The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973

The Critical Determinants of Application of Blockchain Technology in Enhancing Cyber security in the Modern Technology Era

Preety Tak
Master's in Computer Application
Managing Director (Infoserv LLC)
Janardan Rai Nagar Vidyapeeth (Rajasthan), Udaipur

Abstract
Blockchain is a framework that joins a unique arrangement of properties to ensure network security, straightforwardness, and perceivability, including a decentralized construction, conveyed records and capacity instrument, agreement convention, brilliant agreements, and uneven encryption. The following six factors—cybersecurity, corruption prevention, e-government advancement, effective governance, political stability, and democratic participation—were put to the test for blockchain adoption. The study demonstrates that political stability, government efficiency, and cybersecurity are important determinants. The possibility that a country will adopt blockchain technology is increased by elevated degrees of cybersecurity and effective government. Ironically, more political stability makes it less likely that blockchain technology will be adopted quickly. The Blockchain Drive filled in as the wellspring of information for blockchain reception, but it is important and crucial to systematically compile information on blockchain efforts throughout the world. Further data collection efforts by international donor organisations are required in order to improve the models for blockchain adoption.
Keywords: Blockchain Technology, Cyber security, Determinants, Modern technology

1. Introduction

The technology involved of Bitcoin, known as blockchain technology (BT), has evolved with a variety of intriguing potential uses. In less than ten years, BT has attracted investments from a wide variety of businesses, encouraged the formation of several consortia, and raised more than US$3.1 billion in venture capital [1]. It is anticipated that the BT-created cryptocurrency market would have a market value of more than US$143 billion [2]. Also, the public sector and academic institutions have used BT [3], and governments have been developing and planning the use of blockchain in the public sector [4]. According to KPMG [5], $14.2 billion was invested in US fintech startups in the first half of 2018. Moreover, BT has been used in both the public and commercial sectors, and according to over 53% of survey participants from Deloitte, BT is a top priority for their businesses [6]. With its features that support verification, identification, authentication, integrity, and immutability guaranteed by cryptography, transparency, decentralised smart contracts, and smart ledgers, blockchain technology promises a new level of conducting business transactions between

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973
untrusted parties. Blockchain technology allows for the sharing of transactions over a wide network of untrusted parties and chronologically linked and duplicated digital ledgers in a decentralised database. Moreover, it offers independent verification assurances that do not require a centralised authority. Moreover, because there are no centralised authority, blockchain services can offer greater security characteristics for distributed systems and can apply immutability against abuse and oversight even in the presence of a malevolent insider. There are doubts regarding BT's durability because it is a cutting-edge technology that holds out a lot of potential [7]. If there is such authority in a system, then the most powerful entities might collude to alter the blockchain or stop the transmission of its data. Many cybersecurity flaws have been found in blockchain implementations, and there have been numerous documented hacks [8]. In a recent article, the New York Times reported that the U.S. Department of Justice is suing the U.S. Department of Justice over its handling of a case involving a rogue prosecutor. By combining address analyses to determine the owner of each wallet, the attackers may determine the international activity of these wallets [9].

These flaws make it uncertain if BT can actually provide the security guarantees it provides. Users' concerns about BT's security have increased as a result of the rising usage of the company as a service provided by governments or big businesses, including the financial technology sector. Many reports regarding cyberattacks and cybersecurity flaws at BT have recently been released. For instance, 8833 active Ethereum smart contracts have a combined balance of 3,068,654 million ethers, or nearly $30 million USD [8], which makes them susceptible. Due to the smart contracts' flaws, monetary losses are likely. For instance, a hacker broke into Mt. Gox in 2014, the biggest BTC trading site, and stole Bitcoins worth US$450 million, causing Mt. Gox to shut down. Another instance is when a hacker was able to access the Decentralised Autonomous Organisation (DAO), a smart contract on the Ethereum blockchain, and steal Ethers, which were worth more than US$60 million in 2016 [10]. According to [11], recent studies on BT's cybersecurity idea have focused mostly on how blockchain may secure both present and future systems.

