Cybersecurity Risk Management Plan for a Blockchain Application Model

Gabriel Kabanda
Africa Leadership and Management Academy

Abstract

The substantive increase in the use of internet-based technologies has subjected organizations to malicious attacks. Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. A blockchain is a data structure, which stores transactional records in the form of a block chained and stored in several databases, and is fundamentally a digital ledger of transactions (DLT) that upon duplication is distributed on the blockchain throughout the entire computer network. To improve on cybersecurity, machine learning is considered for data mining among the data. This research is purposed to determine a cybsersecurity risk management plan, develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities, ascertain how the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the financial services sector. The research used the Pragmatism paradigm, which is a philosophy that is closely linked to the Mixed Method Research (MMR). The Focus Group comprised a total of 100 participants from the Masters students attending the Applied Business Informatics module taught by the author at the University of Zimbabwe in 2020. An Online survey method was also used for the quantitative approach where 10 participants were involved. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the General deterrence theory (GDT) were used to formulate the Cybersecurity strategy. Blockchain cyber vulnerabilities were determined. A model structure for block chain technology and cryptocurrency was developed and an explanation provided on how the framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to financial services sector.

Key Words: Cybersecurity; Artificial Intelligence; Machine Learning; Cyber Risk; Blockchain Technology; Cryptocurrency; Bitcoins; Pragmatism paradigm.

Cybersecurity Risk Management Plan for a Blockchain Application Model

Background

Cybersecurity is the practice of protecting systems, networks, and programs from digital (malicious) attacks. Cyberattacks can potentially target access, change or destroy sensitive information; can be used to extort money from people; or disrupt normal business operations. Cybersecurity is the policy framework and technologies purposed to protect the confidentiality,

assurance, and availability of computing resources from attack (Berman, D.S., et al, 2019). Idebdou, N. (2015) also states that cyber security entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption. The currrent trends in Cybersecurity in 2021 includes the following:

- Phishing and Social Engineering (Phishing is the practice of sending fraudulent emails that resemble emails from reputable sources.)
- Ransonware (Ransomware is a type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid.)
- Internet of Things (IoT) Susceptibility (The Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction)
- Cloud Vulnerability and Cloud Security (Microsoft Azure, Google Cloud Platform (GCP), Amazon (AWS)).
- Third-party vulnerabilities
- Internal attacks
- Data Rights Compliance

Sensors, analyzers and a user interface constitute a network intrusion detection and prevention system, as shown on Figure 1 below, depicted as Intrusion Detection System (IDS) components.

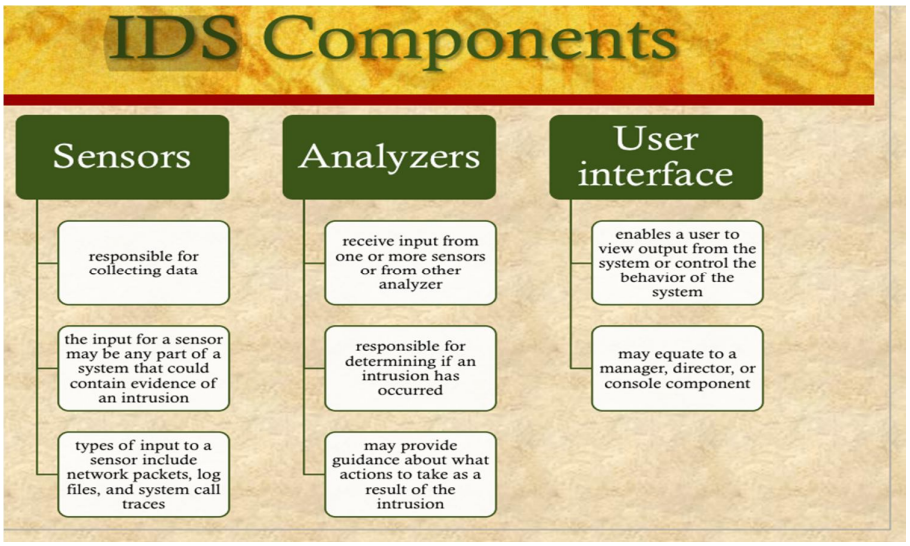


Figure 1: The IDS Components (Source: Stallings, W.(2015))

New technologies often come with new security concerns. According to Bringas, P.B., and Santos, I. (2010), research in network anomaly detection has applied several well-known Artificial Intelligence paradigms to address the security concerns. ***"Cybersecurity Risk Management"*** means policy frameworks and technologies that thwart risks in computer networks, applications and data in a networked environment and its associated assurance.

The common types of attacks in using the Internet of Things (IoT) identified by Elmamy, S.B. (2020) are tabulated below on Table 1. A denial of service (DoS) attack renders a system inaccessible by its legitimate users.

Table 1: *Layer-based attacks in IIoT systems* (Source: Elmamy, S.B. (2020))

Layer	Attacks	Description
Application	Injection	Untrusted data that is sent to an interpreter or database
	Brute force	An attempt to guess a password via sending various passwords
	Malware	A malicious code can attack mail and web services
Middleware	Flooding	Repeating the request of a new connection until the IIoT system reaches maximum level.
	De-synchronization	Disruption of an existing connection
Network	DoS	Attempt to stop or reduce activity of an IIoT
	MIM	Violating data confidentiality or integrity during transfer
	HELLO flood	Uses HELLO packets as weapon to launch the attack on IIoT system
	Sybil	A single node duplicates its node to be in multiple locations
Perception	Eavesdropping	Deducing data sent by IIoT devices across network
	RFID tracking	Modifying a content of a tag or trying to disable it
	Jamming	Creating radio interference and exhaustion on IIoT devices

One of the latest IT solutions that require information security risk management (ISRM) and considered not only as an innovative technology, but as a potential revolution in the business is

Blockchain. Risk analysis includes processes such as identification of activity, threat analysis, vulnerability analysis and guarantees. One of the completed phases in information security risk assessment process is risk analysis.

A blockchain is a datastructure, which stores transactional records in the form a block chained and stored in several databases, and is is fundamentally a digital ledger of transactions (DLT) that upon duplication is distributed on the blockchain throughout the entire computer network. Blockchain is a type of DLT where a hash is used to record the transactions with an immutable cryptographic signature. A group of transactions constitute a block, and a record of every transaction is appended to every participant's ledger. The basic process of Blockchain is shown on Figure 2 below.

