Iberian Journals

Iberian Journal of Applied Sciences and Innovation

2021 vol 1, Issue3

An in-depth analysis of the major cryptocurrency security attacks

Mohammad Sadeghi

Sahand University of Technology

Mo_sadeghi@outlook.com

***Abstract*— increasing public interest in cryptocurrencies, as well as the accountability, transparency and stability of cryptocurrencies, has prompted research into the promise of blockchain technology. However, there is a major concern in dealing with the accountability deficit for all cryptocurrencies, two of which are currency theft and shutdown. This article analyzes cryptocurrency attacks, currency shutdowns, and theft that have been reported in various cases.**

***Keywords*— cryptocurrency, cryptocurrency attack, theft, shutdown, blockchain, DDoS**

I. INTRODUCTION

Cryptocurrency network becomes stronger in terms of security when more miners join the network. The complexity of system hacking increases with network hashing [1]. The miners are determined to get their maximum reward. New miners prefer to join pools with higher hash rates, hoping to increase their chances of solving a block. Mining workers seek to maximize their rewards by pursuing strategies such as self-extraction and jump pool based on their needs and the pool reward system. Miners seek to maximize their rewards by following strategies such as selfish mining and pool hopping based on their needs and pool reward system. The Bitcoin system is also prone to potential capture by the miner who makes up the largest share of the network [2,3].Currency exchanges often face security breaches for stealing coins, resulting in weaker currencies as bitcoin transactions are not revocable, hackers regularly steal bitcoins from individuals and companies and leave victims without any referral. Those services that suffered from DDoS attacks, are most likely to take measures to prevent it [4,5].

II. SELFISH MINING

This section describes 25%-Attack on the cryptocurrency network - or the selfish mining. According
to Ittay Eyal And Emin Gun Sirer [6], if the hash power is 0-25%, the selfish extraction will earn a higher profit than the fair share, unless the cryptocurrency block release protocol is patched. Between 25 and 33%, even if it is patched, will earn a higher return on

equity. Between 33% and 50%, no repair is possible and a selfish mining does not need to be well connected to the network to win.

This selfish mining is prohibited by a coalition that controls less than a quarter of the resources. This threshold is below the wrong level of 1/2, but it is better than the current reality that a coalition of any size can endanger the system [7].

Selfish mining force honest miners to waste their computational time in the branch to be orphaned. Selfish mining pools work secretly on their reputable private branch, while honest miners spend their resources adding blocks to shorter blockchain branches. Because selfish miners do not make up the majority of the computing power in the network, the private chain maintained by them will not be longer than the public chain. Once they form the majority, they will no longer need to follow this strategy because other miners can not go faster than their pool. Selfish miners are waiting for most networks to be formed to control the blockchain [8,9]. In order to eliminate selfish extraction, 2/3 of the network must work honestly [10].

There are two self-extracting network signatures that can be used to determine when to do selfish-mining, but they are not easy to measure definitively. The first and strongest sign is the existence of abandoned chains (orphans), where the block race, which takes place as part of a selfish extraction, passes blocks that are not included in the block chain [11]. Unfortunately, abandoned blocks cannot be counted, because the current protocol prunes such blocks and throws them away from the inside. A measuring instrument that connects to the network from a small number of points may lose abandoned blocks. The second indicator of selfish extraction activity is the time interval between successive blocks. A selfish miner who has an honest chain length *N* with a length chain *N+1* crush, shows a block very soon after its previous sample. Because natural extraction events must be independent, block discovery time is expected to be distributed exponentially [12,13,14]. Deviation from this distribution indicates mining activity. The problem with this approach is that it only detects a subset of selfish miner behavior (transition from mode 2 to mode 0 in the state apparatus), signature behavior occurs relatively infrequently, and such statistical information may take a long time to obtain significant statistical data [15].

Although miners may collude in a selfish act of extracting the equation, they may prefer to conceal it to avoid public criticism and retaliation. Hiding behaviors of selfish-mining, it is difficult to prevent it. A selfish pool may never use different addresses, IP, forge the time of creating the block, and showing its size. The rest of the network do not even suspect that the pool near the threshold is dangerous [16].

In addition, if an identification mechanism is set up, a selfish group knows its parameters and uses them to prevent identification. For example, if a protocol for rejecting blocks is defined with a creation time below a certain threshold, the collection can release its hidden blocks just before that threshold [17].

The potential line of defense against selfish mining pools is to infiltrate counter-attacks in selfish pools and reveal their hidden blocks to miners. However, selfish pool managers can, in turn, selectively reveal blocks to subsets of pool members, identify spy nodes through intersections, and fire nodes that have leak information [18].