It's crucial to recognise these three blockchain characteristics: There are three types of ledgers: 1) decentralised and distributed networks, where each node maintains a complete record of transactions; 2) irreversible and immutable, where the ledger is append-only with immediate reconciliation allowing trusted exchanges; and 3) nearly real-time updates of the ledger [16]. All three of these qualities may be advantageous to the government since they make it possible for transactions to be completed in a secure and safe manner, which is crucial for government organisations that handle sensitive data gathered from the public. Blockchain offers a quick and effective way to retain documents in the public sector while maintaining their secrecy and integrity [19].

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973

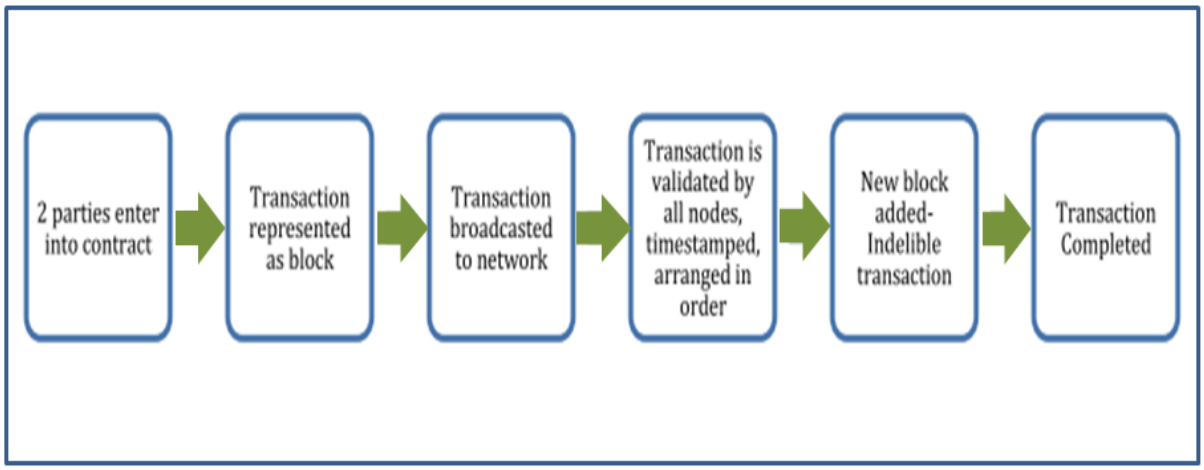

Figure1 Work flow of Blockchain

Several blockchain initiatives have been launched by national governments worldwide just a few of the American federal agencies that have started blockchain initiatives. As a pioneer in e-government, Estonia has tested the use of blockchain in voting, identity management, and healthcare. United Arab Emirates, Singapore, and Switzerland have also started moving towards embracing blockchain for identity management. Blockchain technology has been adopted for property records and transactions in Brazil, Sweden, and the United Kingdom. The analysis is helpful in determining the elements that facilitate early technology adoption.

1.1 Objectives-

- To illustrates the key elements of blockchain adoption to implement best practises in modern technology.
- To show the need of effective cybersecurity in a nation-state and to highlight common characteristics of blockchain adoption so that other countries can implement best practises.
- To lists a few nations that are pioneers in using blockchain technology.

2. Literature Review

2.1 Blockchain Technology

Blockchain innovation comprises of carefully designed and alter obvious computerized records that are worked as disseminated frameworks without a focal vault and much of the time without a focal power, like an administration, bank, or organization. It empowers clients inside a local area to keep exchanges on a neighborhood shared record. At the point when exchanges are distributed as a component of the customary working of the blockchain network, they can't be changed. In 2008, the BT concept and other computer ideas and technologies were combined to create a brand-new coin that was based on blockchain. With the send-off of the BTC digital currency in 2009, which enabled digital money transfers within a distributed ledger, BT rose to fame. Clients' computerized privileges can be moved to another Bitcoin user and digitally signed in Bitcoin. In addition, a circulated gathering of clients freely oversees and keeps up with the BTC blockchain, and this, joined with cryptographic instruments, makes BT's strength towards resulting endeavors to change the record by manufacturing the exchange or modifying the blocks. The BTC blockchain reports

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973
this transfer freely to all the organization clients in order for them to independently verify the transaction's validity. Some people prefer to limit blockchain technology (BT) to cryptocurrency solutions mainly since it has made it possible for the expansion of multiple crypto currency systems, like Ethereum and Bitcoin. Nevertheless, many different industrial sectors are considering utilising BT in their applications [12].

