Journal of Sustainable Economics and Management Studies (ECOMAN)

VOLUME: 3, ISSUE: 1

JUNE 2022

ISSN: 2718-1057

e-ISSN: 2791-8084

Istanbul Gelisim University Press

Journal of Sustainable Economics and Management Studies (ECOMAN)
(International Peer–Reviewed Journal)

VOL. 3 • ISSUE 1 • JUNE 2022 • ISSN: 2718-1065 & e-ISSN: 2791-8084

Owner on Behalf of Istanbul Gelisim University
Prof. Dr. Bahri ŞAHİN

Correspondence:
Istanbul Gelisim University,
Cihangir Mh. Sehit J. K. Er Hakan Oner Sk. No: 1 34310 Avcilar / Istanbul / TURKEY
Phone: +90 212 4227000 **Fax:** +90 212 4227401
E-mail: ecoman@gelisim.edu.tr
Web: https://dergipark.org.tr/en/pub/ecoman

CONTENTS

Pages

Journal of Sustainable Economics and Management Studies
(ECOMAN)
ISSN: 2718-1065 & e-ISSN: 2791-8084
Vol. 3, Issue 1, June 2022

Article Statistics

Articles of this Issue	2
Corrected Articles	2
Rejected Articles	
Accepted Articles	

All articles submitted to our journal are analyzed by plagiarism detection tools.

The Environmental Effects of Cryptocurrency Mining in the World

Fatih ULAŞAN*

Abstract

Cryptocurrency is called as a digital or virtual currency, is included in the financial system independently of the monopoly of legal authorities and is difficult to control. Since the market value and transaction volume of cryptocurrencies is very large, it brings significant change on a global scale. Cryptocurrencies have disadvantages as well as advantages. Some of environmental impacts triggered by the cryptocurrency mining can be expressed as the high electricity consumption, the increased carbon footprint and the generation of the electronic waste. In this study, the structures of the cryptocurrency and block-chain technology are analyzed, and the amount of energy consumed by the cryptocurrency mining and its environmental dimensions (environmental and social consequences) are examined. Lastly, activities to prevent the environmental impacts of mining activities are evaluated.

Keywords: *Cryptocurrency, Public Administration, Technology, Bitcoin, Environment*

1. Introduction

The developments experienced in the last 50 years have been so great that they have caused a profound impact on societies and countries. Especially with the spread of the "internet" in 1993, technological developments became widespread and the internet began to change traditional systems. The presentation of Bitcoin in 2009 changed the definition and conditions of the use of money. Bitcoin can be seen as a breakthrough for the computer science field, based on 20 years of research on the cryptographic currency and 40 years in cryptography by thousands of researchers in the world. It offers a method for Internet users to transfer a unique digital property to other Internet users, while ensuring that the transfer is safe for everybody. Contracts, assets, bonds and etc. are exchanged by means of a distributed trust network which does not need or rely on a central intermediary such as banks or brokers. The owner can just send his/her own assets, recipients can just receive them, assets can just be in a place at a time, and anyone can verify transactions and the proprietorship of assets at any time (Marc, 2014). The cryptocurrency is the next level in the process of the evolution of money and can be

Original Research Article
Received: 09.10.2023
Accepted: 30.10.2023
* Dr., Republic of Türkiye Ministry of Justice (Public Prosecutor), Zonguldak, TÜRKİYE.
E-mail: fatih_ulasan@hotmail.com ORCID https://orcid.org/0000-0003- 3301-4823

thought as the electronic money that has no connection with objects of the material world. The creation of money, the distribution of money and the maintenance of money are not directed and controlled by a central bank. This system uses the software that shares peer-to-peer connection and manages exchanges like a digital wallet. It has a decentralized structure in a large community. The transfer of the currency from one wallet to another consists of coins, security accounts, debit cards, bank accounts, paper money and digital bits without requiring collateral. Cryptocurrency relies on the specialized personal computer hardware that mines new coins with the process requiring the significant computing power (Pasquale, Rana, Tarabella, and Tricase. 2017:1-2).

Nowadays, people's interest in cryptocurrencies is increasing in number due to their rapid price changes, the volatility in markets and their speculative features. For example, Bitcoin is considered as the most commonly used virtual currency around the world. There are 1565 cryptocurrencies used in today's markets. The total capital size of Bitcoin, the most frequently used cryptocurrency, is 115 billion dollars (Taş and Kiani, 2018: 370). On February 2011, the value of Bitcoin was 1 US dollar. In March 2013, the market value of Bitcoin reached 100 dollars and the transaction volume exceeded 1 billion dollars. Bitcoin has become very popular and has continued to rise regularly due to the excessive demand. The rapid value increase experienced by Bitcoin has risen regularly and broken new records, despite the experience of speculative sudden losses in value in some periods (Demartino, 2018: 42-66). However, in an uncontrolled way, people started mining with their own computer hardware, then in rooms full of processors and graphics cards, which are the main mining hardware, which accelerate the mining process, and finally with devices that only provide the mining process. This has resulted in the unbalanced and uncontrolled high energy expenditures and electronic waste throughout the world. The negative environmental effects caused by the energy consumption, carbon emissions and the amount of the electronic waste during the crypto mining raise concerns about cryptocurrencies. An average of 81% of global energy consumption is based on fossil fuels, and since the interest in the crypto mining increases, it is likely to cause serious problems in the energy consumption in the future (International Energy Agency, 2020). Although there are many studies on the financial advantages, legal recognition, use and risks of cryptocurrencies, the number of studies on the effects of the energy consumption, carbon emissions and the amount of the electronic waste resulting from the production of these digital assets on the environmental sustainability, global warming and climate changes are limited. The aim of the article is to examine the effects and possible consequences of the production chain of cryptocurrencies on environmental sustainability and to contribute to the literature by making suggestions.

In the first part of the article, basic concepts about the cryptocurrency and cryptocurrency mining are explained. First of all, blockchain technology, which is the work system of Bitcoin and alternative cryptocurrencies, is explained and the historical

background, features and the functions of the blockchain technology are examined. Then, the main algorithms that enable this technology to work are explained. The mining process that ensures the operation and the survival of the blockchain technology is explained. In the second part, the dangers caused by the mining process on the environment are explained. The environmental problems caused by mining operations in the world are examined and their environmental effects are analyzed in detail and the steps taken to reduce these effects are evaluated.

2. Cryptocurrency

Cryptocurrency can be briefly defined as a digital or virtual currency with the encryption for security purposes. Money is placed in virtual wallets through the use of passwords and is used with the same password. The feature of the crypto money is that it is used without any central authority, is closed to the intervention of countries, and cannot be manipulated (Günay and Kargı, 2018: 62; Bunjako , Trajkovska and Kacarski , 2017: 32). This feature mostly comes from the technology called as blockchain. Satoshi Nakamoto's original article titled Bitcoin in 2008 included the word of blockchain. Blockchain, the underlying technology of cryptocurrency, is defined as a block of data chained in the cryptographic form (Altay & Sumerli, 2020: 28).

In the Turkish law, when the issue of attributing the monetary value to crypto assets is evaluated within the scope of the law of obligations and the subject of the act is money, the payment with crypto assets should be accepted as an datio in solutum (Çon , 2022: 234). Cryptocurrencies are also defined as the virtual and digital money or crypto assets. The article 3 of the regulation by the OECD, the European Union and the Central Bank of Turkey on April 16, 2021, defines cryptocurrencies and states that: *It refers to intangible assets that are created virtually using distributed ledger technology or a similar technology and distributed over digital networks, but are not qualified as fiat money, registered money, electronic money, payment instrument, securities or other capital market instruments.*" (6493 Sayılı Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun, 2013). The cryptocurrency is created to facilitate peer-to-peer transactions and is independent of any intermediary. Coins are not printed or produced physically and they only exist digitally. Since cryptocurrencies cannot be stored in the bank, they cannot be withdrawn from there, but their transfer is possible.

The only proof of the existence and ownership of the crypto money is the transaction record in the blockchain. These records contain cryptocurrency records that are distributed on the blockchain, similar to an accounting ledger, and are open to everyone. It is possible to use cryptocurrencies as a peer-to-peer medium of the exchange when there is an accounting ledger. This ledger is accessed via blockchain and personalized passwords are used. Those who prepare ledgers are called as miners. They approve the transactions by acting similar to the clearing house and update the account books by acting similar to accountants (Türk Bilişim Vakfı, 2020: 33-34). David Chaum, the first software expert of digital currencies, founded the International Cryptological Research

Institute and created the DigiCash, which is described as the first digital payment system (David Chaum personal Webpage, 2023). When the concept of the cryptocurrency is mentioned, it essentially emerged on October 31, 2008, when Satoshi Nakamoto sent an e-mail with "Bitcoin P2P e-cash paper" to "the cryptography mailing" group of a site called metzwod.com (Rodrigues, 2021). Nakamoto announced Bitcoin as the first cryptocurrency with his article published in 2008 under the name of end-to-end payment system and made history about the first digital money in a distributed database made with the encryption technology (Berentsen, 2019).

2.1. Cryptocurrency Concept

The form of money does not matter if it is used as a means of the payment and accepted by society. In this case, the expected benefit from money can also be obtained through paper, electronics or simple metals. The evolution of money started from the commodity money and progressed to the electronic virtual currencies that are popular these days. Although the virtual money is not basically money regulated by any institution or organization, it is also used as money in its traditional sense in certain situations. While defining the virtual money, the European Central Bank (2012) stated that it had no regulation, was generally controlled by those who create it, and was a money accepted by the virtual society. The digitalization of money has accelerated commercial transactions and made them safer, thanks to the rapid movement of money. Due to the existence of different ideas and definitions on cryptocurrencies, the European Parliament has categorized the definitions made by various organizations such as the European Central Bank, IMF, Payments and Market Infrastructures Committee, European Banking Authority and the World Bank, and although there is no unity for the definitions, cryptocurrencies are considered as sub-types of virtual currencies. The cryptocurrency can be treated similarly to money (in return for which goods and services can be received), but is independent of national borders, central banks, financial institutions and fiat currencies (it is not issued by the state and transactions are not intermediary). Additionally, the cryptocurrency can be bought and sold on global exchanges that operate according to cryptographic principles that ensure secure and verifiable transactions, and is based on the data sharing between users directly, without a third party such as a central server (Ertz & Boily, 2019).

2.1.1. Features of the Cryptocurrency

The cryptocurrency was born as a digital asset that is secure and transferable with the help of cryptography, and the popularity of Bitcoin increased especially in 2011, and following the increase in this popularity and recognition, alternative crypto currencies began to emerge (White 2015: 383-384). The crypto asset was first designed and implemented as a solution to the financial crisis. Satoshi implemented this electronic payment system, believing in the unshakable and durable nature of the cryptographic proof instead of trust in currency. The crypto asset is based on the cryptographic proof rather than trust, and two parties can transact directly with each other without a 3rd

party intermediary. Buyers can be protected by routine escrow mechanisms (Nakamoto, 2008: 1). This is the peer-to-peer electronic network that gives people the opportunity to make anonymous transactions without financial intermediaries. It was initially used for online payments in the form of the electronic cash that could be held as a means of exchange for short or long-term investment purposes or for speculation purposes. As its popularity and frequency of use increased over time, the days were used in many tasks such as business and company mergers. Since regulated capital raising processes are not implemented in this system, it is also used in Initial Coin Offerings (ICO), which are used as a quick and easy source of financing for startups (Peters, Panayi and Chapelle, 2015; Murşan , 2023: 40). Recently, the number of crypto assets has increased significantly in the world, and cryptocurrencies with more than 500 different types such as Bitcoin, Ethereum, Ripple, Litecoin and Dash have increased day by day. These assets are not tied to any authority or center, are digital in nature, cryptocurrency prices vary, and have the anonymity in use. Although there are many crypto currencies, they have some common features (Doğan and Hilal, 2021: 143);

- It has a limited range of uses and also a limited range of acceptance,
- The opportunity for public or private companies to insure crypto money is very limited.
- It is a very complex and advanced system produced with cryptology.
- It can be produced by mining,

The change and deletion of transactions is very difficult due to the structure of the system.