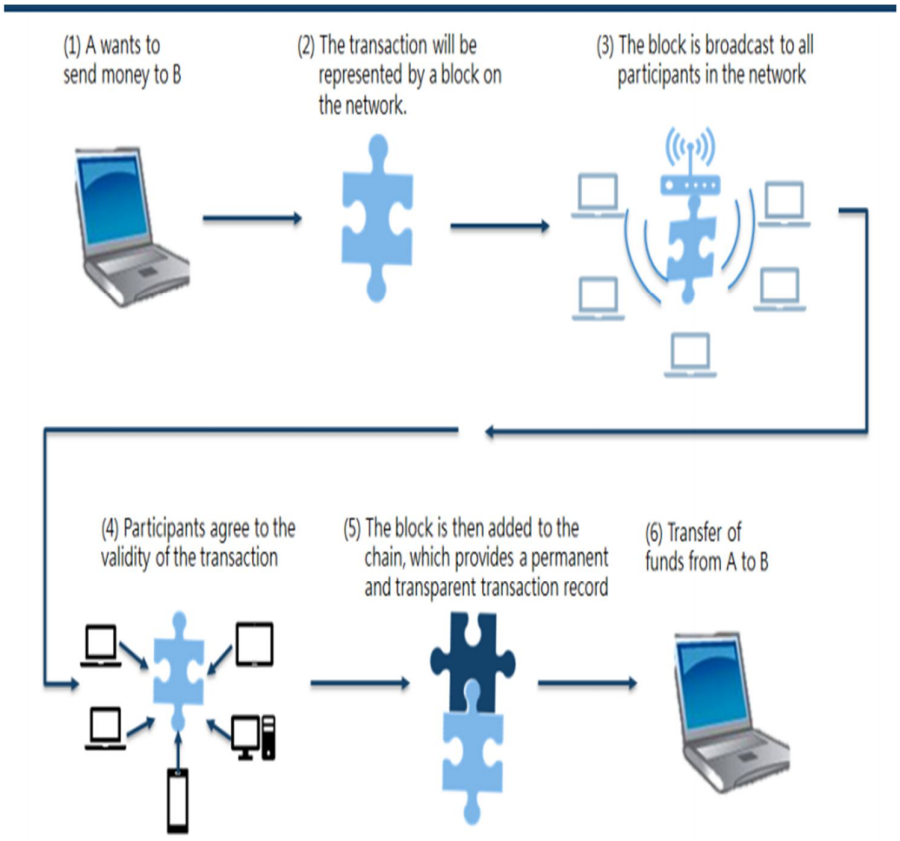


Figure 2: Basic Process of Blockchain

A cryptocurrency is a digital currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Many cryptocurrencies are decentralized networks based on blockchain technology. The purpose is to enable micro-transactions at a very low cost (Nowinski,

W., and Kozma, M., 2017). One of the most commonly used application of blockchain technology is Cryptocurrency.

The National Institute of Standards and Technology (NIST) emphasizes that blockchain technology:

- Groups the signed transactions according to a certain cryptographic pattern into blocks that form a ledger.
- Secures the ledger by a cryptographic link to each block and its validated previous entry.
- Automatically manages conflicts using established rules.
- Duplicates the ledger copies across the entire network.

Blockchain mainly relies on three concepts which are:

i. Peer-to-peer network
ii. Distributed Consensus
iii. Public-key Cryptography.

The basic benefits of using Blockchain Technology include the following:

- Time savings
- Cost savings
- Tighter security
- Enhanced privacy
- Improved auditability
- Increased operational efficiency

Artificial Intelligence (AI) is about computer systems that simulate human intelligence processes, including learning, reasoning, and self-correction. AI works with the help of Artificial Neurons (Artificial Neural Network) and scientific theorems (If-Then Statements, Logics). The special ability of AI is to reach a solution based on facts rather than on a preset series of steps, and this is what most closely resembles the thinking function of the human brain. AI is characterised by the ability to simulate human behavior and cognitive processes, capture and preserve human expertise, obtain fast response, and manage huge volumes of data quickly. On the contrary, human intelligence is about intuition, judgement, common sense, creativity, beliefs, effective communication, plausible reasoning and critical thinking.

Machine Learning (ML) is the enabling process of computers to learn. ML is regarded as a scientific discipline concerned with the design and development of algorithms that allow machines to mimic human intelligence. Artificial Neural Networks (ANNs) are the ML algorithms inspired by the central nervous system, where computers are programmed to teach themselves from data as opposed

to instruction to perform specific tasks. ML can handle data mining among the data. Truong, T.C., et al (2020) classified ML into three classes:

1. Supervised learning
2. Unsupervised learning, and
3. Reinforcement learning.

The roadmap for building a Machine Learning System is shown on Figure 3 below.

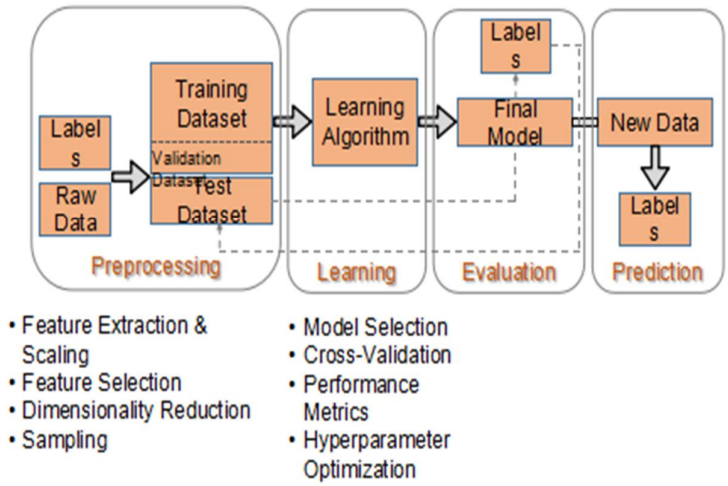


Figure 3: Roadmap for Building Machine Learning Systems

Statement of the Problem

The substantive increase in the use of internet-based technologies has subjected organizations to malicious attacks. A blockchain is a datastructure, which stores transactional records in the form a block chained and stored in several databases, and is fundamentally a digital ledger of transactions (DLT) that upon duplication is distributed on the blockchain throughout the entire computer network. To improve on Cybersecurity, ML is considered in order to do data mining among the data.