The idea of electronic money was first presented in the Nakamotos white paper [13], and after the 2009 debut of the BTC digital money, BT became one and only of the most discussed advances. Blockchain is a collection of data blocks connected by a cryptographic hash function, with replicated data kept on the servers of all participants. The database of BT contains absolute data. It can only expand by authorised users (miners) with strong cryptographic capabilities adding new blocks (data) at the end of the chain. They can do this by using a competitive mining scheme to add the new blocks. Blockchain is not bitcoin. One of the numerous programmes using BT to help the BTC digital currency organization, which enables the transmission of digital money inside a distributed ledger, is Bitcoin. There are other additional cryptocurrencies, including Binance Coin, Ethereum, Bitcoin Cash, Litecoin, and Ripple (XRP) (BNB). BTC users can digitally sign over their ownership of a BTC to another BTC user. A circulated gathering of clients freely oversees and keeps up with the BTC blockchain, and this, joined with cryptographic instruments, makes BT's non-renouncement capacity against endeavors to alter the record by fashioning the exchange or changing the blocks. The BTC blockchain declares this move openly to all organize clients, permitting them to check the exchange's legitimacy freely.

Private, civic or permission less, and united or consortium blockchains are the three basic varieties of BT. Both private and association blockchains are regarded as permissioned; access rights must be granted by a permission management body to known and trustworthy participants. Bitcoin, Etherum, and Monero are a few examples. With the advent of the internet, the world has become a global village.

2.2 Risks to Cybersecurity and Incidents on the Blockchain Network

From 2011 and the first half of 2019, we counted 65 real-world cybersecurity events that had a negative impact on blockchain systems. Based on the cost of the stolen coins at the time the assaults were identified, we compute the impact statistics that were provided by the source. As our exploration depends on openly accessible information from discussions, news channels, and other academic publications, the reported examples might not be comprehensive. Most occurrences don't provide enough information on the actual circumstances that led up to them. As a result, we offer an elevated cataloguing of 3 sorts, namely smart contract faults, scams, and hacks.

Around US$3 billion has been spent as a result of cybersecurity incidents between 2011 and 2019. Hacking caused the largest loss, which is equivalent to more than US$1.6 billion. Scams caused the second-highest loss, which is equal to more than US$1.1 billion, while smart contract errors caused the third-highest loss, which is equal to more than US$289 million. From 2015, both the price of BTC and the frequency of attacks grew significantly, reaching a peak of 12 attacks in 2018. The amount of loss caused by the occurrences followed the same pattern, peaking in 2018 at US$1.6 billion after reaching US$7 million in

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973
2015. There were just seven occurrences in the first half of 2019 and a loss of US$131 million.

The main 10 online protection occurrences on blockchain networks somewhere in the range of 2011 and 2019 in terms of monetary damage demonstrates that a Ponzi scheme inflicted the biggest damage lost a combined total of US$660 million [12] after investing in Ifan and Pincoin in April 2018. Victims were unable to pay out their gains. The investment is promoted as a risk-free activity with earnings of up to 45% monthly through a variety of bonus schemes that provide early investors an advantage over later investors. This is a standard pyramid scheme. The second-largest loss was incurred by Coincheck, which experienced a record deficiency of 530 million in digital currency [18] as a result of an external intrusion into their system in January 2018. With 68% of the BTC market, Coincheck offers exchange and wallet services [19].

3. Research Methodology

The adoption of blockchain by a nation is the reliant variable for this review. There isn't currently global organisation gathering information on country usage of blockchain technology. We used the IBI data in this work since no other complete data were accessible from a trustworthy institution [7]. Our dependent variable, which shows whether a nation has implemented blockchain technology or not, is based on the IBI data. As a result, the dependent variable only has two possible values: 1 for adoption and 0 for non-adoption. As of 2018, 40 nations have implemented blockchain-related activities [7]. Since those countries are only now beginning to adopt technology, these nations are the top users of blockchain. There are 213 nations in the globe that make up our population, according to figures provided by the World Bank. We utilise LR to find the characteristics that explain the adoption of blockchain technology because the dependent variable is binary. Version 15 of the STATA statistical programme was used for the calculations. As will be detailed below, there are 6 self-governing variables that correlate to the 6 hypotheses. We are one year behind the independent variables [20].