III. 51 PERCENT-ATTACK

It was commonly believed that the cryptocurrency system is safe as long as the majority of participants honestly followed the protocol, and the "51% attack" is the most important concern [19]. The most important security issue of the blockchain-based system is the so-called 51% attack. Bitcoin measures the level of computing activity on the network in terms of hash [20]. It is based on the fact that commanding 51% of the processing power on the network is very difficult and expensive for an attacker. Blockchain can be maliciously distorted when more than 51% of the hash is controlled by a node (a miner or miner pool) [21]. Unknown extraction pool GHash, which apparently belongs to CEX Russia, had 55% of the total network extraction energy for a period of 24 hours. However, no 51% attacks occurred in this pool [22,23]. A mining pool in China, Ghash.io, slightly crossed the 51% threshold in 2014 [24].

When a pool covers 51% or more of the network, it can easily cause waste by building its chain faster than the network and spreading it whenever it wants [25]. It can reject any block selected by any competing miner, reject any selected transaction, block specific transactions, and charge high fees from a specific address for the transaction to be entered in the blockchain. The most important disadvantage is the complete denial of services in the sense that pool can ignore every single block found by competitors and orphan them, thus stopping all transactions. So it is not entirely true that cryptocurrency does not require any trust because all participants must trust the goodwill of miners who have amassed more than 51% of their computing power [26,27]. If such an attack is successful, confidence in the currency is likely to be lost and its value as a currency will decline rapidly [28].

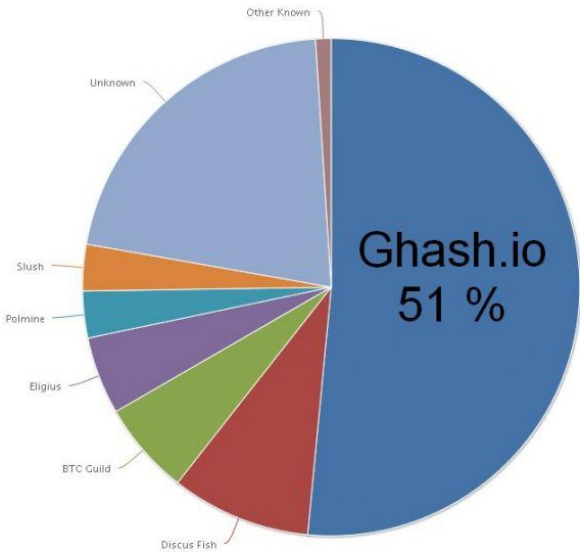

Figure 1: Distribution of 51%-attack

In a blockchain with a fixed fork due to reduction, the effective hash power of an attacker increases because he always extracts to expand his blocks while other extractors are not integrated. This allows a 51% attack with less than 51% hash power [29].

IV. DOUBLE SPENDING ATTACK

Nowadays, cryptocurrency is increasingly used in fast payment scenarios, where the exchange time between currency and commodity is short. It takes tens of minutes to confirm the transaction and is therefore unsuitable for fast payment. Although the average trading time is approximately 10 minutes, the standard deviation is approximately 15 minutes [30].
Cryptocurrency developers implicitly acknowledge this problem, informing users that they do not need to wait for payment confirmation until payment is high. However, this does not solve the problem, and only limits the damage because the system is still vulnerable to attacks at twice the cost. So far, attacks on double payouts in bitcoin or similar mechanisms to prevent them have not been studied [31,32].

V. DENIAL OF SERVICE ATTACKS

There are several reasons why we believe DDoS attacks worth studying on its own. First, there are unique incentives in the game that attack DDoS rewards, like merchants who profit by preventing others from trading. Second, the illegal environment of cryptocurrency with DDoS; An attractive tool for reckless operators has facilitated crime for profit. There are 142 unique attacks DDoS that 40 of them have been registered for bitcoin services. At this time, 7% of all known operators such as exchange offices, mining pools, gambling operators, eWallets, and more financial services have been attacked [33]. We find that exchanges and mining pools are more likely to DDoS like the Cloudflare, Incapsula, or Amazon Cloud Protect. Those services that are attacked are more than three times more likely than operators that are not attacked to buy anti-service services. Large mining pools (those with at least 5% historical stock of insects) are much larger than small pools DDoSed are. However, the most common scourge to harass cryptocurrency participants has been denial of service attacks [34]. Because cryptocurrency transactions are not revocable, hackers regularly steal bitcoins from individuals and companies, and leave victims without any referral. Those services that suffered DDoS attack, most likely now take steps to prevent DDoS. Identifying the time of denial of service can be difficult [35-39]. Most of reported DDoS attacks are related to mining

pools. There were very few reported attacks initially targeting pools, however, DDoS on gambling websites, and eWallets joined them [40-44]. The most targeted service group is currency exchanges (41%) followed by mining pools (38%). These are followed by gambling (9%), finance (5%), and eWallets (4٪)[45-48].