2.1.2. Mining

Cryptocurrencies are basically a system created by combining multiple complex technologies. The name of the mathematical problem solving in the existing blocks in the blockchain is considered as the cryptocurrency mining, and this mining is the name of the method in validating the virtual money transactions obtained after complex transactions with special software devices and hardware and subsequently rewarded with the virtual money as the outcome of the transactions. All transactions such as the Bitcoin and altcoin mining are carried out with this method. Miners carry out these transactions by purchasing electronic parts such as computer processors and graphics cards, and millions of devices that perform the transactions try to solve unique problems in the blocks in order to surpass each other. After solving the problem, they produce new virtual currencies and cryptocurrency rewards are earned in return. Rewards can be converted into the fiat currency using online exchange platforms. The cryptocurrency mining is mostly done in four different mining types (Binance Academy,2023) as the CPU, GPU, ASIC and Cloud mining.

Since the number of miners were small in the early days, it is possible to earn high amounts from mining. However, in the current situation, the number of miners have

increased, the cost has increased and the profits have decreased. While miners ensure the security of the blockchain and the transfer of cryptocurrency, the transactions are documented in the distributed ledger. Because the blockchain technology is called as an open account, users have the opportunity to control their transactions (Dilek and Furuncu, 2018:96).

2.2. Blockchain Technology

The control, management, maintenance and security of data have become very important for people. Blockchain technology, which emerged to meet these needs, was introduced in 2008 and became known with Bitcoin in 2009. Blockchain is known as a distributed ledger and a distributed, shared, encrypted, irreversible and incorruptible information store. Blockchain is a digital platform utilized to store and verify all the transaction history between users of the system. From a technical perspective, it is considered as "*a database of chronologically arranged packets of transactions known as blocks* ", against which a proposed transaction can be securely controlled against the integrity of a particular block (Kakavand, Kost De Sevres oath Chilton, 2017; Wright and De Filippi, 2015). It is a database consisting of blocks and questionable transactions that make blocks (Ünal and Uluyol, 2020:168).

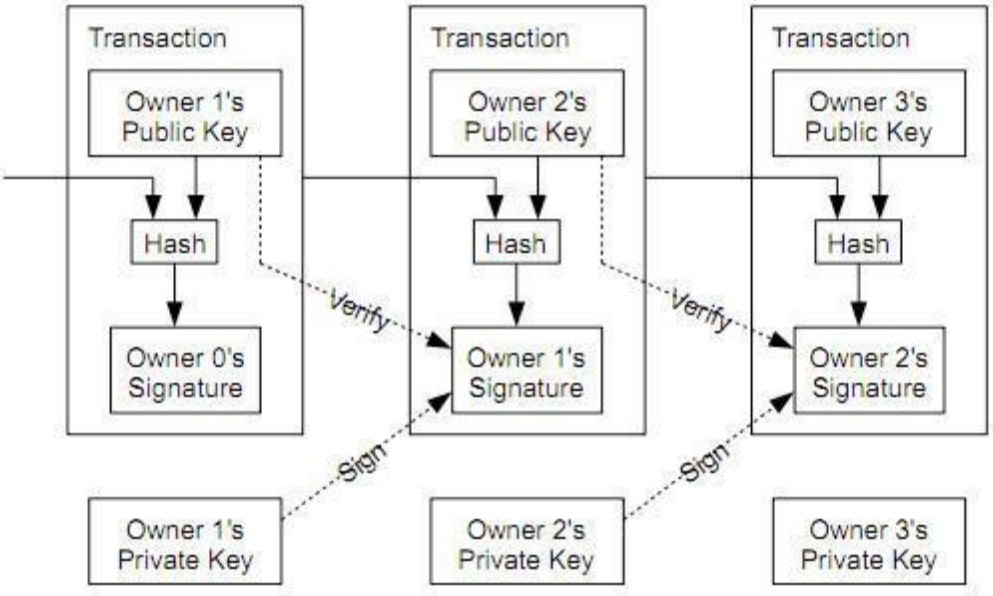
2.2.1. The Main Concept and Definition of Blockchain

Blockchain basically emerges as a specialized form of a connected list structure and can be expressed as a special connected list structure formed with hash-pointers (Ünsal and Kocaoğlu, 2018: 55). With the blockchain technology, the data is cryptographically signed and the blockchain acts as a decentralized record system where it can be stored in an agreed upon format. Blockchain is immutable and is extremely difficult for any information to change, especially if there is no network consensus (Dinh and Thai, 2018: 50). Each block has the information within itself, and this information must be linked to the previous block, which develops the chain and provides the custody. For example, by examining the blood, AI reveals what disease a person has and if this information is uploaded to the chain, other connected devices can also see the diseases that the person has. If other devices upload data from the system that analyzes blood, all devices can have the ability to use the system that examines blood. Blockchain provides transparency and accountability regarding when the user accesses their data and who accesses the data. This feature could give blockchain a huge advantage for the global notary system in the future. Additionally, blockchain stores personal and sensitive data even on diskless media, and databases have digitally signed data. Blockchain technology has the potential to seriously change today's societies and is thought to go beyond the traditional structure and contribute trillions of dollars to the global and national economy (Salah, Rehman , Nizamuddin & AlFuqaha , 2019; Önder, 2020).

2.2.2. Features of Blockchain

It has a database that is open and transparent to anyone using the blockchain, all transactions are recorded in the system, and since it is stored independently of each other by end computers within the central network structure, it can be resisted to issues arising due to central disruptions (Florea and Nitu: 2020: 67) and the accounts are numbered and numbers, and the transactions made from the accounts are seen transparently, but the owner of the transaction is not known. The use of cryptocurrencies as currency, means of money transfers and digital payment system are described as "Block-Chain 1.0". In addition, "Block-Chain 2.0" is defined as the realization of all financial transactions in the future, such as bonds, bills or loans, instead of simple money transfers. "Block-Chain 3.0" is defined as applications that can create added value in all fields such as government, health, culture, science and art, beyond financial markets and make life easier (Gediz Oral and Yeşilkaya, 2021: 216-217)

Figure 1: Blockchain Data Structure



Source: (Nakamoto, 2008: 6)

This figure shows the Block-Chain data structure and transactions are carried out by creating a new block by connecting the last link of the previous chain to the other chain, creating a new link, with the approval of the person who made the previous transaction. The first block was named 'Genesis Block'. All transactions that start with the Genesis Block are recorded in the databases of those who make transactions on the system. In case of a new transaction, all the transactions are also controlled (Gediz Oral and Yeşilkaya, 2021: 216-217). Blockchain has 3 main features (Murşan, 2023:15, Ramada, 2016; Biyan and Carda, 2021: 96-97):

1) Decentralized Distributed System:

Transactions can be made within the system without the authority of any institution or organization, and the information provided on the network is open to everyone.

2) Block Structure Immutability:

Transactions can be made within the system without the authority of any institution or organization, and the information provided on the network is open to everyone.

3) Being Safe:

Before making transactions in the blockchain, identity is checked and there are private keys that are subject to very strict conditions. Data is stored by nodes and decrypted only using private keys. Blockchain also incorporates multiple technologies and creates a comprehensive structure thanks to various applications. In a way, it can be thought of as a digitized decentralization.

3. Effects of Cryptocurrency Mining on the Environment

The cryptocurrency mining is the process that results in the production of cryptocurrencies and is carried out with the certain hardware. It is done with hardware with different features called CPU, GPU and FPGA. The selection of systems with the high transaction speed for the cryptocurrency production causes transactions to be completed faster. The miner software can start when there is a certain amount of cryptocurrency in the digital account. In the ASIC mining, the high-tech technical equipment is utilized. Mathematical problems integrated on blocks are calculated in a shorter time. Bitcoin and similar currencies produced with high calculation speed work and their production capacity are covered by ASIC mining. The most essential tool required for the GPU mining is the graphics card, and mining is completed in a faster way with high-capacity graphics cards (Aktas, 2022). The mining process may vary depending on each cryptocurrency, and the process may take longer depending on the algorithms used and the mining difficulty level of the cryptocurrency. The difficulty with the mining is the price of electricity and the price determines the profitability and incentives to involve or leave the mining market (Antonopoulos, 2017). Also, the effects of the cryptocurrency mining on the environment include the electricity consumed by the equipment, the heating of the equipment that contributes to the gradual warming of nature, the carbon footprint, the electronic waste and the gradual reduction in air quality.

3.1. The Effects of the Cryptocurrency Mining on Electricity Consumption

Energy costs are of the great importance in the cryptocurrency mining. Miners who complete the mathematical equation the fastest will have their transactions confirmed and receive a small reward in the form of Bitcoin payments. In the beginning, the mining process did not affect the amount of electricity in the states. But later, more people entered the mining business, and after large companies became involved in the mining business, this job became more difficult and caused extraordinary increases in electricity

expenses. Hundreds of thousands of computers are competing to solve the same problem, and only one of them is entitled to receive the Bitcoin fee by solving the problem, and the others do not receive any reward even though they spend energy. Most of the electricity used is wasted because 99.99% of all machines fail to win the race. It also takes a lot of time, for example more than 10 minutes per Bitcoin transaction (Rodect and Adams, 2023). It is thought that the 2023 average energy consumption of a Bitcoin transaction could be same as hundreds of thousands of VISA card transactions. Approximately 90 percent of the 21 million Bitcoins have been mined by mid-2021, and it is estimated that the last Bitcoin will be mined around 2140. As Bitcoin approaches supply limits, computational power also increases. The energy needed for mining is increasing. In 2021, Bitcoin increased over $60,000. This was partly due to China's attempt to block domestic crypto mining since May 2021 (Best, 2023). In May 2023, Bitcoin mining consumed approximately 95.58 terawatt-hours of electricity. A Bitcoin transaction required 1,449 kWh to finish, roughly the same amount of energy that the average US household consumes in 50 days. The average cost of a kilowatt-hour (kWh) in the US is 12 cents, resulting with about the $173 energy bill for one mining operation. Although the energy consumption per transaction was 703.25 kWh, Visa's energy consumption was 148.63 kWh. However, the energy consumption of cryptocurrencies cannot be predicted exactly. This is due to the decentralized structure of the nature of the cryptocurrency mining, the lack of the standardized recording, the existence of dynamic and continually growing mining, the diversity of energy resources and the fact that mining activities are private and secret (Kolesnikov, 2023).

Bitcoin is generally considered to be free from government control. This can be described as a valid thought in early days for the Bitcoin mining with a regular laptop. However, in days of massive mining companies, the Bitcoin mining requires plentiful sources of the cheap electricity. It is not possible for the Bitcoin mining to carry on without the plentiful electricity. Electricity supply is directed and managed by countries (Coppola, 2018). At first, states did not care about the energy consumed by mining because it did not change the level of equality and social and economic balance. However, in recent years, states have begun to react to mining. 75 percent of the mining takes place in China because of the closeness to hardware manufacturers and low electricity prices. China has put a ban on financial institutions from trading cryptocurrencies, and has tried to prevent the competition of other cryptocurrencies with its digital yuan project. the Tesla company stated that it would not accept decentralized virtual assets as a medium of payment and the severe environmental effects of the mining jeopardized the environmental sustainability (Alonso, Jorge-Vázquez, Fernández and Forradellas, 2021: 4). However, the cryptocurrency can be controlled indirectly and in a limited way. For instance, the use of traditional currencies by states is not completely free. Banks, credit card networks, and other intermediaries can control who can use their financial networks and what they can be used for. Bitcoin can be taken in a fast and easy way. An account can be opened at a Bitcoin exchange such as Coinbase. People send Bitcoin to

the digital wallet of the seller and have to wait for that transaction to be verified by the Bitcoin network. This process goes into maintaining the vast Bitcoin public ledger and is where most of the electrical energy is consumed. Miners from all over the world have competed to become the ones verifying transactions and entering them into the public ledger of the transactions. Successful miners are rewarded with newly produced Bitcoins. Bitcoin miners must purchase powerful computers and consume enormous amounts of energy to complete transactions quickly. Winners are rewarded with 6.25 freshly minted Bitcoins, worth approximately $50,000, which is estimated to confirm a standard "block" of Bitcoin transactions. Because of the high profits of this system, many people have started mining. Although it is extremely easy to record transactions in the ledger, "trusted" computers are required to do this. It is very difficult for unreliable actors to commit fraud because it requires them to have majority power. Mining cryptocurrencies thus transforms electricity into security, but these processes cause a large amount of energy waste (Huang, O'Neill and Tabuchi, 2021).