The Global Cybersecurity Index (CyberSec), a gauge of a nation's cybersecurity, is the first independent variable. The International Telecommunication Union (ITU), a specialised body of the UN for information and communication technologies, provided the statistics. The index gauges the 193 ITU Member States' dedication to cybersecurity. The ITU Global Cybersecurity Agenda's five pillars—legal, technological, organisational, capacity building, and international cooperation—are used to measure the index. Higher numbers indicate a better commitment to cybersecurity policy. This score runs from 0 to 1. It is assumed that countries with better Cybersec scores will adopt blockchain technology.

H1: Blockchain will be used by nations with greater levels of cyber security.

The U.N. E-Government Development Index (E-Gov), which gauges e-government success internationally, serves as the second independent variable. The development of e-government in United Nations Member States is shown in this index. The E-Government Development Index takes into account access factors like infrastructure and educational levels in addition to a country's website development to show how that nation is utilising information

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973
technology. The index is a combined measurement of three crucial aspects of e-government, including the quantity and calibre of online services, the state of the telecommunications system, and the availability of skilled workers in the field. Higher values on this indicator, which goes from 0 to 1, represent nations where e-government development is more advanced. It is assumed that countries with stronger E-Gov ideals will adopt blockchain technology.

H2: Blockchain will be used by nations with a greater level of e-government development.

Government Effectiveness (GovEff), the third independent variable, is based on World Bank governance metrics. This variable reflects opinions on the effectiveness of public services, the civil service's effectiveness and level of political independence, the effectiveness of policy creation and implementation, and the legitimacy of the government's adherence to such policies. The estimate provides the aggregate indicator score for the nation in standard normal distribution units, i.e., 2.5 to 2.5, with zero as the mean. We postulate that adoption of blockchain technology will result from improved government efficiency.

H3: Blockchain will be adopted by nations with more effective governments.

The Control of Debasement (Defilement) List, one of the World Bank's administration markers, is the fourth autonomous variable. This variable thinks about conclusions how much open authority is utilized for private advantage, enveloping limited scope and huge scope debasement as well as the "catch" of the state by elites and confidential interests. The standard blunder shows how precisely the evaluation of administration is made. Less exact assessments are demonstrated by better quality blunder values. The gauge gives the total pointer score to the country in units of a standard typical circulation with a range of 1.8 to 2.3 and a mean of zero. We believe that using blockchain technology would help a nation combat corruption on a larger scale.

H4: Blockchain adoption will be higher in nations with stronger anti-corruption measures.

4. Results and Discussion

Figure 2 shows a graph of the unrestricted factors, contrasting the Group I nations (those that have not implemented blockchain) with the Group 2 countries. Group I consists of 175 nations, though Group II is made up of 42 nations. The standard of all of the blockchain reception variables is, on average, greater for Group II nations than Group I republics. The average index of Global Cybersecurity for Group I nations is 0.30, but it is 0.65 for Group II nations. For nations in Groups I and II, the readings for the UN E-Government Development Index are 0.50 and 0.78, respectively. Similar trends may be seen in the governance of World Bank metrics for reducing corruption, improving government performance, maintaining political immovability, and promoting voice and liability. In these, the averages for Group 2 nations are positive and above zero whereas the averages for Group 1 countries are negative. This data demonstrates that nations that have adopted blockchain technology have better results across the board. This suggests that countries who are early adopters of blockchain technology have stronger national contexts for cyber security, corruption, digitalized-government growth, effective governance, and political immovability [20].

The Ciência & Engenharia - Science & Engineering Journal
ISSN: 0103-944X
Volume 11 Issue 1, 2023
pp: 964 – 973