The size of the extraction pool depends on its Chance of DDoS attack. If it is observed that it has at least 5% of the share, we consider the pool to be large. All other pools are considered small. Table 1 Shows how DDoS attacks occur - it varies depending on the size of the pool. 5 Cases of 8 large pools (63%) suffered DDoS attacks, and out of 41 small pools only 7 (17٪). Attackers make more money by targeting large pools, as removing one of them significantly increases the chances of winning the round [49-51].

Table 1. Statistics of DDoS attacks to mining pools

	Small pools		Large pools	
	Quantity	Percent	Quantity	Percent
With DDoS	7	17.1٪	5	62.5٪
Without DDoS	34	82.9٪	3	37.5٪

VI. DISCUSSION

Blockchain attacks can be viewed from two perspectives. First, stock exchange attacks to steal their property, and second, mining attacks to reward more miners. The most important attacks include 51% attack, double spending, and selfish mining. Miners seek to maximize their rewards by following strategies such as selfish mining and pool hopping based on their needs and pool reward system. Presenting a mining strategy that enables pools of colluding miners lead to earn more income from their mining capacity. More income can lead new miners to join a selfish mining pool, a dangerous dynamic that enables the selfish mining pool to grow into the majority.

VII. CONCLUSION

Blockchain with distributed consensus, established trust, immutability, distributed identity, and perpetually verifiable claims may appear to be the ultimate technology without security flaws. But new age security attacks are emerging, which are very high complexity and can cause enormous irreparable damage. Understanding these attack vectors is crucial for anyone developing and implementing blockchain solutions. Cryptocurrency and crime describe attempts to obtain digital currencies illegally, such as through phishing, fraud, supply chain attacks, hacking, or measures to prevent unauthorized transactions and storage technologies.

REFERENCES

[1] Karamizadeh, S., Abdullah, S. M., Manaf, A. A., Zamani, M., & Hooman, A. (2013). An overview of principal component analysis. Journal of Signal and Information Processing, 4(3B), 173.

[2] Karamizadeh, S., Abdullah, S. M., Halimi, M., Shayan, J., & javad Rajabi, M. (2014, September). Advantage and drawback of support vector machine functionality. In 2014 International conference on computer, communications, and control technology (I4CT) (pp. 63- 65). IEEE.

[3] Zeidanloo HR, Manaf AB, Ahmad RB, Zamani M, Chaeikar SS. A proposed framework for P2P Botnet detection. International Journal of Engineering and Technology. 2010 Apr 1;2(2):161.

[4] Chaeikar SS, Zamani M, Chukwuekezie CS, Alizadeh M. Electronic Voting Systems for European Union Countries. Journal of Next Generation Information Technology. 2013 Jul 1;4(5):16.

[5] Mazdak Z, Azizah BA, Shahidan MA, Saman SC. Mazdak technique for PSNR estimation in audio steganography. InApplied Mechanics and Materials 2012 (Vol. 229, pp. 2798-2803). Trans Tech Publications Ltd.

[6] Azarnik, A., & Shayan, J. (2012). Associated risks of cloud computing for SMEs. Open

International Journal of Informatics (OIJI), 1(1), 37-45.

[7] Chaeikar SS, Abd Razak S, Honarbakhsh S, Zeidanloo HR, Zamani M, Jaryani F. Interpretative key management (IKM), A novel framework. In2010 Second International Conference on Computer Research and Development 2010 May 7 (pp. 265-269). IEEE.

[8] Chaeikar SS, Ahmadi A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. Signal Processing: Image Communication. 2019 Feb 1;70:233-45.

[9] Alizadeh, M., Salleh, M., Zamani, M., Shayan, J., & Karamizadeh, S. (2012). Security and performance evaluation of lightweight cryptographic algorithms in RFID. Kos Island, Greece

[10] Shayan, J., Azarnik, A., Chuprat, S., Karamizadeh, S., & Alizadeh, M. (2014). Identifying Benefits and risks associated with utilizing cloud computing. arXiv preprint arXiv:1401.5155

[11] Hooman, A., Marthandan, G., Yusoff, W. F. W., Omid, M., & Karamizadeh, S. (2016). Statistical and data mining methods in credit scoring. The Journal of Developing Areas, 50(5), 371-381.