There is need for proactive security measures against cyber attacks, and in particular a cybsersecurity risk management plan which leads to the development of a Blockchain Technology Application Model that manages cyber risks. It is of primordial importanve to ascertain how the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the Financial Services sector.

Research Objectives

The major objectives of this research were to:

a) Determine the cybersecurity risk management plan that incorporates Machine Learning (ML) algorithms.
b) Develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities.
c) Ascertain how the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the Financial Services sector.

Research Questions

The key research questions were as follows:

a) What is the proactive cybersecurity risk management plan that incorporates Machine Learning algorithms?
b) How do you develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities?
c) How does the Framework of Blockchain Technology and Cryptocurrency address cyber rsisks and creates value for the Financial Services sector?

Literature Review

According to National Institute of Standards and Technology (NIST) (NIST, 2018), the NIST Cybersecurity framework is purposed to reduce cyber risk and improve security to the critical infrastructure. The NIST Cybersecurity Framework shown on Figure 4 provides organizations with a mechanism to:

1. depict the current cybersecurity state
2. represent describe the proper cybersecurity condition
3. identify and prioritize improvement opportunities
4. progressively move towards the desired cybersecurity state
5. communicate the cybersecurity risk with all the key stakeholders.

The NIST framework (NIST, 2018) comprises five elements which are purposed to identify, protect, detect, respond and recover the network in the unlikely event of a cyber-attack, as shown below on Figure 4.

Figure 4: NIST Cybersecurity Framework Core components. (Source: NIST, 2018))

The General Deterrence Theory advocates the use of strong deterrents and penalties to dissuade people from doing malpractices and perpetrating cyber-attacks (Schuessler, D.L., 2009). The four main elements of the General Deterrence Theory are illustrated in Figure 5 below (Alanezi, A.A., 2014). The whole interaction process among the attacker and the protecting agent can be presented as a Game theory approach that could serve as a balancing and strategizing tool for predicting the behavior of the attacker and based on the solution to that game, to find an equilibrium point for optimal results.

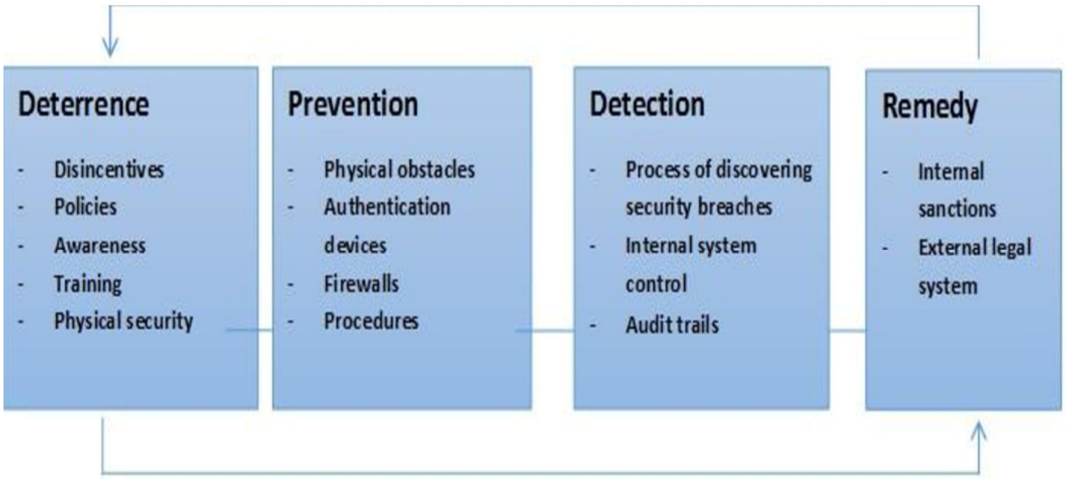


Figure 5: Elements of the General Deterrence Theory (GDT) (Source: Alanezi, A.A., 2014))

Cryptography encrypts the information into an unreadable, referred to as cipher text, in order to protect the information. The recipient, who possesses a secret key, is the only one who can decipher it into plain text. Data is valuable and needs to be protected. Cryptographic algorithms can be classified in various ways, but the major focus is on the number of keys that are employed for encryption and decryption, and by their use. The three types of algorithms that are commonly used are (Kessler, J.B., and Hunt, A., 2019), https://www.garykessler.net/library/crypto.html):

1. *Secret Key Cryptography (SKC):* Primarily used for privacy and confidentiality, uses a single key commonly referred to as the **symmetric encryption**.
2. *Public Key Cryptography (PKC):* Uses one key for encryption and another for decryption; also called **asymmetric encryption,** and this primarily used for authentication, non-repudiation, and key exchange.
3. *Hash Functions:* These are primarily used for message integrity and uses a mathematical transformation to irreversibly "encrypt" information using a digital fingerprint.

The training phase in NIDS is represented by Figure 6 below, which shows the importance of the algorithm used and the data for training in order to develop a final method after a refinement process through a refiner model.

