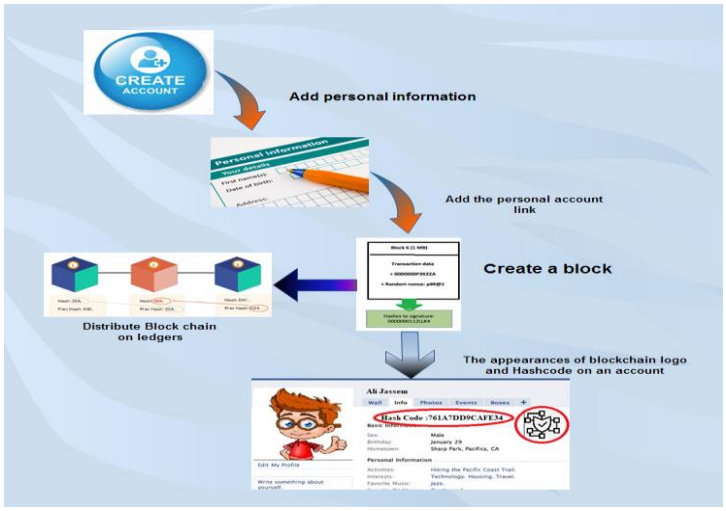

Figure 4: The sequence of the authentication process by block chain

Table 1 shows the difference between authentication mechanisms between social networking pages such as Twitter, Facebook, and block chain. As is clear, the proposed mechanism is considered a new and effective idea to reduce fake pages, as well as to give confidence to personal accounts.

Table 1: Different authentication mechanisms in social networking

Comparison	Facebook	Twitter	Block chain trust
Logo			
Procedures	Difficult	Difficult	Easy
Authentication mechanism	Manual by attaching personal documents and a URL account	Manual by attaching personal documents and a URL account	Personal information stored in block
Target category	Journalists,Popular Brand or Businesses,Government Officials, Celebrities,Media,Entertainment,Sports Companies	Journalists,Popular Brand or Businesses,Government Officials, Celebrities,Media,Entertainment,Sports Companies	Everyone
Duration of obtaining a logo	From 2 days to 5 days	Days	Immediate
Report abuse	Facebook Company	Twitter Company	ledger distributed on a chain
Terms to get a logo	Paper document and URL account, compelling reasons to get a logo	Paper document and URL account, compelling reasons to get a logo	Personal information stored in Block chain
Limit fake pages	Effective	Effective	Effective

The number of pages documented using the blockchain is expected to increase because of its ease as well as being a successful alternative to authenticate, and confirm the identity of account holders and reduce the fake pages. Anyone can easily check through the hash code on a personal page and then match it with the personal information in the block. On the other hand, the effectiveness of the proposed mechanism does not require papers, i.e. the traditional way through official government documents in order to ascertain the identity of a service applicant.The role of social networking is expected to be limited to social networking, a focus on the social objectives for which it was created and give a third-party opportunity to document personal pages.

Figure 5 show personal pages after receiving the logo and hash code, which allows followers to infer the pages of their favorite characters, in addition to the possibility of verification through the hash code, and the possibility of comparing personal information on the profile page and the block.

Figure 5:Personal page after the appearance of the logo and hash code.

6. CONCLUSION

This research provides a model of an effective technical mechanism capable of electronic authentication using the block chain, in order to be a substitute for the authentication mechanisms used in social networks and to create a secure environment that all users can handle safely and confidently. The proposed model uses the trust algorithm of the blockchain. This model relies on creating trust by distributing the stored block of personal information to all ledgers. This block is encrypted and does not accept modification or deletion, hence the block becomes a reference to verify personal information stored in the block which is then linked to the personal information in the social media account. The result is a hash code that appears on the profile page, through which any follower can compare the information stored in the block with the information shown on the account. If there is a match, the account is authenticated, and the reverse is false. This research contributes significantly to authenticating social media pages, finding technical alternatives to reduce the risks faced by social media users, as well as highlighting the possibility of adding third parties to reduce the number of fake pages, and create a safe environment.

Future work will include detailed verification of the technical aspect; in addition, a real scenario test will performed. Once applied to social networking pages, analysis of the results will be performed to resolve any problems that may face the application of the block chain technology in the authentication process.

REFERENCE

[1] Coyle, C., & Vaughn, H. (2008). Social networking: Communication revolution or evolution? Bell Labs.