[12] Alizadeh M, Hassan WH, Zamani M, Khodadadi T, Shojae Chaeikar S. A prospective study of mobile cloud computing. International Journal of Advancements in Computing Technology. 2013;5(11):198-210.

[13] Chaeikar SS, Manaf AB, Zamani M. Comparative analysis of Master-key and Interpretative Key Management (IKM) frameworks. Cryptography and security in computing. 2012 Mar 7:203.

[14] Dehzangi, A., & Karamizadeh, S. (2011). Solving protein fold prediction problem using fusion of heterogeneous classifiers. INFORMATION, An International Interdisciplinary Journal, 14(11), 3611-3622

[15] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[16] Shojae Chaeikar S, Zamani M, Chukwuekezie CS, Alizadeh M. Electronic Voting Systems for European Union Countries. Journal of Next Generation Information Technology. 2013 Jul 1;4(5):16.

[17] Chaeikar SS, Manaf AA, Alarood AA, Zamani M. PFW: Polygonal Fuzzy Weighted—An SVM Kernel for the Classification of Overlapping Data Groups. Electronics. 2020 Apr;9(4):615.

[18] Yazdanpanah S, Chaeikar SS. IKM-based Security Usability Enhancement Model. IRACST-International Journal of Computer Science and Information Technology & Security (IJCSITS). 2012 Aug(4).

[19] Karamizadeh, S., Abdullah, S. M., Zamani, M., & Kherikhah, A. (2015). Pattern recognition techniques: studies on appropriate classifications. In Advanced Computer and Communication Engineering Technology (pp. 791-799). Springer, Cham

[20] Alizadeh, M., Hassan, W. H., Behboodian, N., & Karamizadeh, S. (2013). A brief review of mobile cloud computing opportunities. Research Notes in Information Science, 12, 155-160.

[21] Honarbakhsh S, Masrom M, Zamani M, Chaeikar SS, Honarbakhsh R. A Trust Based Clustering Model for Dynamic Monitoring in Ad hoc Network. InInternational Conference on Computer and Computational Intelligence (ICCCI 2010) 2010 Dec 25.

[22] Zamani M, Manaf AA, Ahmad R, Jaryani F, Taherdoost H, Chaeikar SS, Zeidanloo HR. Genetic audio steganography. International Journal on Recent Trends in Engineering & Technology [IJRTET]. 2010;3(2):89-91.

[23] Karamizadeh, S., Abdullah, S. M., & Zamani, M. (2013). An overview of holistic face recognition. IJRCCT, 2(9), 738-741.

[24] Karamizadeh, F. (2015). Face Recognition by Implying Illumination Techniques–A Review Paper. Journal of Science and Engineering, 6(01), 001-007.

[25] Yazdanpanah S, Shojae Chaeikar S. Secure SMS Method Based on Social Networks. International Journal of Scientific Research in Science, Engineering and Technology. 2016: 2(6): 368-376.

[26] Karamizadeh, S., & Arabsorkhi, A. (2018, January). Methods of pornography detection. In Proceedings of the 10th International Conference on Computer Modeling and Simulation (pp. 33-38).

[27] Chaeikar SS, Ahmadi A. SW: A blind LSBR image steganalysis technique. InProceedings of the 10th International Conference on Computer Modeling and Simulation 2018 Jan 8 (pp. 14-18).

[28] Karamizadeh, S., Abdullah, S. M., Zamani, M., Shayan, J., & Nooralishahi, P. (2017). Face recognition via taxonomy of illumination normalization. In Multimedia Forensics and Security (pp. 139-160). Springer, Cham

[29] Yazdanpanah S, Shojae Chaeikar S, Zamani M, Kourdi R. Security features comparison of master key and IKM cryptographic key management for researchers and developers. In International Conference on Software Technology and Engineering, 3rd(ICSTE 2011) 2011. ASME Press.

[30] Shojae Chaeikar S, Jafari M, Taherdoost H, Kar NS. Definitions and criteria of CIA security triangle in electronic voting system. International Journal of Advanced Computer Science and Information Technology. 2012 Oct;1(1):14-24.

[31] Chaeikar SS. Pixel Similarity Weight for Statistical Image Steganalysis (Doctoral dissertation, Universiti Teknologi Malaysia).