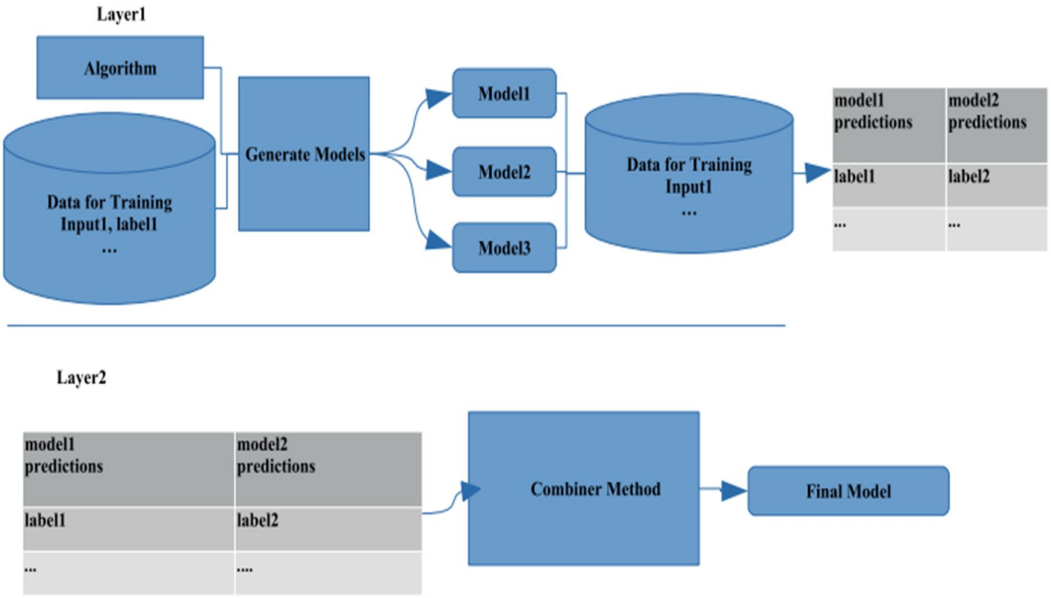


Figure 6: Training phase of tracking approach (Source: Demir, N., and Dalkilic, G., 2017)

Bitcoins and Cryptocurrency

The brief history of Bitcoins is shown on Figure 7 below.

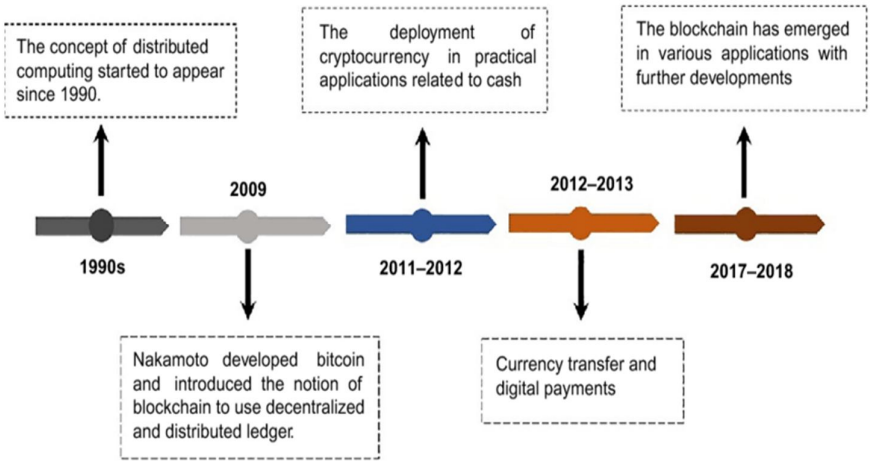


Figure 7: History of Bitcoins (Source: Adopted from [3])

a. Anonymity Of Bitcoins

One of the advantages of using bitcoins is anonymity, as was highlighted by Idebdou, N. (2015) and Brecese, J. (2013). Anonymity is unique and not shared publicly (Idebdou, N., 2015). Transactions are irreversible in the bitcoin network and it is close to impossible to trace back a transaction.

b. ***Volatility Of Bitcoins***

The volatility of cryptocurrencies arise from the fact that there is no central authority regulating them and their supply is fixed. There is no policy in place to regulate the growth in cryptocurrencies such as the monetary policy in fiat currencies. So since bitcoins have no central bank to regulate inflation, the currency has become an instrument of speculations.

c. Lack Of Adequate Infrastructure

The lack of adequate information communications technology (ICT) infrastructure in most developing nations present challenges for the adoption of crypto currencies in countries like Zimbabwe as these require internet connection for their trading and movement. However, ICT development in sub-Saharan Africa has grown rapidly the past decade. According to GSMA (2018) the overall mobile subscription penetration in Africa reached 44% in 2017 compared to 25% from 2010. The growing access to mobile connectivity has been vital to empower people and driving economic growth by increasing efficiency and productivity. The same report by GSMA (2018) also suggests that Mobile adoption has also had its impact on labor, estimated to have created 3 million jobs in 2017. The same report states that 7.1% of the GDP ($110 billion) across sub-Saharan Africa is generated by mobile technologies and services and is projected to constitute 7.9% of GDP ($150 billion) by 2022 (GSMA, 2018). Even though it is getting more common for people in urban areas to

have a mobile phone, the mobile coverage is still limited in rural areas with an absence of fixed connectivity, electricity grids and consequently an internet connection (Danho and Habte, 2019).

Benefits of Blockchain Technology

The benefits of using blockchain technology in digital currency includes the following:

1. *Decentralization*

To reduce the cyber-crime storage risks, a decentralized fashion is used to store the customer records and encourage consistency in the recording processes.

2. *Improved Privacy Control*

A single trusted third party can no longer adequately handle customer information. Smart contracts can be used to handle customers' data on behalf of the entire financial ecosystem.

3. *Immutability*

Customer information recorded in the blockchain is permanent and cannot be changed, which is crucial for tracking as the information is easily accessible by all financial institutions involved.

4. *Customer Product Personalization and Profile Management*

Block chain technologies can enable much more accurate, secure and privacy friendly profiling of both consumers and businesses, which accommodates personalized customer profiles.

Information Risk Management Process

The Information Risk Management Process is illustrated on Figure 8 shown below.