3.2. Effects of the Cryptocurrency Mining on Carbon Footprint

Global climate change is changing the temperature values of our planet. Some of these changes have occurred due to humans. The damages caused by humans to nature has filled the atmosphere with carbon dioxide and other heat-trapping gases. Increasing temperatures on Earth cause glaciers to melt, sea levels to rise, and destructive weather situations to increase. Climate change directs people's daily lives by affecting agriculture, energy use and public health. In addition, global warming will reduce productivity, cause mass migration, reveal security threats and negatively affect economic growth. The attention to cryptocurrencies in the last few years began to make the negative features of Bitcoin visible. The Bitcoin network consumes the high amount of electricity for mining. Many scientists claim that every year Bitcoin networks can produce approximately over 100 million tons of carbon dioxide (Othman and Dob, 2022:5-6). Carbon emissions constitute almost 75% of greenhouse gas emissions and cause the global temperature to increase by 1.5 °C. The issue of carbon emissions is at the center of the problem in determining the steps to be taken within the scope of combating climate change. Thus, economic sustainability has become a global priority in the last two years and has attracted the attention of environmental academics, policy makers and international organizations in various countries for decades (Khezri et al., 2022). It seems that a consensus has been reached that the first step to be taken to prevent CO2 emissions is to reduce fossil fuel use and energy consumption. The cryptocurrency mining, which has received increasing attention especially in recent years, requires a high amount of energy due to its production structure. For this reason, it has become one of the important areas of discussion on environmental issues such as carbon emissions. In the research conducted by Kohler and Pizzol (2019: 13598), Bitcoin networks spent 31.29 TWh with a carbon footprint of 17.29 MtCO2-eq. Additionally, Mora and colleagues (2018) expected that the processing for Bitcoin networks can cause the increase of a 2°C

in global temperatures by 2050. The increase in carbon footprint is not only related to the high amount of electricity consumed, but also from which sources the amount of electricity consumed is obtained. Electricity consumption in mining causes a high increase in carbon emissions. Carbon emissions per transaction was 162 kg CO2 at the end of 2017 and it increased to 545.03 kg CO2 in the middle of 2021. The electricity consumption per transaction for Bitcoin production was 1,147.43 kWh. For Ethereum, the electricity and carbon emissions per transaction in 2021 were 77.7 kWh and 36.91 kg CO2. On an annual basis, carbon emissions for the Bitcoin production was 52.66 Mt CO2. It is same as the overall of carbon emissions occurred in Sweden. The yearly electricity consumption for Bitcoin was 110.86 TWh, almost same as the energy consumption in the Netherlands (117.10 TWh) (Yılmaz and Kaplan, 2022:161). Compared to traditional online banking, one bitcoin are equal to the carbon footprint of 330,000 credit card transactions (Lindwall, 2022). Krause and Tolaymat (2018) state that mining activities for 4 cryptocurrencies (BTC, ETH, LTC and XMR) mined between 2016 and 2018 were liable for 3-15 million tons of carbon dioxide emissions.

3.3. Effects of the Cryptocurrency Mining on Electronic Waste

Damages to the environment as a result of human activities such as production and consumption went unnoticed for a while, thanks to nature's ability to renew itself. However, due to the quantitative and qualitative increase in environmental pollution over time, the environment could not recover and began to deteriorate. (Büyükkeklik, 2008:20). In recent years, waste generation has increased dramatically worldwide in recent years without any signal of slowing down in the future. By 2050, the global municipal solid waste production is estimated to escalate by approximately 70% to 3.4 billion metric tons. China is liable for the largest share of the universal municipal solid waste (over 15%), and the U.S. is the largest waste producer in terms of population. When considering "the special waste" (hazardous, e-waste, agricultural, industrial waste and etc.), the largest producer of municipal solid waste is the United States (Alves, 2023). More than 40 million tons of electronic waste is produced every year. But this is also a problem that predates Bitcoin, and Bitcoin only contributes to a small part of the problem (Bitcoin Magazine, 2021). Also, Bitcoin has started to produce e-waste at an alarming rate in recent years. Bitcoin's growing energy consumption raised serious doubts about the sustainability of the virtual currency. E-waste poses an increasing threat to the world, from heavy metals and toxic chemicals to water and air pollutions. Bitcoin's e-waste reached 30.7 metric kilotons per year on May 2021(Vries and Stoll, 2021). Electronic waste generally refers to discarded computer equipment and electronic items. According to the research, a single transaction on the Bitcoin network creates 272 grams of electronic waste (Young, 2021). The UN stated that e-waste was the world's fastest-increasing waste stream, expanding 21% between 2014 and 2019 to 53.6 million metric tons, of which below a fifth is recycled. As of May 2021, San Francisco produces some 30.7 metric kilotons of e-waste each year due to Bitcoin mining (The Economic Times,

2021). The Bitcoin network processed 112.5 million transactions in 2020 (compared to 539 billion transactions processed by traditional payment service providers in 2019), with each transaction generating "at least 272 grams of e-waste." This is equivalent to the weight of two iPhone 12 minis (Hern, 2021).

4. Activities to Prevent the Environmental Impacts of Mining Activities

Problems that had not yet emerged when cryptocurrencies first appeared began to emerge later. This is due to the late realization of the value of cryptocurrencies and the profits that can be obtained from them. However, people's excessive interest in the cryptocurrency mining has also brought environmental problems. Steps are being taken or planned to be taken by countries in different ways in order to reduce or eliminate the environmental impacts of the mining process, which refers to the production of crypto currencies. China and the United States are the places where the cryptocurrency mining is most concentrated. Cryptocurrency miners prefer places where electricity is cheap. However, China realized the risks posed by cryptocurrencies and ordered the closure of 26 mines in Sichuan, known as the second most intensive mining region in the country. Inner Mongolia and Quinhai provinces, which are sparsely populated but rich in coal or hydropower, have also ordered the closure of all cryptocurrency mines (Euronews, 2021). Due to the negative impact of the cryptocurrency mining on the environment, Iran issued regulations against the cryptocurrency mining, banned the cryptocurrency mining for four months, and announced that this activity draws more than 2 gigawatts of energy from the national electricity grid every day (BBC, 2022). Kosovo has faced the worst energy crisis in the last decade due to production cuts and has imposed a ban on the cryptocurrency mining in order to reduce electricity consumption. Faced with outages at coal-fired power plants and high import prices, authorities were forced to impose power cuts (Reuters, 2022).

There are various strategies that can be used to lessen the environmental effects of the Bitcoin mining. The most rational step that can be taken at this point is to follow a more technologically innovative approach and turn to crypto mining using renewable energy sources rather than fossil fuels. This will reduce dependence on fossil fuels and lessen greenhouse gas emissions. Another approach is to increase the efficiency of Bitcoin mining hardware. This would reduce the amount of energy required to verify transactions on the network and could also reduce the need for cooling systems. Also, Bitcoin mining could be used to support other environmental initiatives. For example, miners could be incentivized to plant trees or invest in renewable energy projects in exchange for rewards in Bitcoin or other digital assets (Bitget, 2023).

- So as to guarantee the endurance of the use of cryptocurrency, it is first necessary to change the type of energy source used. One of the solutions put forward to reduce the environmental effects of the cryptocurrency mining is to perform the cryptocurrency mining with renewable energy sources. Nearly a quarter of the cryptocurrency miners utilize water to power installations, and hydropower

accounts for 23.12 percent of the total energy used in the cryptocurrency mining. Wind is utilized to produce the power for 13.98 percent of the cryptocurrency mining, and nuclear and solar account for 7.94 percent and 4.98 percent of the total power respectively utilized in the cryptocurrency mining. Approximately 2.40 percent of the cryptocurrency mining uses other renewable energy sources. After all, nearly 52.4 percent of the cryptocurrency mining relies on the renewable energy for the power needs (Jafri, 2023). Renewable energy sources, unlike traditional energy sources, cannot be produced continuously. However, since the energy produced during periods of low consumption at night is often wasted, this excess energy can be stored and used by converting it into digital currency. Some Canadian companies have taken steps to transfer renewable energy into bitcoin mining operations. For example, Toronto-based Hut 8 Mining has a partnership with a local company to use surplus hydroelectric power. Bitfarms, a Canadian bitcoin mining company, mines its facilities using hydroelectric energy from nearby dams. Exxon mines bitcoins with excess energy from fossil fuels. Additionally, areas in need of heating, such as greenhouse areas, can benefit from Bitcoin mining as a low-cost heat source. For example, in Canada, a greenhouse owner used ASIC devices instead of heaters to provide greenhouse heat (Seyhan, 2023).

- In case of Bitcoin Mining activities, deterrent penalties are imposed, which may include financial penalties and, in some cases, imprisonment. For instance, people or companies that mine the illegal cryptocurrency in Hong Kong can be fined up to $500,000 or imprisoned for five years (Berman, 2019). However, due to the nature of the cryptocurrency mining, there is not enough data on where and how it is done. For this reason, mining activities can continue even if there are restrictions in these countries. The cryptocurrency mining ban is not the solution. Because it is difficult to understand that cryptocurrency mining is taking place, and people doing this secretly can cause greater damage to the environment. Instead of banning the cryptocurrency mining, companies that want to mine can be controlled by licensing. For instance, Iran had issued more than 1,000 crypto mining licenses across the country under past regulatory rules. Iranian authorities announced that nearly 6,914 illegal crypto mining farms were closed in May 2022 (Küçükel, 2022). In this way, by licensing cryptocurrency miners, countries know where, how much, how and with what equipment miners mine, and when necessary, they can cancel their licenses and stop mining activities. In addition, energy-saving minimum standards should be imposed on the hardware, equipment and cooling systems used in excavation work. In addition, the regulation of allocating environmental share from mining profits can have a positive effect, reducing the environmental impact, and investing in the environment can be made with the environmental share collected (Yavuz, 2023: 85-90).

Conclusion

Cryptocurrencies started to come to the fore in 2008. Cryptocurrency has been called digital or virtual currency and is difficult to control because it is included in the financial system independent of the monopoly of legal authorities. Cryptocurrencies are important on a global scale due to their very high market value and transaction volume. Crypto exchanges are not the only way to own cryptocurrency. It is also possible to earn money by mining cryptocurrency. Cryptocurrencies have attracted the attention of many people with their recent development in financial markets. In addition to being an investment and payment tool, this digital money has the opportunity to earn money through the cryptocurrency mining, which has enabled this virtual money to reach large masses. Today, 81% of energy consumption has been provided by fossil fuels. The cryptocurrency mining using energy obtained from fossil fuels has caused great harm to the environment. Since it is currently very difficult to prevent the cryptocurrency mining, the use of alternative energy sources can contribute to the environment. In addition, especially those who mine crypto money go to places where electrical energy is cheap and there is concentration in these places. Some states are disturbed by this situation and ban or restrict cryptocurrency mining (Yılmaz and Kaplan, 2022:167). Also, crypto investment scams and fake applications have become major problems in South Africa and the Asia-Pacific countries. In Europe, scammers have been found to threaten to reveal victims' browsing history on adult websites unless they provide a private key or send cryptocurrency (NDM News Network, 2023).

The cryptocurrency mining refers to the reward of high-capacity computers with new crypto money after producing crypto money or approving the money transfer and processing it in the common ledger. In particular, Bitcoin experienced a record rise in 2020, reaching 63 thousand dollars (BBC, 2021), and increased the interest in cryptocurrency mining. The interest in cryptocurrencies and the money earned from the mining in the early days have encouraged people for the cryptocurrency mining. Later, the difficulty of finding computer hardware, electricity consumption and its impact on the environment have caused the intense debate about the cryptocurrency mining. Especially since the cryptocurrency mining is done without any supervision and control mechanism, it is difficult to obtain data such as electricity consumed, carbon footprint and electronic waste. However, data obtained from researchers shows that the damage caused by cryptocurrencies to the environment is great. Certain ways can be tried to reduce the environmental impacts of the cryptocurrency mining. For example, a more technologically innovative approach can be followed and renewable energy sources can be used instead of fossil fuels. This reduces dependence on fossil fuels and causes greenhouse gas emissions to decrease. Additionally, the environmental damage can be reduced by increasing the efficiency of cryptocurrency miners' hardware. However, states can take precautions against the cryptocurrency mining, impose various restrictions, or the environmental damage caused by the cryptocurrency mining can be

eliminated with a special tax. Taxes collected can be used to protect the environment. It is necessary to regulate the cryptocurrency mining in order to reveal the scope and effects of the cryptocurrency mining and at the same time reduce its environmental impacts. Briefly, countries should reduce the negative effects of the cryptocurrency mining on the environment by taking steps to reduce negative environmental impacts, such as licensing the cryptocurrency mining, encouraging renewable energy, receiving an environmental share from mining revenues, and producing energy from the heat created by the mining process and hardware. Such measures taken by countries will reduce the negative effects of the cryptocurrency mining and make it easier to control the cryptocurrency mining.