[32] Karamizadeha, S., Mabdullahb, S., Randjbaranc, E., & Rajabid, M. J. (2015). A review on techniques of illumination in face recognition. Technology, 3(02), 79-83.

[33] Karamizadeh, S., Cheraghi, S. M., & MazdakZamani, M. (2015). Filtering based illumination normalization techniques for face recognition. Indonesian Journal of Electrical Engineering and Computer Science, 13(2), 314-320.

[34] Taherdoost H, Sahibuddin S, Namayandeh M, Jalaliyoon N, Kalantari A, Chaeikar SS. Smart card adoption model: Social and ethical perspectives. Science. 2012 Aug;3(4).

[35] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[36] Chaeikar SS, Yazdanpanah S, Chaeikar NS. Secure SMS transmission based on social network messages. International Journal of Internet Technology and Secured Transactions. 2021;11(2):176-92.

[37] Shayan, J., Abdullah, S. M., & Karamizadeh, S. (2015, August). An overview of objectionable image detection. In 2015 International Symposium on Technology Management and Emerging Technologies (ISTMET) (pp. 396-400). IEEE.

[38] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011, May). Packet loss differentiation of TCP over mobile ad hoc network using queue usage estimation. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 81-85). IEEE.

[39] Chaeikar SS, Zamani M, Manaf AB, Zeki AM. PSW statistical LSB image steganalysis. Multimedia Tools and Applications. 2018 Jan;77(1):805-35.

[40] Karamizadeh, S., Shayan, J., Alizadeh, M., & Kheirkhah, A. (2013). Information Security Awareness Behavior: A Conceptual Model for Cloud. International Journal Of Computers & Technology, 10(1), 1186- 1191.

[41] Chaeikar SS, Moghaddam HS, Zeidanloo HR. Node Based Interpretative Key Management Framework. InSecurity and Management 2010 (pp. 204-210).

[42] Karamizadeh, S., Abdullah, S. M., Shayan, J., Nooralishahi, P., & Bagherian, B. (2017). Threshold Based Skin Color Classification. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(2-3), 131-134

[43] Fard, M. A. K., Bakar, K. A., Karamizadeh, S., & Foladizadeh, R. H. (2011, May). Improve TCP performance over mobile ad hoc network by retransmission timeout adjustment. In 2011 IEEE 3rd International Conference on Communication Software and Networks (pp. 437-441). IEEE

[44] Karamizadeh, S., Abdullah, S. M., Shayan, J., Zamani, M., & Nooralishahi, P. (2017). Taxonomy of Filtering Based Illumination Normalization for Face Recognition. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(1-5), 135-139.

[45] Azarnik, A., SHAYAN, J., ZADEH, S. K., & PASHANG, A. (2013, February). Lightweight authentication for user access to Wireless Sensor networks. In Proceedings of the 12th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications (EHAC'13), Cambridge, UK (pp. 35-39).

[46] Duan, W., Nasiri, R., & Karamizadeh, S. (2019, December). Smart City Concepts and Dimensions. In Proceedings of the 2019 7th International Conference on Information Technology: IoT and Smart City (pp. 488-492).

[47] Karamizadeh, S., & Arabsorkhi, A. (2017). Enhancement of Illumination scheme for Adult Image Recognition. International Journal of Information and Communication Technology Research, 9(4), 50-56

[48] Dehzangi, A., Foladizadeh, R. H., Aflaki, M., & Karamizadeh, S. (2011, April). The application of fusion of heterogeneous meta classifiers to enhance protein fold prediction accuracy. In Asian Conference on Intelligent Information and Database Systems (pp. 538-547). Springer, Berlin, Heidelberg.

[49] Karamizadeh, S., & Arabsorkhi, A. (2018). Skin Classification for Adult Image Recognition Based on Combination of Gaussian and

WeightKNN. International Journal of Information and Communication Technology Research, 10(2), 56-62.

[50] Fard, M. A. K., Karamizadeh, S., & Aflaki, M. (2011). Enhancing congestion control to address link failure loss over mobile ad-hoc network. arXiv preprint arXiv:1110.2289.