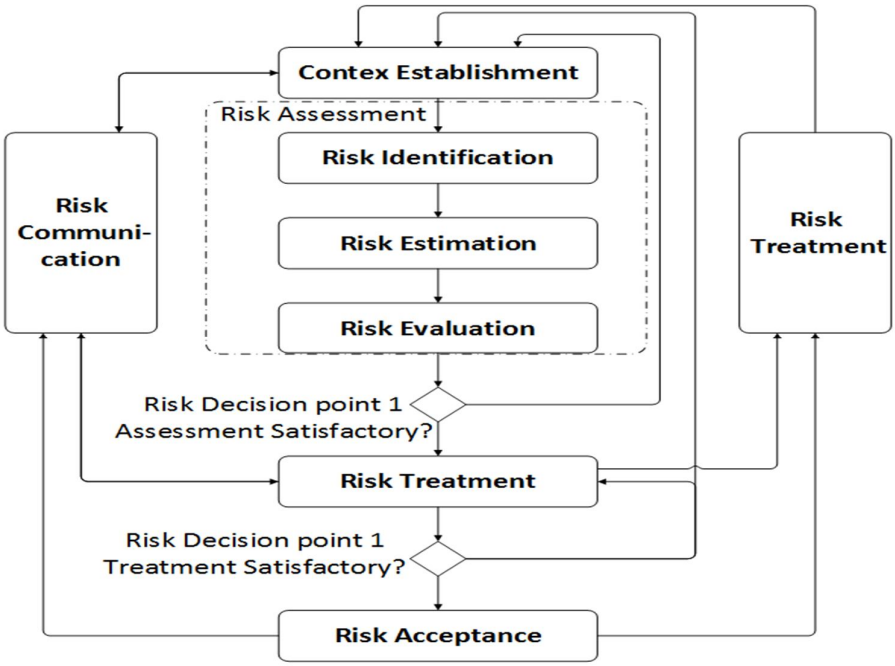


Figure 8: The ISO/IEC 27005:2011 Information Security Risk Management process (Source: Abdelwahed, I.M., et al, 2017)

Research Methodology

The research used the Pragmatism paradigm, which is a philosophy that is closely linked to the Mixed Method Research (MMR). Pragmatism places a greater emphasis on practical solutions to applied research questions and inquiry, and prefers those methods and theories which are practical and more useful for use in specific contexts (Peter, G.R., et al, 2005). Pragmatism mixes both qualitative and quantitative methods on the basis of "what works".

In this research, a mixed method approach was taken, which involves mixing both qualitative (Focus Group discussions) and quantitative methods (an online survey). Literature review and document analysis were also used in this research.

Focus Group Discussions

The Focus Group comprised a total of 100 participants from the Masters students attending the Applied Business Informatics module taught by the author at the University of Zimbabwe in 2020. The participants were organised into 10 Focus Groups, each with 10 people. The key questions discussed by the Focus Group discussions are the key research questions:

a) What is the proactive cybersecurity risk management plan that incorporates Machine Learning algorithms?

b) How do you develop a Blockchain Technology Application Model that manages cyber risks and vulnerabilities?
c) How does the Framework of Blockchain Technology and Cryptocurrency address cyber rsisks and creates value for the Financial Services sector?

A Focus Group is a qualitative research design which involves collecting data through guided group interaction. Focus Group discussions are a predetermined semi-structured interview led by a skilled moderator to interrogate a topic or a set of questions. The group comprises a small number of selected participants who are assigned a topic or set of questions to discuss. Focus Group discussions are used to enhance understanding or get into a deeper level of discussions than is normally done through a survey. Clearly defined research questions are often used in the Focus Group discussions. The participants are free to openly discuss the questions given until there is a consensus.

Quantitative Approach

The quantitative method makes use of numerical data which is easily transformed into usable statistics. Quantitative methods are characterised by the following:

- Data accuracy and reliability
- rationality and eventually causality of the independent variables on the dependent variables,
- numerical values for use in statistical techniques and sophisticated software,
- forecasting ability,
- control of the validity of the relationship between independent variables and the dependent variable.

However, quantitative methods face difficulty in accounting for all the variables involved, assumes that facts are true all the time and to all people, and often exclude degrees of freedom and choice of other options.

a) Daniel, (2016) presented the following advantages and disadvantages of the Quantitative Method:

1. Advantages of Quantitative Research Approach

- The quantitative method makes use of statistical data which saves on time and resources. Emphasis is placed on numerical values in the data collection and analysis. Quantitative research approach are commonly used in scientific research where huge volumes of numerical data is generated. Data (numbers, percentages and measurable figures) can be calculated and

analysed using statistical packages such as SPSS (a statistical package for social science) which save lot of energy and resources.

- The use of scientific methods for data collection and analysis makes generalization possible with this type of approach. Interaction made with one group can be generalized.
- Replicability is possible with this research approach as this can be repeated several times and still get the same results.
- The quantitative research method accommodates the use of control and study groups.
- Finally,the researcher is detached from the research approach, which eliminates researcher bias with either the data collection or data analysis. Therefore, the objectivity of the researcher is not be compromised.

2. *Disadvantages of Quantitative Research Approach*

- Detachment of the researcher from the participants may be considered a weakness within the quantitative research approach.
- It is difficult to get an in-depth study of the phenomena within its natural settings. The researcher may not be able to understand the group or individuals working with him nor will he appreciate them.
- Practical reality often requires both quality and quantity dimensions in research.
- There is very little flexibility in the order to follow during the testing of a hypothesis.

Conducting quantitative research

Quantitative research design uses two common approaches, descriptive and experimental. When conducting a quantitative research, a large participant sample size which ideally is representative of the overall population, is used. Through deductive reasoning the approach is narrowed down from being generic to being specific. The purpose of quantitative research in market research is to:

- Help researchers know whether or not there is an actual demand or market for the product or services that the company is offering.
- Estimate the number of people who are willing to avail your product or service.
- Identify your most ideal target demographic.
- Give a typical example of the target consumers' purchasing behaviour.
- Identify the change in market trends and patterns.

The main methods used in quantitative research are:

1. ***Survey*** where data is collected from responses given the participants through questionnaires.
2. ***Tracking*** which involves observing the behaviour of the participants in creating a pattern.
3. ***Experiments***, which manipulate one variable to produce a change in the other variable.
4. ***Structured interviews*** which uses a set of pre-planned questions to ask the participant. Structured interviews can easily be quantified.

Online Survey Method

A survey is used a data collection instruments used for soliciting responses from a predefined group of participants on a topic of interest. Due to the COVID-19 pandemic, the Web-based survey has become increasingly important and the safest method to use. An Online survey method was also used for the quantitative approach where 10 participants were involved.

What are the advantages of an online survey?

1. **Accuracy:** The error rate is low with an online survey**,** as the respondents register their responses by easy selection buttons with no human intervention necessary.
2. **Easy and quick to analyze:** Since all the responses are registered online, it is straightforward to analyze the data in real-time.
3. **Ease of participation:** In this new age technology-oriented universe, most people on this planet have access to the internet. Respondents prefer receiving the survey over the email.
4. **Great branding exercise:** In an online design, organizations or businesses have this opportunity to develop their questionnaire to align with their brand.
5. **Respondents can be honest and flexible at the same time:** The short precise questions used in an online survey encourage participants to complete the survey on time.
6. **Survey templates: Survey templates are available to guide the participants on how to answer the questions and the** templates are vetted questionnaires which are very focused and specific to the research problem under investigation.