REFERENCES

AKTAS, O. (2022, September 23). *Bitcoin ve Kripto Para Madenciliği Nedir? Nasıl Yapılır?* Retrieved from https://dosyahaber.com/post/bitcoin-ve-kripto-para-madenciligi-nedir-nasil-yapilir-1663901409

ALONSO, S. L., JORGE-VÁZQUEZ, J., FERNÁNDEZ, M. A., & FORRADELLAS, R. F. (2021). Cryptocurrency Mining from an Economic and Environmental Perspective. Analysis of the Most and Least Sustainable Countries. *Energies 14, no. 14: 4254.* , 1-22.

ALTAY, T., B. & SUMERLİ, S., S. (2020). Dünyada ve Türkiye'de Blok Zinciri Teknolojisi: Finans Sektörü, Dış Ticaret ve Vergisel Düzenlemeler Üzerine Genel Bir Değerlendirme . *Avrupa Bilim ve Teknoloji Dergisi-Ejosat Özel Sayı (ARACONF)*.

ALVES, B. (2023, August 31). *Global Waste Generation - Statistics & Facts.* Retrieved from https://www.statista.com/topics/4983/waste-generation-worldwide/#topicOverview

ANTONOPOULOS, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain.* O'Reilly Media.

AVRUPA MERKEZ BANKASI (2012). Virtual Currency Schemes. Retrieved from https://www.ecb.europa.eu /pub/pdf/ other/virtualcurrencyschemes201210en.pdf

BBC. (2021, April 19). *Kripto Para Madenciliğinin Avantajları Ve Riskleri Neler?* Retrieved from https://www.bbc.com/turkce/haberler-turkiye-56809480

BBC (2022, January 05). *Enerji krizindeki Kosova Kripto Para Madenciliğini Yasakladı*. Retrieved from https://www.bbc.com/turkce/haberler-dunya-59885200

BERENTSEN, A. (2019). Aleksander Berentsen Recommends "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto. B. Frey, & C. Schaltegger (Dü) içinde, *21st Century Economics.* Springer, Cham.

BERMAN, A. (2019, April 04). *Hong Kong: Illicit Crypto Mining Operations Are Punishable by Fine or Imprisonment*. Retrieved from https://cointelegraph.com/news/hong-kong-illicit-crypto-mining-operations-are-punishable-by-fine-or-imprisonment

BEST, d. R. (2023, May 09). *Energy Consumption of a Bitcoin (BTC) and VISA Transaction as of May 1, 2023*. Retrieved from https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/#statisticContainer

BINANCE ACADEMY. (2023, Nisan 13). What Is Cryptocurrency Mining and How Does It Work? Retrieved from https://academy.binance.com/en/articles/what-is-crypto-mining-and-how-does-it-work

BITCOIN MAGAZINE (2021, October 21). *How Bitcoin Mining is Solving Our E-Waste Crisis.* Retrieved from https://bitcoinmagazine.com/business/bitcoin-mining-solve-e-waste-crisis

BITGET. (2021, October 07). *Bitcoin Madenciliğinin Çevresel Etkileri*. Retrieved from https://www.bitget.com/tr/academy/the-environmental-impact-of-bitcoin-mining

BUNJAKO, F; TRAJKOVSKA, O. G.; KACARSKI, E. M. (2017). Cryptocurrencies–Advantages and Disadvantages. Retrieved from https://goo.gl/R9psS6

BÜYÜKKEKLİK, A. E. A. (2008). Sürdürülebilir Kalkınmanın Ekonomik Çevre Boyutları Açısından Atık Yönetimi ve E-Atıklar. *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 1*(2).

COPPOLA, F. (2018, May 30). *Bitcoin's Need For Electricity Is Its 'Achilles Heel'*. Retrieved from Forbes: https://www.forbes.com/sites/francescoppola/2018/05/30/bitcoins-need-for-electricity-is-its-achilles-heel/?sh=5f3ce7172fb1

ÇON, Ö. (2022). Kripto Varlıkların İcra Ve İflâs Kanunlarında Görünümüne Dair İsviçre Örneği . *Türkiye Adalet Akademisi Dergisi*(51), 229-258.

DAVID CHAUM PERSONAL WEBPAGE. (tarih yok). *Project Page:Digicash*. Retrieved from David Chaum Personal Webpage: https://www.chaum.com/ecash/

DEMARTINO, I. (2018). *Bitcoin Rehberi.* (K. Tekneci, Trans.) İstanbul: Epsilon Yayınevi.

DİLEK, Ş., & FURUNCU, Y. (2018). Bitcoin Mining and Its Environmental Effects. *İktisadi ve İdari Bilimler Dergisi, 33*(1).

DOĞAN, B., & HİLAL, E. (2021). Türkiye'de Kripto Paralar Üzerine Yapılan Akademik Çalışmalar. M. Atalay içinde, *Dijital Çağda İşletmeler ve Veriye Dayalı Uygulamalar* (s. 137-167). Ankara: İksad Publishing House.

ERTZ, M., & BOILY, É. (2019). The Rise of the Digital Economy: Thoughts On Blockchain Technology and Crypto Currencies for the Collaborative Economy. *International Journal of Innovation Studies, 3*(4), 84-93.

EURONEWS. (2021, June 21). *Çin'den Yerel Yönetimlere Kripto Para Madenciliğini Engelleme Emri: Tamamen Temizleyin.* Retrieved from https://tr.euronews.com/2021/06/21/cin-den-yerel-yonetimlere-kripto-para-madenciligini-engelleme-emri-tamamen-temizleyin

GEDİZ ORAL, B., & YEŞİLKAYA, Y. (2021). Kripto Para İkilemi: Karapara Aklama Ve Bitcoin. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* (39), 209-239.

GIUNGATO, P., RANA, R., TARABELLA, A., & TRICASE, C. (2017). Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. *Sustainability, 9*(12), 1-11.

GÜNAY, H. F.; KARGI, V. (2018). Kripto Paranın Vergilendirilmesi Fikrinin Mali Yönden Değerlendirilmesi. *Journal of Life Economics, 5*(3), 61-76.

HERN, A. (2021, September 17). *Waste From One Bitcoin Transaction 'Like Binning Two Iphones'*. Retrieved from https://www.theguardian.com/technology/2021/sep/17/waste-from-one-bitcoin-transaction-like-binning-two-iphones

HUANG, J., O'NEILL, C., & TABUCHI, H. (2021, September 03). *Bitcoin Uses More Electricity Than Many Countries. How Is That Possible?* Retrieved from New York Times: https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html

INTERNATIONAL ENERGY AGENCY. (2020). *World Energy Balances: Overview. International Energy Agency Statistics Report. .* Retrieved from https://www.iea.org/reports/world-energy-balances-overview

JAFRI, A. (2023, March 31). *More than 50% of Bitcoin Mining Uses Renewable Energy*. Retrieved from https://cryptoslate.com/more-than-50-of-bitcoin-mining-uses-renewable-energy/

KAKAVAND, H., KOST DE SEVRES, N., & CHILTON, B. (2017, Ocak 1). *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*. Retrieved from https://ssrn.com/abstract=2849251

KHEZRI, M., HESHMATI, A., & KHODAEI, M. (2022). Environmental Implications Of Economic Complexity And Its Role In Determining How Renewable Energies Affect CO2 Emissions. *Applied Energy, 306*.

KOLESNIKOV, N. (2023, August 30). *60+ Bitcoin Mining and Energy Consumption Statistics For 2023 You Need to Know*. Retrieved from https://www.techopedia.com/bitcoin-mining-and-energy-statistics#:~:text=The%20energy%20consumption%20of%20a,while%20Visa's%20consumed%20148.63%20kWh.

KÖHLER, S., & PIZZOL, M. (2019). Life Cycle Assessment of Bitcoin Mining. *Environmental science & technology, 53*(23), 13598-13606.

KRAUSE, M. J., & TOLAYMAT, T. (2018). Quantification Of Energy And Carbon Costs For Mining Cryptocurrencies. *Nature Sustainability, 1*(11), 711-718.

KÜÇÜKEL, V. (2022, September 05). *İran'da Yeni Düzenleme: Kripto Madencilerine Lisans Veriliyor!* Retrieved from https://paratic.com/iranda-yeni-duzenleme-kripto-madencilerine-lisans-veriliyor/

LINDWALL, C. (2022, February 03). *Crypto Has a Climate Problem.* Retrieved from https://www.nrdc.org/stories/crypto-has-climate-problem

MARC, A. (2014, January 21). *Why Bitcoins Matters*. Retrieved from New York Times: http://dealbook.nytimes.com/2014/01/21/why-Bitcoin-matters

MORA, C., ROLLINS, R. L., TALADAY, K., KANTAR, M. B., CHOCK, M. K., SHIMADA, M., & FRANKLIN, E. C. (2018). Bitcoin Emissions Alone Could Push Global Warming Above 2 C. *Nature Climate Change, 8*(11), 931-933.

NAKAMOTO, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* 03 17, 2023 tarihinde https://bitcoin.org/bitcoin.pdf adresinden alındı

NDM News Network. (2023, February 10). *Kaspersky Reveals 49% of Cryptocurrency Users Experienced Cryptocurrency Crime.* Retrieved from https://digitalterminal.in/trending/kaspersky-reveals-49-of-cryptocurrency-users-experienced-cryptocurrency-crime

OTHMAN, A., & Dob, A. B. (2022). *Bitcoin Mining's Energy Consumption and Global Carbon Dioxide Emissions: Wavelet Coherence Analysis.* Arab Monetary Fund .

ÖDEME VE MENKUL KIYMET MUTABAKAT SİSTEMLERİ, ÖDEME HİZMETLERİ VE ELEKTRONİK PARA KURULUŞLARI HAKKINDA KANUN. (2013, Haziran 20). Resmi Gazete: 27.06.2013-28690, Sayı: 6493.

ÖNDER, M. (2020). Yapay Zekâ: Kavramsal Çerçeve. (İ. Demir, & M. Önder, Dü) *Yapay Zeka Stratejileri ve Türkiye. ULİSA 12*.

PETERS, G. W., PANAYI, E., & CHAPELLE, A. (2015). Kripto Para Birimleri Ve Blok Zinciri Teknolojilerindeki Eğilimler: Parasal Bir Teori Ve Düzenleme Perspektifi. *Mali Perspektifler Dergisi, 3*(3).

REUTERS. (2022, January 05). *Kosovo Bans Cryptocurrency Mining To Save Electricity*. Retrieved from https://www.reuters.com/markets/commodities/kosovo-bans-cryptocurrency-mining-save-electricity-2022-01-04/

RODECT, D., & ADAMS, M. (2023, May 23). *Understanding Blockchain Technology*. Retrieved from Forbes: https://www.forbes.com/advisor/investing/cryptocurrency/what-is-blockchain/

RODRIGUES, F. (2021, Ekim 31). *Bitcoin White Paper Turns 13 Years Old: The Journey So Far*. Retrieved from Cointelegraph Web Sitesi: https://cointelegraph.com/news/bitcoin-white-paper-turns-13-years-old-the-journey-so-far

SALAH, K.; REHMAN, M. H. U.; NIZAMUDDIN, N. & ALFUQAHA, A. (2019). Blockchain for AI: Review And Open Research Challenges. *IEEE* , 10127– 10149.

SEYHAN, A. (2023, May 07). *Bitcoin Madenciliği: Yenilenebilir Enerji Kaynaklarının Değerlendirilmesi ve Enerji Verimliliğinin Artırılması*. Retrieved from https://ahmetseyhan.medium.com/bitcoin-madencili%C4%9Fi-yenilenebilir-enerji-kaynaklar%C4%B1n%C4%B1n-de%C4%9Ferlendirilmesi-ve-enerji-verimlili%C4%9Finin-6672fcc21a18

TAŞ, O., & KIANI, F. (2018). Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme. *Bilişim Teknolojileri Dergisi, 11*(4), 370-372.