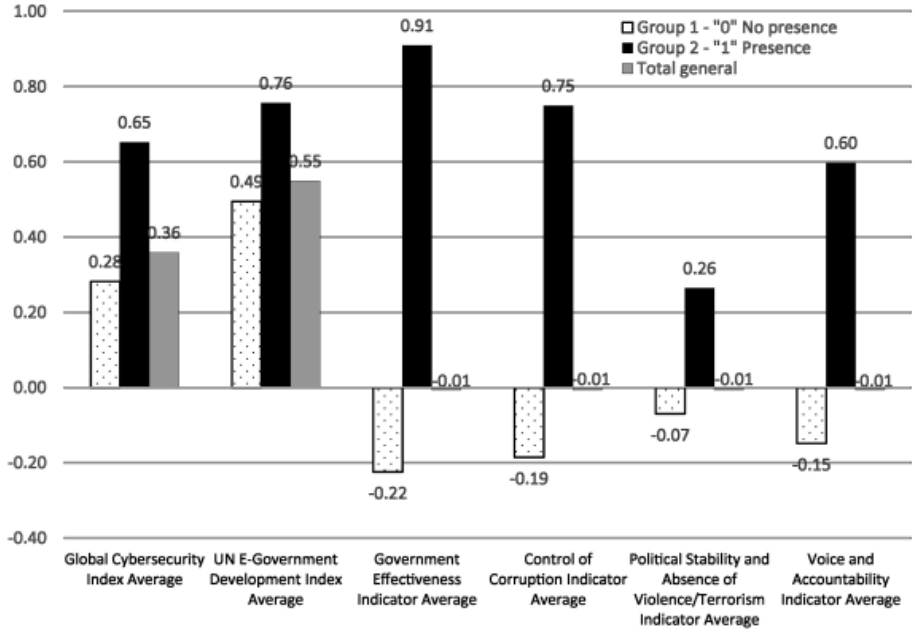

Figure 2 Averages of the key aspects of blockchain adoption in the public sector are compared across groupings of nations, adapted from [20].

The data supports 2 hypotheses (H1 and H3) which contend that improved cyber security and efficient government are crucial for blockchain acceptance. The likelihood of adopting blockchain technology rises by 6.12 percentage points on average for each point a country gains on the idex of Global Cyber security. According to this, the likelihood of accepting blockchain technology rises by 2.65 % focuses on normal for each extra rate point that a nation's Administration Performance score improves [20].

4.1 Consequences of the findings

Overall findings highlight the organisational, technological, and conservational elements that support blockchain implementation among major national governments. The biggest adopters of technology are those worried about cybersecurity. Blockchain presents a number of cybersecurity opportunities, especially with the safe disseminated record. Digitalized government advancements did not seem to be a reliable indicator of the main blockchain adoption. This conclusion is especially intriguing since it demonstrates that the adoption of new technologies is not always linear, i.e., nations do not always need to already have sophisticated technology infrastructure to adopt innovations like blockchain. Other perceived motivations (such as security, quarrying, digital currency, or other government responsibilities like E-casting a ballot, management of identity, clinical management, etc.) may encourage countries to adopt blockchain technology more quickly.

Effectiveness of government is a strong analyst of top blockchain adopters on the internal organisational side. Early adoption of blockchain is more common in nations with better levels of civic and domestic services quality. Blockchain presents chances to boost business productivity and provide services in novel ways. For instance, smart contracts might improve the effectiveness of contracting methods with automatic expenditures and make the replies more safe, precise, and effective than the current bureaucracy. Control of corruption,

regardless of what blockchain promises in terms of objectivity and traceability, does not seem to be a key predictor of the main adopters. Defilement is a complex political and cultural issue that could possibly be constrained by blockchain-based innovation arrangements.

Political immovability is a strong interpreter of blockchain adoption on the external environment side, but not in the way we predicted. The likelihood that blockchain technology will be adopted by the top adopters declines with increased political stability. Moreover, democratic involvement is not a reliable indicator of blockchain acceptance. Ultimately, the adoption of blockchain has a contradictory connection with the outside world. Our non-linear connection tests demonstrate that the prototypical parameters are accurate. The political instability difficulties up to a point might encourage the adoption of blockchain technology.

5. Conclusion

This research has various policy ramifications. Blockchain is important for cybersecurity, to start. Blockchain use is advancing quickly in nations with improved cybersecurity. Blockchain integration into a nation's cyber security plan would be a good idea. Blockchain adoption would be challenging without taking cybersecurity into account. Cybersecurity is a key issue for all governments throughout the world in this quickly expanding digital era. Blockchain can aid in delivering transparent and secure digital processes. Second, countries trying to improve the efficiency of their governments have a good chance to do so by using blockchain technology. Our research demonstrates that encouraging governments to actively use blockchain is important. E-casting a ballot, management of identity, clinical management, management of supply chain, and property management are just a few of the uses for blockchain that are possible. Blockchain has the potential to improve record keeping, speed up reconciliation, boost security, and reduce access management costs [9]. By automated payments, smart contracts provide increased administrative effectiveness and short reaction times.