RESULTS AND ANALYSIS

Cybersecurity national challenges

The national challenges of Cybersecurity as given by the Focus Group includes the following:

- Lack of clarity on the responsibilities with regards to ownership of Cybersecurity roles.
- The monotonic increase in the ubiquitous nature of technology and raid advances in the Internet of Things (IoT), which increases the risk on cybersecurity.

- The exclusion of Cybersecurity strategy in the formulation and development of the Business Strategy of organizations.
- The risk of over relience on one service provider to effect financial transactions at a national level.
- Inadequate enforcement of Service Level Agreements (SLAs) with service providers to ensure performance.
- Low internet penetration rates for the majority of the people in smaller towns, villages and other remote areas.
- Lack of adequate technical measures to handle Cybersecurity.
- Inadequate national awareness training programmes and campaigns.
- Huge skills gaps in Cybersecurity and delinquency in the competence levels.
- There is no simplification of the national ICT Policies and Cybersecurity policies for the benefit of ordinary citizens and people at grassroots levels.
- The higher education system is not offering meaningful programmes and courses on Cybersecurity skills and competences.

Cybersecurity Framework

The Cybersecurity Framework in developing nations faces the challenges in infrastructure, legal frameworks, educational awareness campaigns, Cybersecurity skills gaps, affordability by the majority of the population, and inappropriate frameworks.

The procedures for managing information security issues can be spelt out in organizational policies (Nielsen, R., 2015). However, a complete Cybersecurity vision is required in each case.

Risk Management Process

The Cybersecurity risk management plan includes:

1. Risk Analysis;
2. Risk Assessment;
3. Risk Mitigation;
4. Risk Monitoring

The Risk Management process is illustrated in Figure 9 below.

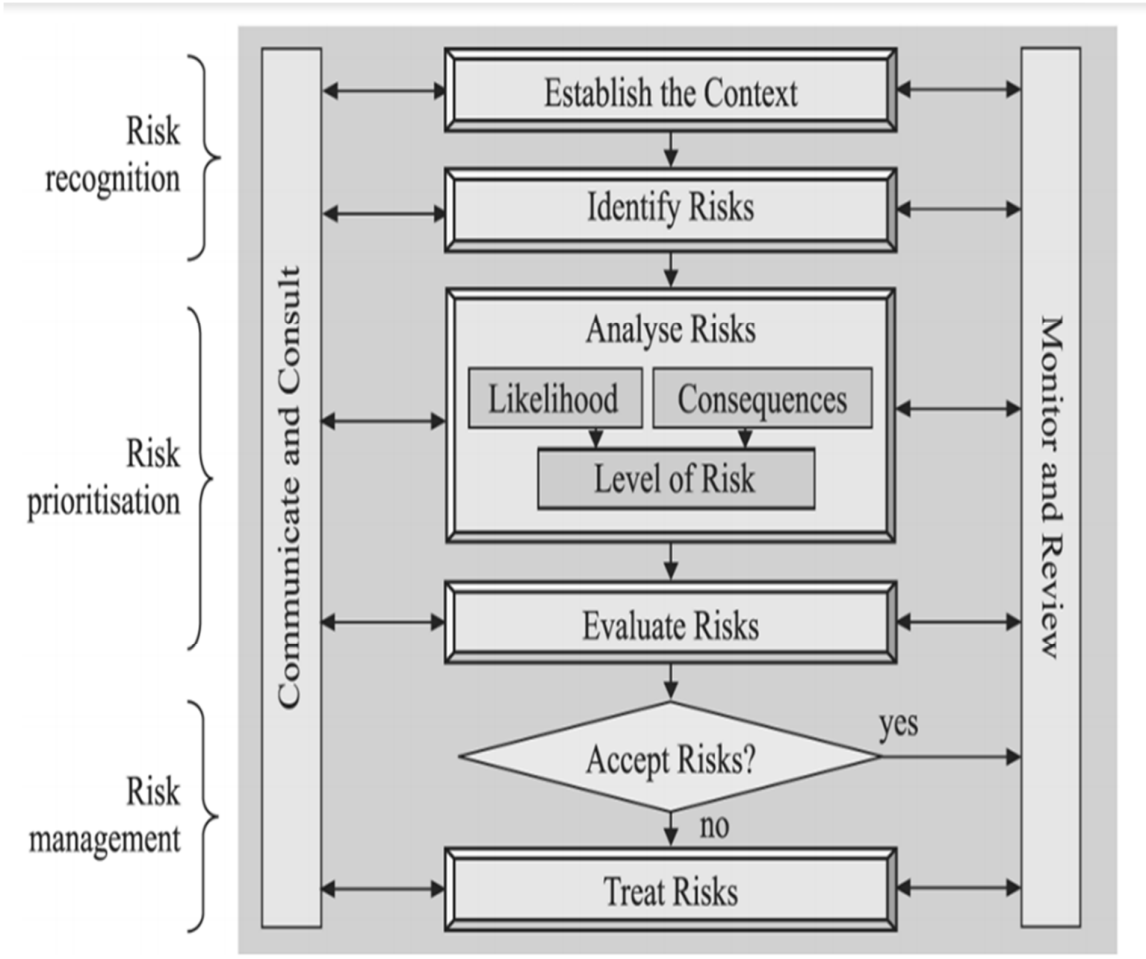


Figure 9: Risk Management Process

The elements of the Cybersecurity Risk Management Plan include the following:

- NIST Cybersecurity Framework with a focus on Identify, Protect, Detect, Respond, Recover dimensions
- Risk Types (focus on 6 risk types) which are Technology, Information, Cyber Risk, Business Resilience, Reputational and Regulatory Risk
- Governance Risk & Compliance
- Third Party Risk Management
- Policies, Standards and Procedures
- Risk Assessment (Identify ,
- Assess, Develop Controls & Make Decisions,
- Implement Controls , Supervise and Evaluate).