THE ECONOMIC TIMES. (2021, September 21). *Bitcoin Mining Generates Tonnes of e-Waste: Study.* Retrieved from https://economictimes.indiatimes.com/markets/cryptocurrency/bitcoin-mining-generates-tonnes-of-e-waste-study/articleshow/86391133.cms

TÜRKİYE BİLİŞİM DERNEĞİ. (2020). *Türkiye'de Yapay Zekânın Gelişimi için Görüş ve Öneriler.* Retrieved from https://www.tbd.org.tr/pdf/yapay-zeka-raporu.pdf

ÜNAL, G., & ULUYOL, Ç. (2020). Blok Zinciri Teknolojisi. *Bilişim Teknolojileri Dergisi, 13*(2).

ÜNSAL, E., & KOCAOĞLU, Ö. (2018). Blok Zinciri Teknolojisi: Kullanım Alanları, Açık Noktaları ve Gelecek Beklentileri. *Avrupa Bilim ve Teknoloji Dergisi*(13), 54-64.

VRIES, A. D., & STOLL, C. (2021). Bitcoin's Growing E-Waste Problem. *Resources, Conservation and Recycling, 175*.

WHITE, L. H. (2015). The Market for Cryptocurrencies. *Cato Journal, 35*(2), 383-402.

WRIGHT, A., & DE FILIPPI, P. (2015, Mart 10). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*. doi:http://dx.doi.org/10.2139/ssrn.2580664

YAVUZ, İ. (2023). Kripto Para Madenciliğinin Çevre Üzerindeki Etkisi (Yayımlanmamış Yüksek Lisans Tezi). *T.C. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü*. İzmir.

YILMAZ, M. K., & KAPLAN, A. (2022). Kriptopara Madenciliğinin Çevresel Sürdürülebilirlik Üzerine Etkileri. In C. Korkut, & M. Bulut (Eds.), *Döngüsel Ekonomi ve Sürdürülebilir Hayat* (pp. 143-174). Türkiye Bilimler Akademisi Yayınları.

YOUNG, M. (2021, September 15). *Bitcoin'in Yıllık Enerji Tüketimi, 2020 Yılını Şimdiden Geride Bıraktı.* Retrieved from https://tr.cointelegraph.com/news/2021-s-btc-energy-use-passes-2020-s-new-study-suggests-each-tx-produces-272g-of-e-waste

Cybersecurity for Small and Medium-Sized Businesses

Oliver A. LUUKKONEN[*], Yeşim ÜLGEN SÖNMEZ[**]

Abstract

Cybersecurity is all the devices and software applications that protect computers, networks, software, critical systems, and data from possible digital threats. The organizations have a responsibility to secure data to maintain customer trust and ensure regulatory compliance. They use cybersecurity measures and tools to protect sensitive data from unauthorized access, as well as prevent disruption to business operations due to unwanted network activity, and implement cybersecurity by streamlining digital defense across employees, processes, and technologies. Small and medium-sized businesses (SMBs) which make up a large portion of organizations, contribute greatly to the economies of many countries. However, SMBs tend to not care enough about cyber security or do not have the resources to implement it. Additionally, cybersecurity research rarely focuses on SMBs. SMBs have extensively switched to remote/hybrid working due to the global pandemic COVID-19 and this transition to remote/hybrid working methods had to adopt new digital strategies and technologies very quickly. This situation has led to the emergence of more cyber risks and cyber-attacks. This study highlights that it is crucial to strengthen SMBs and future preparedness against cybersecurity threats. Specifically, in this study, cyber security problems and deficiencies in SMBs are identified and suggestions are offered to eliminate them. Also, the work has shown the importance of why the countries should give importance to SMB cybersecurity as well as the defense industry and future studies should focus more on SMB cybersecurity applications.

Keywords: *Medium Businesses, Small Businesses, SMBs Cybersecurity, SMB Cyber-attacks, SMB Defense Techniques*

1. Introduction

Daily life that moved to the internet, has introduced many new words into our lives such as *Cybernetics*, *Cyber*, and *Cyberspace* and the transfer of crimes to the internet created the terms *Cyber Crimes* and *Cyber Security*. Cybersecurity is

Original Research Article
Received: 28.07.2023
Accepted: 15.11.2023
[*] MA Student, Department of Computer Science, Sam Houston State University, Huntsville, USA. E-mail: oal006@shsu.edu ORCID https://orcid.org/0009-0009-1384-4118
[**] Dr., Department of Software Engineering, Faculty of Technology, Fırat University, Elazığ, TÜRKİYE. E-mail: phdyus@gmail.com ORCID https://orcid.org/0000-0002-2090-0263

defined as things that are done to protect a person, organization, country and their computer information against crime or attacks carried out using the internet ('Cambridge Dictionary', 2023; Eş & Serdar, 2021).

Cybersecurity is all devices and software applications that protect computers, networks, software, critical systems, and data from possible digital threats. The fact that businesses use technologies such as the internet, intranet, and extranet and that many of their employees carry out internet-connected transactions has made businesses the target of electronic attacks but they have a responsibility to secure data to maintain customer trust and ensure regulatory compliance (Chidukwani, Zander, & Koutsakis, 2022; Eş & Serdar, 2021; Levy & Gafni, 2022).

They use cybersecurity measures and tools to protect sensitive data from unauthorized access, as well as prevent disruption to business operations due to unwanted network activity, and implement cybersecurity by streamlining digital defense across employees, processes, and technologies (Levy & Gafni, 2022).

Small and medium-sized businesses (SMBs) which make up a large portion of organizations, contribute greatly to the economies of many countries. However, SMBs do not care enough about cyber security or do not implement it. Additionally, cybersecurity research also rarely focuses on SMBs. SMBs have switched to remote/hybrid working due to the global pandemic COVID-19 and this transition to remote/hybrid working methods had to adopt new digital strategies and technologies very quickly (İyem & Danyal, 2021; Levy & Gafni, 2022). This situation has led to the emergence of more cyber risks and cyber-attacks.

Small and Medium-Sized Businesses (SMBs) are important for economic development in most countries, especially in the Western world, as they represent the majority of businesses (Levy & Gafni, 2022; Zec, 2015). Gafni and Pavel stated that SMBs, a term generally used in the United States (USA), are known as Small and Medium Enterprises (SMEs) in Europe (Gafni & Pavel, 2019). Sizes vary between countries. Different regions have their definitions of "small or medium" and are usually measured by the number of employees. For example, the European Commission (2022) stated that organizations with less than 250 employees are considered SMEs. While organizations with fewer than 500 employees are considered SMBs in the United States ('U.S. Small Business Administration', 2023), other countries account for SMBs as organizations with fewer than 500 employees.

Throughout the world, SMBs are a huge part of the growing global economy (Paulsen, 2016). It constitutes 90% of the global economy and more than 50% of employment worldwide (Chidukwani et al., 2022). They generate a significant portion of a country's overall national income (GDP) along with creating new jobs that stimulate a country's economic growth ('World Bank SME Finance: Development news, research, data | World Bank', 2023). According to estimates, 600 million jobs will be needed by 2030 to accommodate the growing global workforce, making the development of SMBs a high priority for many governments around the world. Most formal jobs in emerging markets are created by SMBs, which create 7 out of 10 jobs ('World Bank SME Finance: Development news, research, data | World Bank', 2023).

Therefore, in terms of both economy and security, SMBs need to have strong cyber security while taking advantage of all the opportunities offered by today's multi-channel digital world. Many SMBs have had to adopt new digital strategies and technologies very quickly to maintain, stabilize, or diversify their business activities and models during the global pandemic and the rise of remote/hybrid working methods. This situation has led to the emergence of additional cyber risks (Eaves, 2023; Levy & Gafni, 2022).

Two main external threat vectors faced by SMBs stand out; Phishing and Social Engineering in the Supply Chain ecosystem ('Ponemon Institute', 2018). When combined with internal threat vectors including lack of risk assessment, poor access control, data, device and password protection, low levels of investment, inadequate training and awareness, and cyber hygiene culture and skills, this creates a potentially very broad attack surface.

Precautions that SMBs should take against cyber-attacks can be listed as follows;

- All data regarding the company's sellers, customers, and sales should be recorded. In short, a list of all information and assets about the company should be created.
- Many security breaches are caused by outdated software, including security software, web browsers, and operating systems. Therefore, it is of great importance to update all technological tools.
- Regardless of the size of the company, it is necessary to have a backup system. It is necessary to back up old information and switch to an automatic backup system. The backup system will make SMBs feel safe against ransomware attacks, which they frequently encounter.

- It is of great importance for SMBs to inform their employees about e-mail fraud incidents. You need to be careful with unusual connections.
- You need to have an action plan ready against hackers. What to do and the methods to be followed in case of any data breach should be determined.
- SMBs need to use complex passwords for the system they use. Additionally, even if a unique password is used, passwords should be updated frequently.
- It is possible to protect against ransomware, albeit partially, thanks to antivirus programs. Therefore, your antivirus program must be running.
- To fully ensure information security, consultancy services on information security should be obtained. There is a need for a security service provider to step in in case of any threat. Here, attention should be paid to the solution tools and service quality of the service provider. In addition, safety standards and compliance with certificates should be checked.

According to research, 80% of SMBs accept IT security as a priority issue, and 50% of them do not have an IT security expert. It was revealed that 30% of them spent less than 1000 USD on IT security in a year.

With the increasing use of e-commerce and evolving technology, one would think it would be almost a given in this day and age that businesses would be making sure they are secure from constant cyber threats. That is not always the case. While large-sized businesses have the luxury of large budgets to dedicate to cybersecurity and manpower, SMBs are not that fortunate because of the inherent challenges that they face, such as limited resources and manning. These challenges can become a hindrance to an SMB's overall cybersecurity. SMBs' limited budget, lack of manpower, and even lack of knowledge of cybersecurity leave them open to attacks (Sill, 2023). Due to these challenges and SMB's high impact on a given economy, they are consistently targeted by cybercriminals and deemed easy targets. With their limitations, SMBs must maximize their limited resources as best they can. Allowing for a large budget dedicated to cybersecurity manpower, the latest cybersecurity technology, and training is just a pipe dream in most SMBs. Even some recommendations for SMBs are not very cost-effective. Fortunately, there are a significant number of resources and recommendations available to SMBs that are perfect for their meager budgets. Utilizing these cost-effective resources and recommendations will allow SMBs to increase their

cybersecurity awareness, training, and security all while spending little to nothing.

This study highlights that it is crucial to strengthen change and future preparedness against the cybersecurity threat. It reveals the cyber threat landscape for SMBs, and why this is so significant challenge faced. In This study, cybersecurity studies in SMBs are examined. Cyber security problems and deficiencies in SMBs are identified and suggestions are offered to eliminate them. The last finding in our study is that the countries should attach importance to SMB cybersecurity as well as the defense industry and future studies should focus more on SMB cybersecurity applications.

2. Literature Study and Background

Nine new-generation technologies that have entered our lives with Industry 4.0. These technologies consist of simulation, autonomous robots, horizontal and vertical system integration, cyber security, Internet of Things (IoT), additive manufacturing, cloud technology, big data analysis, and augmented reality (Demir, Sarıışık, & Öğütlü, 2022). While researching the design principles of Industry 4.0, they tried to determine the usage potential of some of the new generation technologies mentioned above during the implementation of Industry 4.0. Transactions carried out by SMBs have increased digitally over the internet network with the Industry 4.0 process. Invoicing, payment of taxes, etc. carried out by businesses. Along with many different transactions, digital commerce constitutes the most important of these topics. Digital commerce, which constitutes one of the important applications of digitalization, has significantly increased its importance all over the world, especially during the "2020 Global Pandemic" period. In fact, digitalization applications that have been used in the trade of goods and services for many years have been used in the supply chain and marketing stages (Demir et al., 2022).