[51] arabsorkhi A, karamizadeh S. Method to improve the illumination normalization in adult images based on fuzzy neural network. فصلنامه11 ;2020 .41 (اطالعات فناوری and 42) :1-12

Iberian Journals

Iberian Journal of Applied Sciences and Innovation
2021 Vol 1, Issue 3

Impact of Big Five Personality Traits on Knowledge Sharing

Ali Manafi
Islamic Azad University of Iran
manafi_@yahoo.com

Behnam Nowrouzi
Islamic Azad University of Iran
behnam.nowrouzi@aol.com

Pegah Mohammadi
Islamic Azad University of Iran
mpegah88@yahoo.com

Abstract— This paper attempts to investigate how big five personality traits affect knowledge sharing in ICT companies of Iran. In this regard, several ICT companies in Tehran were studied. 355 questionnaires were gathered. At the end the result showed that extraversion, conscientiousness, agreeableness, and openness to experience have significant and positive impact while neuroticism has significant and negative impact on knowledge sharing.

***Keywords*— Extraversion, Agreeableness, Openness to experience, Conscientiousness, Neuroticism, knowledge sharing, ICT**

I. INTRODUCTION

There are many evidences that show that knowledge sharing can increase innovation in an organization (e.g. Manafi,& Subramaniam, 2015a,b; Akram et al., 2020). By SECI model (Nonaka and Takeuchi, 1995), knowledge sharing results knowledge creation. Hence, improving the level of knowledge sharing can be useful for every company and organization. Several researchers (e.g. Nguyen & Prentice, 2020; Manafi,& Subramaniam, 2015a,b; Goh &Sndhu, 2014) have characterized knowledge sharing by two dimensions including, knowledge collecting and knowledge donating. By considering the overlap of knowledge sharing and personal behavior, we need to know which personal factors are affecting knowledge sharing. In other words, the role of big five personality on knowledge sharing behavior make some ambiguities. There are many research about big five personality traits and their effects (Chaturvedi, et al., 2020; Buecker et al., 2020; Holmström, 2015; Martin et al., 2007; Komarraju & Karau, 2005). The big personality is defined as extraversion, agreeableness, openness to experience, conscientiousness, and neuroticism. On the other hands, there are many ICT companies in Iran that their performances are really dependent to the level of knowledge and innovation. These companies can improve their level of knowledge and innovation by knowledge sharing. Therefore, this study aims to find how big five personality traits can affect knowledge sharing in ICT companies of Iran.

II. Literature Review and Hypotheses Development

There are many researches that show that knowledge sharing is very important for an organization. It is consistent with resource-based

view (Nonaka and Takeuchi, 1995). According to Barney human capital can be exploited as source toward sustainable competitive advantage, because the existing knowledge of human capital is rare, non-imitable, and valuable. Table1 shows some research regarding knowledge sharing.

Table1: Related research to Knowledge Sharing

Independent variables	Dependant variables	References
Human resources practices Transformational leadership Organizational justice Organizational culture Diversity…	Knowledge sharing	Cummings, (2004); Xue et al., (2011); Manafi,& Subramaniam (2015a,b); Bradshaw et al., (2015); Tamta & Rao (2017); Zhang,(2018); Sung & Choi (2019); Akram et al.,(2020)
Knowledge sharing	Innovation; Knowledge creation; Financial performance; Organizational performance…	Kamaşak & Bulutlar (2010); Manafi,& Subramaniam (2015a); Castaneda & Cuellar (2020); Obeidat & Tarhini (2016); Nguyen & Ha (2020)

As shown in Table.1, some research are showing that which factors can affect knowledge sharing while other research concentrating the outcomes of knowledge sharing. In other words, knowledge sharing can be considered as intervening variables. Table.2 demonstrates shows the definitions of personality traits based on the different research. In other words, each trait can be characterized by different dimensions which they are shown in the Table2.

Table2: Big five personality traits

Extraversion	Sociability Assertiveness Talkativeness Excitability
Agreeableness	Affection Trust Kindness Altruism, Other prosocial behavior
Openness to experience	Like to try new things Impressed by novelty Seeking out new things Open to other people suggestion
Conscientiousness	Organized and principled Responsible Forward-thinking Persistent Goal oriented
Neuroticism	Anxiety Angry-hostility Self- conscientious, Impulsiveness Vulnerability

There are various researchers (Cobb-Clark & Schurer, 2012; Agyemang et al., 2016; Lotfi et al., 2016; Arpaci & Unver, 2020; Mahmoud et al., 2020) who have worked on big five personality traits and their outcomes. These research usually are in the area of psychology, management, or other social sciences. By above discussion, we can develop the following hypotheses:

H1: Extraversion affects knowledge sharing significantly and positively

H2: Agreeableness affects knowledge sharing significantly and positively

H3: Openness to experience affects knowledge sharing significantly and positively

H4: Conscientiousness affects knowledge sharing significantly and positively

H5: Neuroticism affects knowledge sharing significantly and negatively

III. Data Analysis and Results

This research applied quantitative method in order to find the relationship between big five personality traits and knowledge sharing. The population of this study was all employees who are working in the ICT companies of Tehran. They are programmer, technicians, and research managers/supervisors. 400 of them were chosen randomly and they were asked to fill up the questionnaire. the questionnaire of this study had 2 parts. The first part was about demographics information of respondents while the second part was to measure the variable of this study including, extraversion, agreeableness, openness to experience, conscientiousness, neuroticism, and knowledge sharing. The items of big five personality traits were adapted based on the mentioned dimensions of the Table2.