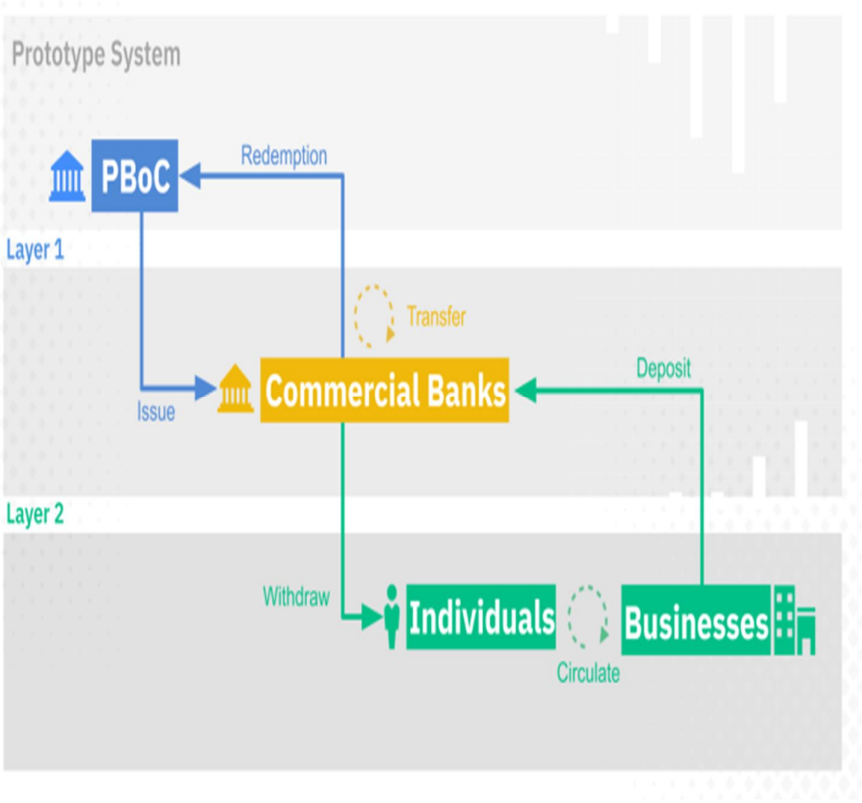
Blockchain Cyber Vulnerabilities

The Blockchan cyber vulnerabilities identified were as follows:

1. *Blockchain code vulnerabilities* from applications that may have inherent software coding errors or have high dependence on encryption algorithms (Abdelwahed, I.M., 2020).
2. *Blockchain platform vulnerabilities from* applications that run on general purpose operating systems and platforms with known risks.
3. *End-User vulnerabilities, e.g. hacking of online wallets, theft of a private key, etc.*
4. *Wallet controls as* digital wallet providers are now minimizing individuals risks and providing better key management services, but the risk is still high on the use of passwords and other user authentication controls (Abdelwahed, I.M., et al, 2017).

Model Structure for Blockchain Technology and Cryptocurrency

The model structure for Blockchain Technology developed is shown on Figure 10 below



.

Figure 10: Model Structure for Blockchain Technology and Cryptocurrency

The five major components of the model structure are:

1. The Distributed Ledger Technology Cryptographic hash functions
2. The DLT Public-Private Key Cryptography
3. The DLT Nodes
4. The DLT Tokens

5. The DLT Blocks in a blockchain to record transactions.

Central Bank Digital Currency (CBDC)

Central Bank Digital Currency is commonly defined as the value of digital representation, electronic storage, and cryptographic transfer, that is expressed digitally, stored electronically, and encrypted for transfer of ownership. It is issued and managed by a sovereign institution such as the Central Bank, subject to the financial laws and regulations in that country. Thus a Central Bank Digital Currency (CBDC) is a form of centralised cryptocurrency, or another form of fiat money, similar to coin and banknote. The functions of CBDC includes the following:

a) Centralized issuance: implies that it is backed by central banks. The monetary policy is formulated by the central bank, such that CBDC has the intrinsic value.
b) Transferability: implies that CBDC can be used as a means of circulation and payment for ongoing value movements in economic activities. The CBDC also needs to achieve the split maintaining the zero-sum principle for more efficient and convenient circulation.
c) Storability: CBDC and the transaction history are securely stored in the form of electronic data in an organization or user's electronic device for query, payment, exchange and management.
d) Offline transaction: Offline transaction of CBDC specifically means that it may not directly communicate with the host servers or the main system when the transaction is performed through the electronic device, and the payer does not exchange information with other devices or systems through communication methods such as wired or wireless.
e) Exchangeability: In the circulation of CBDC in the digital world, it is also necessary to satisfy the exchangeability, including the equivalent exchange between one CBDC and other forms of the same sovereign currency, as well as the foreign exchange between CBDC and other sovereign currency.

The three-layered blockchain and cryptocurrency application technology model is as follows:

1) *Regulatory Layer*

The regulatory layer is mainly in charge of controlling and governing the whole life cycle of CBDC throughout the technical and policy aspects, so as to maintain the healthy and stability of the financial environment dominated by CBDC. The Regulatory layer mainly includes the Central Bank, public key infrastructure (PKI) with identity authentication as the core, and other regulatory bodies such as sovereign institutions.

2) Network Layer

The network layer is a bridge between the top regulators and ordinary users. It is different from the p2p network structure mostly adopted by decentralized cryptocurrencies, network layer in

CBDC adopts two different network structures. One is a tree hierarchy structure centred on central bank and other regulatory agencies, and the other is a local distributed structure composed of commercial banks and other third-party operators.

3) User Layer

User layer comprises the low-level users and their transactions, which are not only the regulatory objects of regulatory player, but also the main data source for verification and processing of network layer. User layer contains cash exchange, CBDC deposit, and CBDC withdrawal, inter-bank payment, cross bank payment, cross-border payment and currency exchange.