This research was conducted on what possible threats, issues, recommendations, and even recommended hardware solutions were sought by previous studies to achieve a better overall potential solution for SMBs. Research Reviews were conducted to better understand previous findings on cybersecurity in SMBs (Levy & Gafni, 2022). This study covers a wide spectrum across different industries and cybersecurity threats/vulnerabilities concerning SMBs to complete a better overall picture rather than just focusing on a specific area. This allows for a more complete solution that would cover most aspects.

2.1. General SMB Cybersecurity

In (Paulsen, 2016), Paulsen researched explained how SMBs are targeted by cybercriminals with little repercussions while also potentially using SMBs as a stepping stone to get access to larger businesses and organizations which could cause even more significant damage to economies. Paulsen gives some general ideas on items that SMBs should take into consideration on how to secure their business. The ideas stated are that cybersecurity checklists are geared more towards actual risk profiles rather than the implementation of the security controls in the checklists, SMBs should conduct a business process analysis to determine critical business resources/processes instead of just hiring security professionals to plug the vulnerabilities. The aim is creating a cybersecurity culture within the SMB through proper training, reinforcement of the training, and ensuring that the right people are hired (Paulsen, 2016).

2.2. SMB Cybersecurity Management Policies

To see about a more technical aspect, (Teymourlouei & Harris, 2019) gave recommendations and techniques such as

- Understanding the level of cybersecurity knowledge of the business,
- Properly training employees,
- Using VPN connections,
- Antivirus software,
- Utilizing possible cloud-based security solutions.

The other recommendations are

- Using proper password management (complex passwords, password expiration, etc.),
- Conducting backups,
- Using utilize encryption for data at rest,
- Securing Wi-Fi networks,
- Utilizing firewalls,
- Enforcing least-privilege.

It even specified utilizing specific software for encryption (VeraCrypt) and VPN (Windscribe) along with introducing a business questionnaire (Chidukwani et al., 2022; 'Ponemon Institute', 2018; Teymourlouei & Harris, 2019).

2.3. SMB Cybersecurity Management

Alahmari and Duncan dealt heavily with cybersecurity risk management using a review procedure that identified cybersecurity risk perspectives for SMBs based on keyword searches among academic databases (Alahmari & Duncan, 2020). The findings on the cybersecurity risk perspectives were threats underestimated by not utilizing proper security and created high-value targets due to weak defense (SMB Threats). Training, behaviour, and commitment played significant roles in security and safety (SMB behaviour), lack of SMB security practices and engagement with research community (SMB Practices), lack of cybersecurity attacks and associated consequences (SMB Awareness), and lack of experts and professionals in executive manager decisions (SMB Decision-Making) (Alahmari & Duncan, 2020).

2.4. Manufacturing SMB Cybersecurity

Heikkila et al. presented cybersecurity in more specialized manufacturing SMBs (Heikkila, Rattya, Pieska, & Jamsa, 2016). They researched discussed cybersecurity risks associated with manufacturing SMBs along with possible solutions for those SMBs. The research discussed ideas like Enterprise Resource Planning (ERP) implementation for SMBs. The biggest cyber-defense limits in SMBs are budget and security awareness. It is costly and complex and it is seen as a risk. The proper and constant training is important role in manufacturing SMBs. Intellectual property theft is a big concern, for manufacturing SMBs that causes too much emphasis being placed on information protection rather than manufacturing process and life cycle security. Manufacturing technology complexity equals higher risk, and SMBs should make use of free material to help security management due to lack of resources and budget (Heikkila et al., 2016).

2.5. Current Cyber Hygiene of SMBs

Manufacturing SMBs showed similar risks with general SMBs which led to research into the next area of current cyber hygiene amongst SMBs. Ncubukezi et al. discussed how cybercrimes have affected SMBs current cyber hygiene (Ncubukezi, Mwansa, & Rocaries, 2020). They found that cyber hygiene varied amongst SMBs with a general lack of standards/guidelines causing bad cyber hygiene along with results showing current security practices and recommendations for good cyber hygiene. The results showed that 93% of malware incidents had antivirus/antispyware software installed, but unsure if they were updated, 83% of SMBs did not dedicated personnel to remind or run device updates, 100% of SMBs relied on passwords for protection that did not

meet criteria, and cybersecurity risk assessment/analysis was not prioritized with employees relying on their knowledge. The recommendations for SMBs were to include proper cybersecurity awareness programs, training, adherence to security measures, and implementing proper security measures (Ncubukezi et al., 2020). Understanding the cybersecurity hygiene of SMBs can allow for an increase in providing suitable solutions.

2.6. Evolution of Cybersecurity Issues in SMBs

With the knowledge gained on the current look of cyber hygiene in SMBs, research focused on the evolution of cybersecurity issues in SMBs. Bhattacharya discussed how changes in information technology have led to an evolution of cybersecurity issues in SMBs in which SMBs tend to fail to evolve with the issues which leave them open for increasing attacks (Bhattacharya, 2015). Bhattacharya presented SMBs constantly fail to put in place proper security policies due to a lack of resources (skills, infrastructure, security assessments, etc.) Information technology evolution has caused SMBs to become more dependent on outsourcing (expertise, cloud computing, etc.). In addition, relying on mobile/portable devices that increase cybersecurity risks, and taking a proactive approach in dealing with evolving cybersecurity threats must include cost-effective, practical, and realistic approaches, which work with the limitations of SMBs (Bhattacharya, 2015).

2.7. Future Proof in SMBs

With the evolution of information technology causing issues with SMBs, research was conducted on possible ways to future-proof cybersecurity in SMBs. Elezaj et al. researched which gave insight on one aspect of future-proofing SMBs (Elezaj, Yayılgan, Abomhara, Yeng, & Ahmed, 2019). They covered Intrusion Detection Systems (IDSs) for SMBs as an important tool for network attacks where an IDS framework consisting of signature-based anomaly detection was utilized to improve the efficiency of detecting network anomalies for SMBs. The research found that challenges facing SMBs regarding IDSs were that there were no IDS public datasets, a gap between intrusion detection results and interpretation, and no self-adaptation. The study further found that utilizing a hybrid IDS (signature-based with anomaly-based) achieved an overall accuracy of 99.9872%. This hybrid IDS checked signature matches first, then tested input on a classifier model and balance to training the model that finally is fed back into the signature database for updating (Elezaj, Yayilgan, Abomhara, Yeng & Ahmed, 2019). This would allow for the self-adaptation of IDSs and protection against possible future

network threats. The biggest concern with utilizing self-adapting IDS is the complexity and cost over regular signature-based IDSs.

2.8. Cyber Attack Impacts on SMBs

Saleem et al. (Saleem, Abedisi, Ande, & Hammoudeh, 2017) presented cybersecurity issues, attack trends, and the effects on SMBs with an emphasis on non-technical individuals. They laid out the cost of attacks, trending threats/challenges, mitigation, and penetration testing value. It stated that attacks like ransomware or the evolution in technology such as cloud and IoT have made it increasingly difficult and costly for SMBs to keep up due to a lack of awareness and emerging threats of IoT device attacks like Mirai are generally caused by a lack of security within the IoT devices. It also provided recommendations in which enterprises should adhere to four security standards (update device software/firmware, encrypt communications/data transfer, strong password policy, and incorporate multi-factor authentication) at a minimum, and conduct regular penetration testing into the SMBs security procedures (Elezaj et al., 2019).

3. Proposed Research and Contributions

While ISO/IEC 27001, COBIT, and NIST have well-laid out standards for cybersecurity frameworks, these are all geared to corporate level-large scale entities in which some of the standards do not fit into SMB concept or there are some others that are more valuable to SMB rather than larger businesses. Moreover, some of the specific standards require extensive workload and/or costs that the SMBs cannot cover. That is why here we base our structure on the common cybersecurity elements that are better fit for SMBs. Specifically, this work proposes to utilize an existing training platform for SMB employees and cost-effective solution to test and patch the system for vulnerabilities.

3.1. SMB Cybersecurity Awareness and Training

Based on the research conducted on cybersecurity in SMBs, indicated that cybersecurity training and awareness were big concerns with SMBs and gave recommendations that proper cybersecurity awareness and training needs to be conducted (Paulsen, 2016; Teymourlouei & Harris, 2019; Elezaj et al., 2019). The greatest issue that SMBs have with conducting proper cybersecurity awareness and training is how to go about it with a limited budget and lack of expertise.

The best solution for SMBs would be to utilize the free and openly available resources online. This is the best cost-effective and time-reducing method for

SMBs. There is no reason that they should re-invent the wheel per se. One of those resources to SMBs for cybersecurity awareness and training is the Department of Defense (DoD) ('Cybersecurity', 2023; Levy & Gafni, 2022) Cyber Exchange Public website (Levy & Gafni, 2022; 'Security Technical Implementation Guides – DoD Cyber Exchange', 2023), This website has numerous free cybersecurity training and awareness modules available to the public. All the modules are self-paced and can be completed usually within an hour, depending on the course. One such course is the Cyber Awareness Challenge training module, which is actually an annual requirement for all DoD personnel to take. It can help give a basic understanding of cybersecurity and increase awareness. These courses can be utilized to satisfy the need for cybersecurity training, awareness, and reoccurring training at SMBs without the need to produce a separate cybersecurity training and awareness program, and with the added bonus of being free.

3.2. Cost-Effective SMB Cybersecurity

Another common concern amongst SMBs found in the literature study was the lack of antivirus/antimalware, firewall, application whitelisting, and encryption software to protect the SMB computers or systems (Teymourlouei & Harris, 2019; Heikkila et al., 2016; Ncubukezi et al., 2020; Saleem et al., 2017). This is a very simple cost-effective solution for SMBs to overcome. This gives SMBs security for antivirus/antimalware, firewall for network protection, and encryption for data at rest, application whitelisting, and code integrity all included with the cost of the OS. While IDSs are valuable assets, utilizing something such as a self-adaptive IDS could be too complex and costly for normal SMBs which leads me to recommend not going the route of hybrid IDSs, but instead sticking with standard signature-based IDSs.

3.3. Securing SMB Computers

The SMB computer's OSs would have to be hardened, firewall setup, and BitLocker to be enabled. This can be a very time-consuming effort where most SMBs would have to hire a dedicated cybersecurity expert to ensure their systems are secure. Most SMBs do not have the time or monetary resources dedicated to handling that, however, there is a very easy cost-effective way to handle it. SMBs can make use of two free applications provided by DoD to secure computers and help with a previous concern in (Paulsen, 2016) that cybersecurity checklists do not show how to implement security controls in checklists. The two free publicly available applications by DoD are Security Content Automation Protocol (SCAP)

and SCAP Compliance Checker (SCC). The applications utilize Defense Information Systems Agency (DISA) created Security Technical Implementation Guides (STIGS) to harden and secure systems ('Security Technical Implementation Guides – DoD Cyber Exchange', 2023). he SCC application is a vulnerability/compliance checker with preloaded STIG benchmarks used to conduct a scan on the computer. While the SCAP application is a Java app used to take the results for the SCC scan and conduct manual STIG checks which were missed by the SCC benchmarks. SCAP can also be used to view STIGs and each of their security requirements. Utilizing SCC and SCAP with the DISA produced STIGs, numerous OSs, applications, and various software can be secured all for no cost to the SMBs.

4. Results and Discussion

SCC and SCAP scans were conducted on a Virtual Machine (VM) loaded with just a plain Enterprise version of Windows 10 (LTSC). The results were recorded to demonstrate on all the security vulnerabilities found with a normal Windows 10 load that would be used by SMBs. Fig. 1 shows how a STIG requirement is displayed in SCAP. The STIG requirement not only discusses why it is recommended, but also how to check for the security requirement, fix action if it is not enabled, and technical references. The SCC application was run with the following Windows 10 benchmarks checked, IE 11 STIG, MS Dot Net Framework STIG, Windows 10 STIG, Windows Defender Antivirus STIG, and Windows Firewall STIG. Fig. 2 shows the SCC application upon start up and Fig 3 shows the results of the SCC application scan.