Knowledge sharing was measured by two dimensions such as collecting and donation, and the items were adapted from the research of Manafi and Subramaniam [2015a]. Table3 shows the items of measuring knowledge sharing.

Table3: Items of Knowledge Sharing

Knowledge Sharing	
Knowledge collecting	I am confident of my ability to access knowledge that the others in my learning environment would consider valuable I have the expertise required to acquire valuable knowledge from my learning environment Most of my colleagues can provide me with valuable knowledge
Knowledge Donating	I share my knowledge with my colleagues when I have learnt something new. My colleagues share with me when they have learnt new things Knowledge sharing amongst colleagues is considered normal in my organization

The research was carried out during Sep 2020 to 2021July. Out of 400 distributed questionnaires, 355 of them were usable, so all analyses were done on 355 data.

The results of reliability test were acceptable according to the Nunally (1978) for each variable because all values were greater than .7. To measure the relationship between variables of this study, Pearson correlation test was applied. The value of correlation test varies between -1 and 1. Table 4 shows the results of Pearson correlation test.

Table 4: Results of Pearson Correlation Test

	1	2	3	4	5	6
1.Knowlwedge Sharing	1					
2.Extraversion	.443	1				
3.Agreeableness	.402	.177	1			
4.Openness to experience	.271	.154	.234	1		
5.Conscientiousness	.477	.217	.171	.311	1	
6.*Neuroticism*	-.222	-.112	-.207	-.216	-.032	1

Table.4, the highest estimated relationship with knowledge sharing refers to conscientiousness while the lowest value refers to neuroticism. It should be mentioned that all personality traits have significant relationships with knowledge sharing because all p-values are less than .05. The next analysis was multiple regression analysis. Table4 shows the results of multiple regression analysis.

Table5: Results of Multiple Regression Analysis

R Square = .714
F = 172.54
P-value of ANOVA= .000
Constant= .255

Impacts	*P-value*	*Unstandardized Coefficient*	*VIF*	*Hypothesis*	*Supported*
Extraversion on Knowledge Sharing	.000	.124	1.3	H1	√
Agreeableness on Knowledge Sharing	.001	.145	1.2	H2	√
Openness to experience on Knowledge Sharing	.000	.177	1.1	H3	√
Conscientiousness on Knowledge Sharing	.023	.201	1.77	H4	√
Neuroticism on Knowledge Sharing	.047	-.122	1.55	H5	√

According to the Table5, the estimated value of r square is .714 that 71.4% of variation of knowledge sharing can be accounted by big five personality traits. All p-values are less than .05 that means that each variable has significant impact on knowledge sharing. Except neuroticisim, all personality traits have positive impact on knowledge sharing. In other words, for every unit increase in neuroticism, knowledge sharing goes down .122 units. However, the regression equation can be written as follow:

Knowledge Sharing= .255 + .124 extraversion+ .145 agreeableness+ .177 openness + .201 conscientiousness -.122 neuroticism

IV. Conclusion

The results of this study showed that all. big five personality traits have significant impacts on knowledge sharing in the ICT companies of Iran. However, all personality traits had positive impacts except neuroticism. In other words, the people with higher level of neuroticism will have fewer tendencies to donate or collect knowledge. The framework of this study can be tested in other scopes and industries. Beside of that big five personality traits has potential to be a good moderator when other variable is affecting knowledge sharing.

REFERENCES

[1] Agyemang, F. G., Dzandu, M. D., & Boateng, H. (2016). Knowledge sharing among teachers: the role of the Big Five Personality traits. VINE Journal of Information and Knowledge Management Systems.

[2] Akram, T., Lei, S., Haider, M. J., & Hussain, S. T. (2020). The impact of organizational justice on employee innovative work behavior: Mediating role of knowledge sharing. *Journal of Innovation & Knowledge*, *5*(2), 117-129.