[2] Boyd, D.M. & Ellison, N.B. (2008), Social Network Sites:Definition, History and Scholarship. Journal of ComputerMediated Communication, 13(1), p. 201-230.

[3] F. Benevenut, T. Rodrigues, M. Cha, and V. Almeida. Characterizing user behavior in online social networks. In Proc. of ACM SIGCOMM Internet Measurement Conference. ACM, 2009.

[4] Brandtzæg Bae Petter and Heim Jan (2009) Why People Use Social Networking Sites. Proceedings of the 3d International Conference on Online Communities and Social Computing: Held as Part of HCI International: 143-152

[5] Ellison, N. B., Steinfield, C., & Lampe, C. "The benefits of Facebook 'friends:' Social capital and college students' use of online social network sites". Journal of Computer-Mediated Communication, 12, (4),1143-1168, 2007.

[6] Marcelo Maia, Jussara Almeida, Virgílio Almeida, "Identifying User Behavior in Online Social Networks", Proceedings of the first Workshop on Social Network Systems, 1 April 2008

[7] Michael Fire,etc,(2014)"Online Social Networks: Threats and Solutions",IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014.

[8] Mohammad H. Allymoun, Nidal F. Shilbayeh, Sameh T. Khuffash, Reem Al-Saidi (2014). Protecting the Privacy and Trust of VIP Users on Social Network Sites, International Journal of Computer, Information, Systems and Control Engineering, Vol. 8 No.9, 1419-1429.

[9] Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing,and privacy on the Facebook. In P. Golle& G. Danezis (Eds.), Proceedings of 6th Workshop on Privacy Enhancing Technologies (pp. 36-58). Cambridge, UK: Robinson College.

[10] Devmane, M., & Rana, N. (2013). Security Issues of Online Social Networks. Advances in Computing, Communication, and Control, Springer. pp. 740-746.

[11] Dustin W. Stout,.(2019). "Social Media Statistics 2019: Top Networks by the Numbers". (On-Line), available:https://dustinstout.com/social-media-statistics/.

[12] Conti, M., Poovendran, R., &Secchiero, M. (2012). FakeBook: Detecting Fake Profiles in On-Line Social Networks. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM). pp. 1071-1078

[13] Facebook, accessed OCT. 14, 2019. [Online]. Available: http://www.facebook.com/

[14] ALEJANDRO RIOJA,.(2019)"Get Verified on Facebook: Page or Profile (Blue + Gray Verification Badge)", JUNE 24, 2019. (On-Line), available:https://alejandrorioja.com/blog/get-facebook-verified/.

[15] HaewoonKwak, Changhyun Lee, Hosung Park, and Sue Moon, 2010,What is Twitter, a social network or a news media?.Proceeding WWW '10 Proceedings of the 19th international conference on World wideweb.Pages 591-600.

[16] Mohammadi E, Thelwall M, KwasnyM,Holmes KL (2018) Academic information on Twitter: A user survey. PLoSONE 13(5):e0197265. https://doi.org/10.1371/journal.pone.0197265

[17] Twitter,.(2019)." About verified accounts", (On-Line), available: https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[19] Dylan Yaga,PeterMell,NikRoby,KarenScarfone,(2018).Blockchain Technology Overview.NISTIR 8202.https://doi.org/10.6028/NIST.IR.8202.

[20] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[21] C. Natoli and V. Gramoli, "The blockchain anomaly," in 15th International Symposium on Network Computing and Applications (NCA), 310-317, IEEE, 2016.

[22] Q. K. Nguyen, "Blockchain-A Financial Technology for Future Sustainable Development," in Green Technology and Sustainable Development (GTSD), 2016, pp. 51–54.

[23] Samer Shorman, Mohammad H Allaymoun and Omer Hag Hamid. (2019). DEVELOPING THE E-COMMERCE MODEL A CONSUMER TO CONSUMER USING BLOCKCHAIN NETWORK TECHNIQUE, International Journal of Managing Information Technology (IJMIT) Vol.11, No.2, May 2019, DOI : 10.5121/ijmit.2019.11204 .

[24] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), pp. 182-191, IEEE, 2016.International Journal of Managing Information Technology (IJMIT) Vol.11, No.2, May 2019.

[25] ImarticusLearning."Infographics: What is Blockchain?".(On-Line), available: https://medium.com/@imarticus/infographics-what-is-blockchain-6a1f93e64e79.