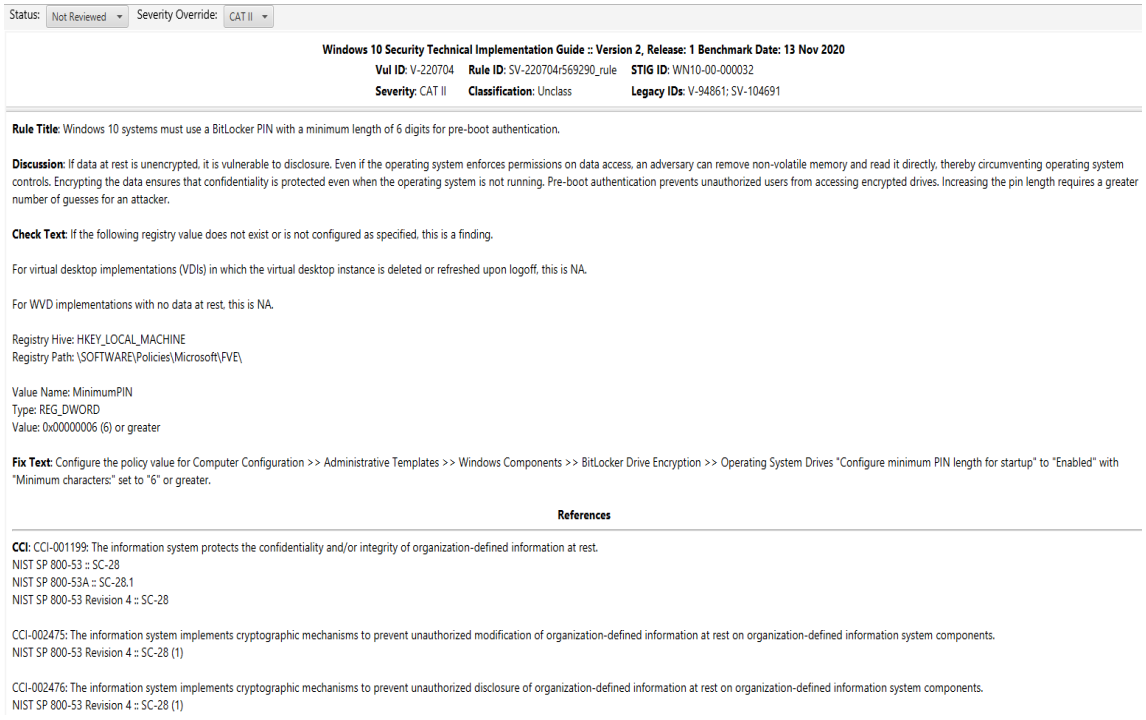


Fig. 1. STIG Security Requirement Displayed in SCAP

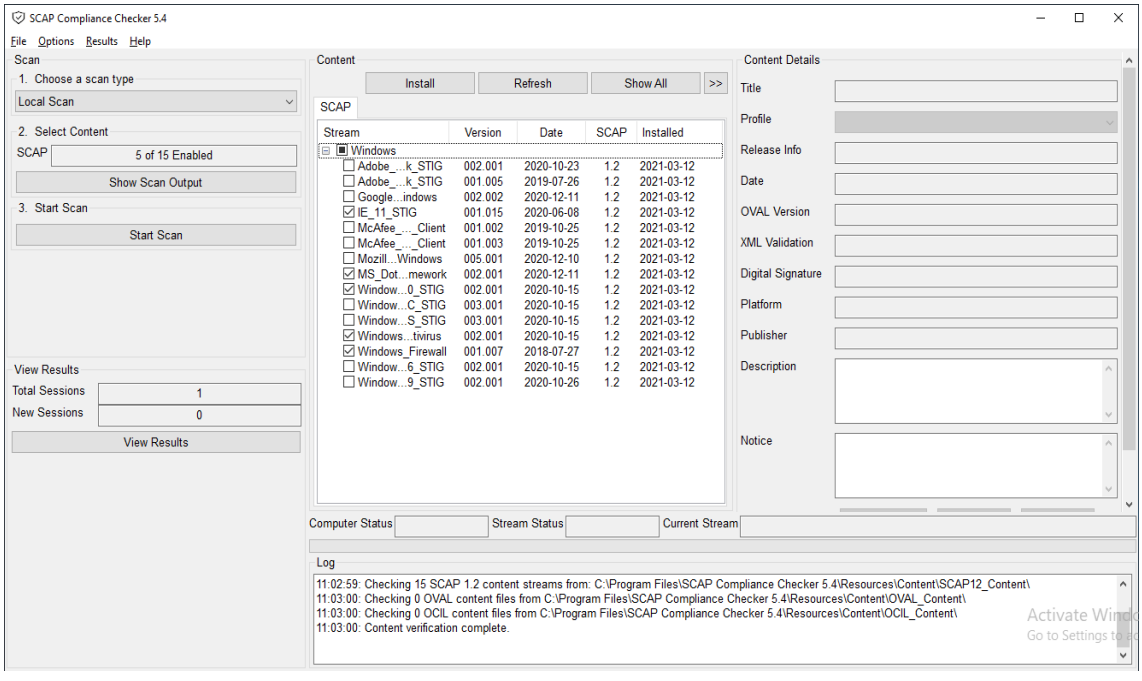
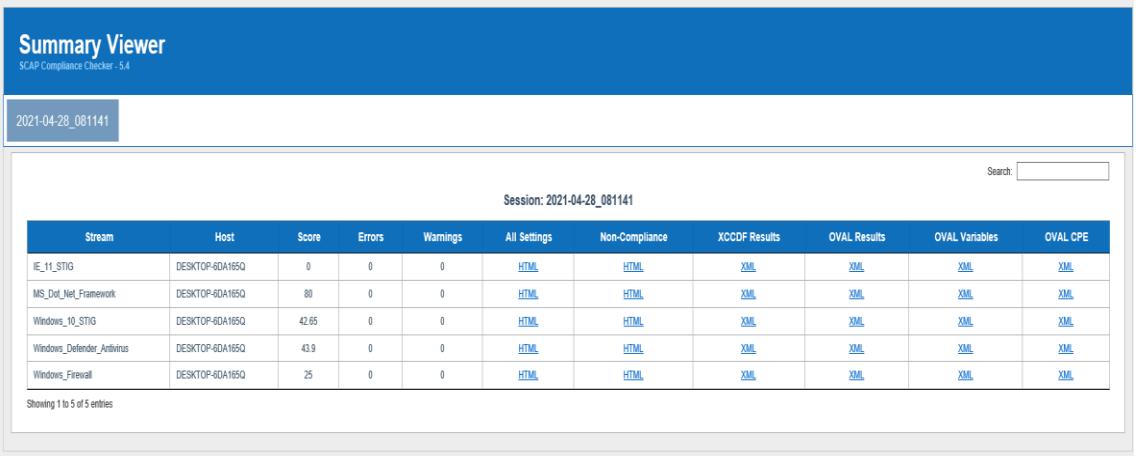


Fig. 2. Starting Stage of SCC Application



Summary Viewer

SCAP Compliance Checker - 5.4

2021-04-28_081141

Search:

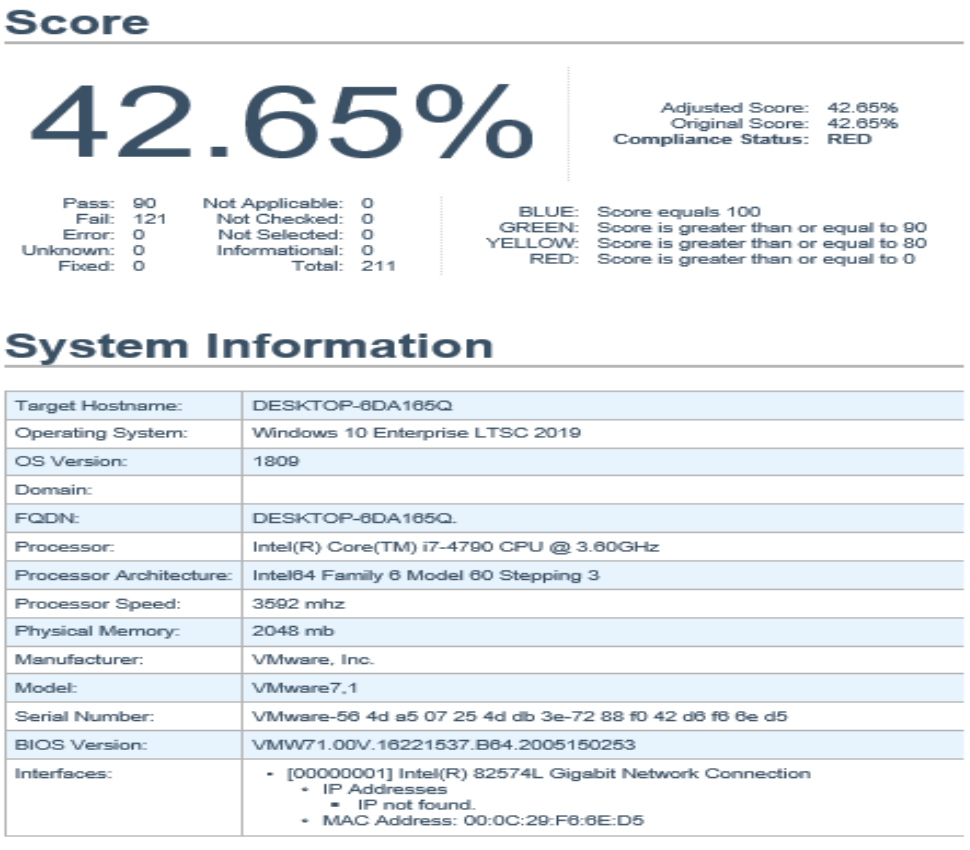
Session: 2021-04-28_081141

Stream	Host	Score	Errors	Warnings	All Settings	Non-Compliance	XCCDF Results	OVAL Results	OVAL Variables	OVAL CPE
IE_11_STIG	DESKTOP-6DA165Q	0	0	0	HTML	HTML	XML	XML	XML	XML
MS_Dot_Net_Framework	DESKTOP-6DA165Q	80	0	0	HTML	HTML	XML	XML	XML	XML
Windows_10_STIG	DESKTOP-6DA165Q	42.65	0	0	HTML	HTML	XML	XML	XML	XML
Windows_Defender_Antivirus	DESKTOP-6DA165Q	43.9	0	0	HTML	HTML	XML	XML	XML	XML
Windows_Firewall	DESKTOP-6DA165Q	25	0	0	HTML	HTML	XML	XML	XML	XML

Showing 1 to 5 of 5 entries

Fig. 3. SCC Scan Results on the SMB Computer

The SCC application scans showed a score of 0% for IE 11, 80% for MS Dot Net Framework, 42.65% for Windows 10, 43.9% for Windows Defender Antivirus, and 25% for Windows Firewall. The higher the score, the more score the area is. As can be seen, a basic Windows 10 system is not very secure. Each individual section can be viewed independently in either HTML or XML. Fig 4 shows a small clip of the breakdown from the Windows 10 section.



Score

42.65%

Adjusted Score: 42.65%
Original Score: 42.65%
Compliance Status: RED

Pass: 90
Fail: 121
Error: 0
Unknown: 0
Fixed: 0

Not Applicable: 0
Not Checked: 0
Not Selected: 0
Informational: 0
Total: 211

BLUE: Score equals 100
GREEN: Score is greater than or equal to 90
YELLOW: Score is greater than or equal to 80
RED: Score is greater than or equal to 0

System Information

Target Hostname:	DESKTOP-6DA165Q
Operating System:	Windows 10 Enterprise LTSC 2019
OS Version:	1809
Domain:	
FQDN:	DESKTOP-6DA165Q.
Processor:	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz
Processor Architecture:	Intel64 Family 6 Model 60 Stepping 3
Processor Speed:	3592 mhz
Physical Memory:	2048 mb
Manufacturer:	VMware, Inc.
Model:	VMware7,1
Serial Number:	VMware-56 4d a5 07 25 4d db 3e-72 88 f0 42 d6 f6 6e d5
BIOS Version:	VMW71.00V.16221537.B64.2005150253

Interfaces:	- [00000001] Intel(R) 82574L Gigabit Network Connection
	  - IP Addresses
	  - IP not found.
	  - MAC Address: 00:0C:29:F6:6E:D5

Fig.4. SCC Scan Results on Windows 10

The SCC application automatically saves the results in various formats that can be imported into various applications, such as OVAL for OpenSCAP (OSCAP) and XCCDF for SCAP. The results are time-stamped based on the date/time format and saved under the user's profile in Windows. To get the most accurate results for the SCAP application, the following STIGs were downloaded and imported into the SCAP application, MS Dot Net Framework V2R1, MS IE11 V1R19, MS Windows 10 V2R1, MS Windows Defender Antivirus V2R1, and Windows Firewall V1R7. Using the SCC application results, the saved XCCDF XML files can now be imported into the SCAP application for manual STIG checks. The SCAP application is a Java-based application that requires the latest version of JRE to be installed to run the application. Fig 5 shows the SCAP application upon start up and Fig 6 shows the results of the imported SCC application scans.