[3] Arpaci, I., & Unver, T. K. (2020). Moderating role of gender in the relationship between big five personality traits and smartphone addiction. Psychiatric Quarterly, 91(2), 577-585.

[4]Bradshaw, R., Chebbi, M., & Oztel, H. (2015). Leadership and knowledge sharing. *Asian Journal of Business Research*, *4*(3).

[5]Buecker, S., Maes, M., Denissen, J. J., & Luhmann, M. (2020). Loneliness and the Big Five personality traits: A meta–analysis. European Journal of Personality, 34(1), 8-28.

[7]Castaneda, D. I., & Cuellar, S. (2020). Knowledge sharing and innovation: A systematic review. *Knowledge and Process Management*, *27*(3), 159-173.

[8]Chaturvedi, M. P., Kulshreshtha, K., & Tripathi, V. (2020). The Big Five personality traits as predictors of organic food purchase intention: Evidence from an emerging market. PalArch's Journal of Archaeology of Egypt/Egyptology, 17(7), 10202-10218.

[9]Cobb-Clark, D. A., & Schurer, S. (2012). The stability of big-five personality traits. Economics Letters, 115(1), 11-15

[10]Cummings, J. N. (2004). Work groups, structural diversity, and knowledge sharing in a global organization. *Management science*, *50*(3), 352-364.

[11]Goh, SK, & Sandhu, MS (2014). The Influence of Trust on Knowledge Donating and Collecting: An Examination of Malaysian Universities. International Education Studies , 7 (2), 125-136.

[12]Holmström, S. (2015). The influence of neuroticism on proenvironmental behavior.

[13]Kamaşak, R., & Bulutlar, F. (2010). The influence of knowledge sharing on innovation. *European Business Review*.

[14]Komarraju, M., & Karau, S. J. (2005). The relationship between the big five personality traits and academic motivation. Personality and individual differences, 39(3), 557-567.

[15]Lotfi, M., Muktar, S. N. B., Ologbo, A. C., & Chiemeke, K. C. (2016). The influence of the big-five personality traits dimensions on knowledge sharing behavior. Mediterranean Journal of Social Sciences, 7(1 S1), 241-241.

[16]Martin LR, Friedman HS, Schwartz JE. Personality and mortality risk across the life span: the importance of conscientiousness as a biopsychosocial attribute. Health Psychol. 2007;26(4):428-36. doi:10.1037/0278-6133.26.4.428

[17]Mahmoud, M. A., Ahmad, S., & Poespowidjojo, D. A. L. (2020). Intrapreneurial behavior, big five personality and individual performance. Management Research Review.

[18]Manafi, M., & Subramaniam, I. D. (2015a). Relationship between human resources management practices, transformational leadership, and knowledge sharing on innovation in Iranian electronic industry. *Asian Social Science*, *11*(10), 358.

[19]Manafi, M., & Subramaniam, I. D. (2015b). The role of the perceived justice in the relationship between human resource management practices and knowledge sharing: A study of Malaysian universities lecturers. *Asian Social Science*, *11*(12), 131.

[20]Nguyen, TM, & Prentice, C. (2020a). Reverse relationship between reward, knowledge sharing and performance. Knowledge Management Research & Practice , 1-12.

[21] Nguyen, P. K., & Ha, T. M. (2020b). Social capital, knowledge sharing and financial performance. *Social Capital*, *14*(1).

[22] Nonaka, I & Takeuchi, H 1995, The knowledge creating company. How Japanese companies create the dynamics of innovation, Oxford University Press, New York

[23] Karamizadeh, S., Shayan, J., Alizadeh, M., & Obeidat, B. Y., & Tarhini, A. (2016). A Jordanian empirical study of the associations among transformational leadership, transactional leadership, knowledge sharing, job performance, and firm performance: A structural equation modelling approach. *Journal of Management Development*.

[24] Sung, S. Y., & Choi, J. N. (2019). Effects of diversity on knowledge sharing and creativity of work teams: status differential among members as a facilitator. *Human Performance*, *32*(3-4), 145-164.

[25] Tamta, V., & Rao, M. K. (2017). The effect of organisational justice on knowledge sharing behaviour in public sector banks in India: mediating role of work engagement. *International Journal of Business Excellence*, *12*(1), 1-22.

[26] Xue, Y., Bradley, J., & Liang, H. (2011). Team climate, empowering leadership, and knowledge sharing. *Journal of knowledge management*.

[27] Zhang, Z. (2018). Organizational culture and knowledge sharing: design of incentives and business processes. *Business Process Management Journal*.