The nations have embraced a number of blockchain initiatives. We did not make a distinction between those who have implemented several initiatives and those who have not. Finally, the analysis of early users of blockchain technology may also be fundamentally constrained by the diffusion of innovation idea. For further insights, other speculations that consider institutional and administration frameworks can likewise be utilized.

References

[1] Alexopoulos, C., Androutsopoulou, A., Lachana, Z., Loutsaris, M.A., & Charalabidis, Y. (2018). BlockChain Technologies in Government 3.0: A Review. EGOV-CeDEM-ePart 2018, 11.

[2] Anand, S. (2018). A Pioneer in Real Estate Blockchain Emerges in Europe. Wall Street Journal. Retrieved from https://www. wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601.

[3] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D. et al. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143-174.

[4] Atzori, M. (2017). Blockchain technology and decentralized governance: Is the state still necessary? Journal of Governance and Regulation, 6(1), 45-62.
[5] Baker, J. (2012). The Technology – Organization – Environment Framework. In: Dwivedi Y., Wade M., Schneberger S. (eds) Information Systems Theory. Integrated Series in Information Systems, 28. Springer, New York, NY.
[6] Batubara, F. R., Ubacht, J., & Janssen, M. (2018). Challenges of blockchain technology adoption for e-government: a systematic literature review. Paper presented at the Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age.
[7] Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. OECD Working Papers on Public Governance (28), 1-53.
[8] Damanpour, F., & Schneider, M. (2008). Characteristics of innovation and innovation adoption in public organizations: Assessing the role of managers. Journal of Public Administration Research and Theory, 19(3), 495-522.
[9] Davidson, S., De Filippi, P., & Potts, J. (2016). Disrupting governance: The new institutional economics of distributed ledger technology. Available at SSRN 2811995.
[10] Diallo, N., Shi, W., Xu, L., Gao, Z., Chen, L., Lu, Y. et al. (2018). eGov-DAO: A better government using blockchain based decentralized autonomous organization. Paper presented at the 2018 International Conference on eDemocracy & eGovernment (ICED
[11] Hou, H. (2017). The application of blockchain technology in E-government in China. Paper presented at the 2017 26th International Conference on Computer Communication and Networks (ICCCN).
[12] Hyvärinen, H., Risius, M., & Friis, G. (2017). A blockchain-based approach towards overcoming financial fraud in public sector services. Business & Information Systems Engineering, 59(6), 441-456.
[13] Iansiti, M., & Lakhani, K. (2017). The truth about blockchain. Harvard Business Review. Harvard University. Retrieved, 27(9). Jun, K.-N., & Weare, C. (2010). Institutional motivations in the adoption of innovations: The case of e-government. Journal of Public Administration Research and Theory, 21(3), 495-519.
[14] Jun, M. (2018). Blockchain government-a next form of infrastructure for the twenty-first century. Journal of Open Innovation: Technology, Market, and Complexity, 4(1), 7.
[15] Karch, A. (2007). Emerging issues and future directions in state policy diffusion research. State Politics & Policy Quarterly, 7(1), 54-80.
[16] Killmeyer, J., White, M., & Chew, B. (2017). Will blockchain transform the public sector. Blockchain basics for government. A report from the Deloitte Center for Government Insights. Retrieved from: www2.deloitte.com/content/dam/ insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-publicsector.pdf.
[17] Kim, K., & Kang, T. (2017). Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology. Retrieved

from https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kangblockchain-technology.pdf.

[18] Krugman, P. (2018). Transaction Costs and Tethers: Why I'm a Crypto Skeptic. New York Times. Retrieved from https://www. nytimes.com/2018/07/31/opinion/transaction-costs-and-tethers-why-im-a-crypto-skeptic.html.

[19] Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (Eds.). (2020). Blockchain for cybersecurity and privacy: architectures, challenges, and applications.

[20] Reddick, C. G., Cid, G. P., & Ganapati, S. (2019). Determinants of blockchain adoption in the public sector: An empirical examination. *Information Polity*, *24*(4), 379-396.