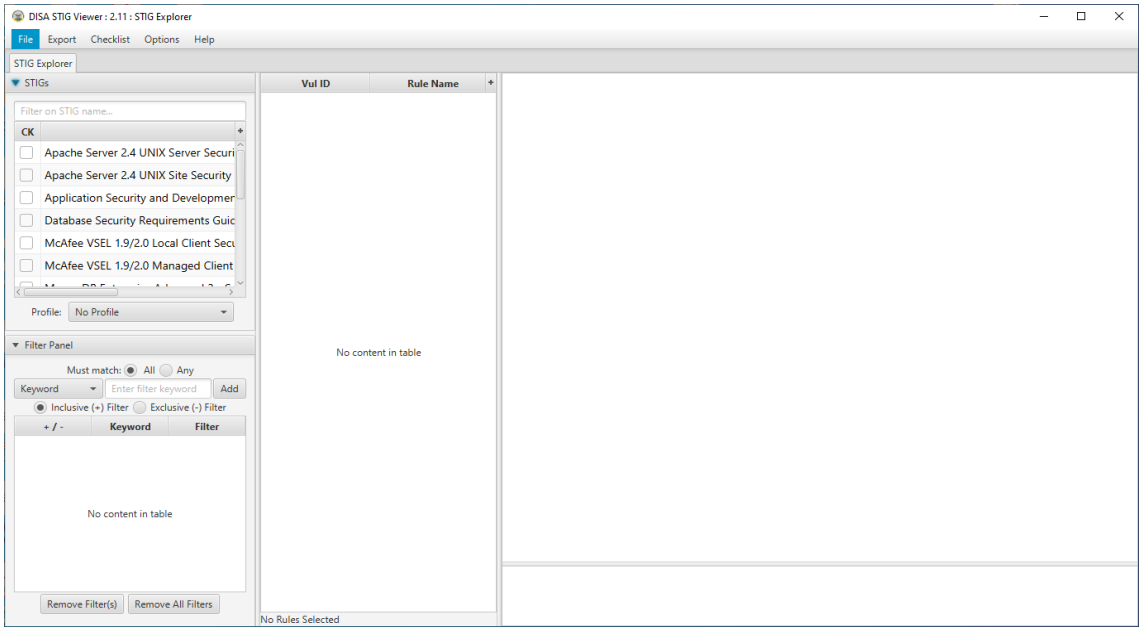


Fig. 5. SCAP Application upon Start-up

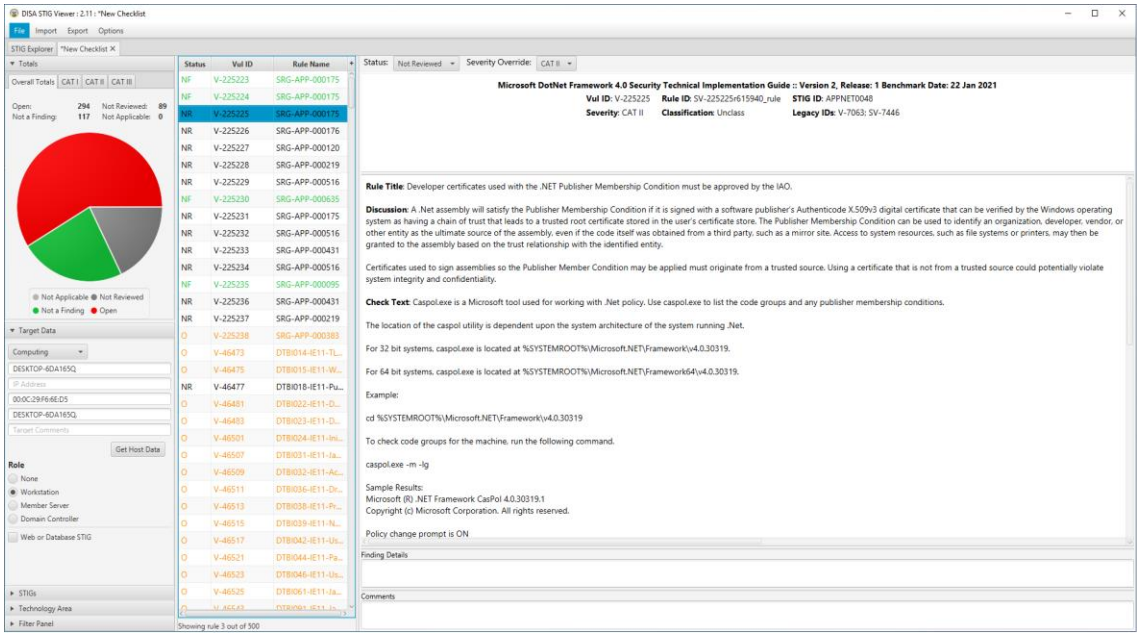


Fig. 6. SCAP Results Obtained from Windows 10 Test Computer

Once the results were loaded and a checklist created, the SCAP application showed a total of 500 findings which 294 were "Open", 117 were "Not a Finding", 89 were "Not Reviewed", and 0 were Not Applicable. Each STIG requirement can be then viewed individually and further assessments can be done to determine fix actions, further guidance, or determination if it is applicable at all.

5. Conclusions and Future Work

SMBs have special requirements that require special considerations to meet their specific needs. Using cost-effective methods that do not hinder their resources (time, manning, and revenue) is the best solution possible instead of relying on the generally accepted cybersecurity standards offered by ISO, NIST, etc. By using free openly available training along with applications designed by the DoD, such as SCC and SCAP, SMBs can ensure that they are as protected as they possibly can be. The items shown are readily available to all and should be utilized as a part of overarching cybersecurity defense.

There will always be a need to find better approaches to securing SMBs. The ones provided offer the bonus of being maintained and updated constantly by the DoD and DISA. This ensures that the latest STIGs and applications are the most up-to-date to better assist SMBs in securing themselves as effectively as possible.

Although the proposed work proved to be effective for a Windows 10 local machine-based SMB, it is also important to note that with sophisticated

Advanced Persistent Threats capabilities and increasing zero-day attacks, the SMB will need to be always on alert for such threats and continue with the regular updates on the systems, training of the employees, and checking other standardizations to enhance the security of such systems. In the near future, we plan to extend this work to other server capabilities and Bring Your Own Device platforms used in SMBs. Also, focusing on a specific SMB type can help the company to create a better-customized security mechanism.

Acknowledgment

The authors of this paper extend their appreciation to Dr. Cihan VAROL for his contribution.

REFERENCES

ALAHMARI, A. & DUNCAN, B. (2020). Cybersecurity risk management in small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. In *Int. Conf. on Cyber Situational Awareness, Data Analytics and Assessment* (pp. 1–5). Retrieved from https://doi.org/10.1109/CyberSA49311.2020.9139638

BHATTACHARYA, D. (2015). Evolution of cybersecurity issues in small businesses, Technology. In *4th Annual Conference on Research in Information* (p. 11). Chicago, Illinois, USA. Retrieved from https://doi.org/10.1145/2808062.280806

CAMBRIDGE DICTIONARY. (2023). Retrieved 7 October 2023, from https://dictionary.cambridge.org/tr/

CHIDUKWANI, A., ZANDER, S., & KOUTSAKIS, P. (2022). A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, 10(August), 85701–85719. Retrieved from https://doi.org/10.1109/ACCESS.2022.3197899

CYBERSECURITY. (2023). Retrieved 8 October 2023, from https://business.defense.gov/Work-with-us/Cybersecurity/

DEMİR, S., SARIIŞIK, G., & ÖĞÜTLÜ, A. S. (2022). KOBİ lerin Endüstri 4.0 Farkındalık ve Olgunluk Seviyesinin Belirlenmesi: Şanlıurfa İli Örneği (Determination of Industry 4.0 Awareness and Maturity Level of SMEs: The Example of Şanlıurfa Province). *Journal of Business Research - Turk*, 14(4), 2938–2955. Retrieved from https://doi.org/10.20491/isarder.2022.1543

EAVES, S. (2023). Security for Small and Medium-Sized Businesses | IoT Security Podcast | PSA Certified. Retrieved 7 October 2023, from https://www.psacertified.org/blog/iot-security-for-small-medium-businesses-podcast/

ELEZAJ, O., YAYILGAN, S. Y., ABOMHARA, M., YENG, P., & AHMED, J. (2019). Data-Driven Intrusion Detection System for Small and Medium Enterprises. In *IEEE 24th Int. Workshop on Computer Aided Modeling and Design of Communication Links and Networks* (pp. 1–7). Limassol, Cyprus. Retrieved from https://doi.org/10.1109/CAMAD.2019.8858166.

EŞ, A., & SERDAR, N. (2021). SİBER Saldirilara Karşı Kobilerin Farkındalık Düzeylerini Incelenmesi: Ankara Ili Örneği. *Journal of Duzce University Institute of Social Sciences*, 11(1), 133–151.

GAFNI, R., & PAVEL, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*, 7(1), 14–26.

HEIKKILA, M., RATTYA, A., PIESKA, A. S., & JANSA, J. (2016). Security Challenges in Small- and Medium-Sized Manufacturing Enterprises. In *Int. Symp. On Small-scale Intelligent Manufacturing Systems* (pp. 25–30). Narvik, Norway. Retrieved from https://doi.org/10.1109/SIMS.2016.7802895

IYEM, C., & DANYAL, Y. (2021). Teknoloji Geliştirme Bölgelerinde COVID-19 Pandemisi Üzerine Nitel Bir Araştırma: KOBİ'lerde Dayanıklılığı Artırmak İçin Acil Durum ve İş Sürekliliği. *Ekonomik ve Sosyal Boyutlarıyla PANDEMİ*, 89–162.

LEVY, Y., & GAFNI, R. (2022). Towards the quantification of cybersecurity footprint for SMBs using the CMMC 2.0. *Online Journal of Applied Knowledge Management*, 10(1), 43–61. Retrieved from https://doi.org/10.36965/ojakm.2022.10(1)43-61

NCUBUKEZI, T., MWANSA, L., & ROCARIES, F. (2020). A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses, In *15th Int. Conf. for Internet Technology and Secured Transactions* (pp. 1–6). London, United Kingdom. Retrieved from doi: 10.23919/ICITST51030.2020.9351339

PAULSEN, C. (2016). Cyber Securing Small Businesses. *Computer*, 49(8), 92–97. Retrieved from https://doi.org/10.1109/MC.2016.223

PONEMON INSTITUTE. (2018). Retrieved from Https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

SALEEM, J., ABEDISI, B., ANDE, R., & HAMMOUDEH, M. (2017). A state of the art survey – Impact of cyber-attacks on SME's. In *Int. Conf. on Future Networks and Distributed Systems '17* (pp. 1–7). Cambridge, United Kingdom. Retrieved from https://doi.org/10.1145/3102304.3109812.

SECURITY TECHNICAL IMPLEMENTATION GUIDES – DoD CYBER EXCHANGE. (2023). Retrieved 8 October 2023, from https://public.cyber.mil

TEYMOURLOUEI, H. & HARRIS, V. E. (2019). Effective methods to monitor IT infrastructure security for small business. In *Computational Science and Computational Intelligence* (pp. 7–13). Las Vegas, NV, USA. Retrieved from

https://doi.org/10.1109/CSCI49370.2019.00009

U.S. SMALL BUSINESS ADMINISTRATION (2023). Retrieved 7 October 2023, from https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threatsVerizon

WORLD BANK SME FINANCE: Development news, research, data | World Bank. (2023). Retrieved 6 October 2023, from https://www.worldbank.org/en/topic/smefinance

ZEC, M. (2015). Cyber security Measures in SMEs: a study of IT professionals' organizational cyber security awareness. *Linnaeus University, Kalmar. Zugriff Unter Http://Www …*, 1–99. Retrieved from https://www.diva-portal.org/smash/get/diva2:849211/ATTACHMENT01.pdf