An Explanation On How the Framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the financial services Sector

The fully enunciated explanation of how the framework of Blockchain Technology and Cryptocurrency addresses cyber risks and creates value to the financial services sector is as follows:

- *Minimal Transaction Fees:* Because cryptocurrency transfers are peer-to-peer and require no centralized intermediaries, transaction costs are minimal and decentralized systems do not charge currency conversion fees.
- *Accessibility:* Cryptocurrencies by their very nature are not subject to the exchange rates, interest rates, transactions charges, or other levies imposed by a specific country.
- *Instant Payments are enables by the* peer-to-peer transactions.
- *Improved security provided by Blockchain technology* than the centralized financial systems, which makes it extremely difficult for hackers to infiltrate.
- *Transparency in the transactions.*
- *Decentralization framework in support of* stakeholder governance, putting decision-making powers in the hands of individuals, not central authorities.
- *Immutability:* The immutable nature of the blockchain's general ledger removes the chance for internal actors to manipulate data to their benefit.

Roadmap for Building Machine Learning Systems

In order to improve on Cybersecurity and cyber risk management, a machine learning approach is the best solution as depicted by the roadmap shown on Figure 11 below.

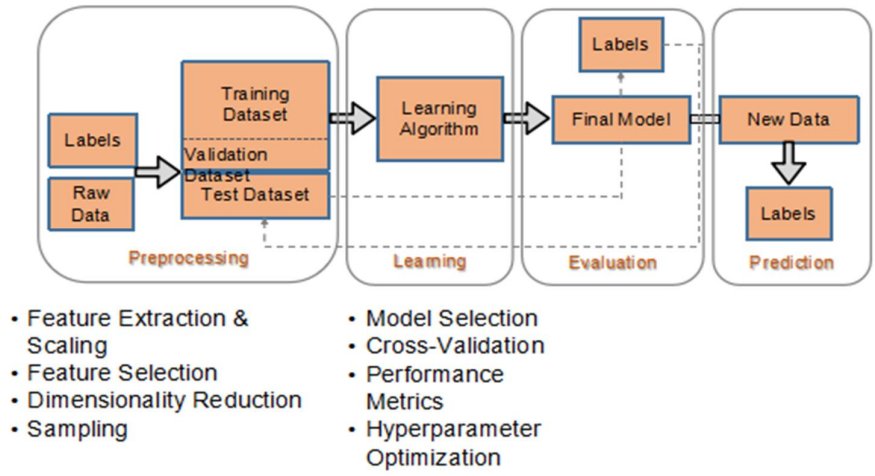


Figure 11: Roadmap for Building Machine Learning Systems

Machine learning is one of the most exciting recent technologies in Artificial Intelligence. Learning algorithms are now being extensively used in search engines used by Google or Bing. According to Higginbottom, (2018) the ultimate goal of AI is to develop human like intelligence in machines which can be accomplished through learning algorithms which try to mimic how the human brain learns (Hall, 2019). Lifelong Machine Learning, or LML, considers systems that can learn many tasks over a lifetime from one or more domains. They efficiently and effectively retain the knowledge they have learned and use that knowledge to more efficiently and effectively learn new tasks.

The key issues in Machine Learning worthy of consideration are as follows:

- What algorithms can approximate functions well and when
- How does the number of training examples influence accuracy
- Problem representation / feature extraction
- Intention/independent learning
- Integrating learning with systems
- What are the theoretical limits of learnability
- Transfer learning
- Continuous learning

Framework for Blockchain Technology Application and Cyber Risks

The framework for Blockchain Technology Application Model is closely associated with basic values of communication such as confidentiality, integrity, authenticity, non-repudiation and availability. The key aspects of bitcoins are:

1. *Confidentiality;* the system has privacy or ability to control access to bitcoin transactions so only authorized individuals can view sensitive information. Confidentiality is provided by having a public key to assign ownership rights and a private key to certify the transaction. Miners verify the transaction on the blockchain, but anyone on the network can also use the public key to verify the transcation.

2. *Integrity;* information of each bitcoin transaction is accurate and reliable and cannot be subtly changed or tampered with by an authorized party. Blockchain records are kept of all transactions.
3. *Authenticity;* All the transactions in blockchain are authentic. This is correlated to the ability to verify the content of the bitcoin transaction which cannot be changed in an unauthorized manner.

4. *Non-repudiation;* meaning that the origin of any action on the bitcoin system can be verified and associated with a user, with no possible denial. Every miner has their own key and certain record of transaction which comprises a combination of number and letter.

5. *Availability;* The information and other critical assets of bitcoin transaction must be accessible to miners and the business when needed (Tampi, M.M., 2019).

How does the BT model address cyber risks?

- *No double-spending:* No double-spending means that once a CBDC owned by a user has been transferred, it cannot be used to pay for other transactions. Unlike a physical currency, CBDC, uniquely identified by a sequence of serial numbers, can be copied and saved multiple times. Therefore, no double-spending is the basic security that all digital currencies need to consider.
- *Unforgeability:* Unforgeability requires that no one can falsify CBDCs issued by the Central Bank or forge a CBDC that is not owned by him/her. These forged CBDCs cannot pass verification. CBDC also requires anti-counterfeiting technology to ensure currency security, just like physical currency.
- *Non-repudiation:* Non-repudiation requires that all participants' actions be recorded from the initiation of the transaction to the end, including the payer, the recipient, and the transaction verifier. No one can deny the transaction steps that he has completed.
- *Verifiability:* Verifiability requires that all transaction records involved in the CBDC system can be validated effectively. This is crucial for CBDC as a currency of circulation and a means of payment. It is also the basis for other security properties.

- *Anonymity:* The physical currency is anonymous in actual circulation. Similarly, CBDC should also be designed for user privacy and anonymity. Throughout the development of cryptocurrencies, the anonymity of CBDC mainly includes anonymity of identity and anonymity of transaction. Intuitively, they require that any unauthorized user cannot obtain, calculate, or infer the identity of a user and the information of a transaction through open source data.

Conclusion

Blockchain is a significant technological breakthrough in decentralized cryptocurrencies (Kabanda, G., 2020)] permitting remote peer-to-peer value transfers amongst parties devoid of a trusted third party. The factors that blockchain may affect the development of payment industry and CBDC include:

a) Cost: Blockchain-based payment systems may offer lower transaction cost than other payment methods, especially in cross-border payment, currency exchange and other payment scenarios involving multiple intermediary entities.

b) Usability: Compared with traditional payment methods, blockchain-based payment methods have some usability advantages, because the blockchain makes the transaction process more intuitive and easier to integrate with other services.

c) Anonymity: Although the blockchain itself does not provide any privacy protection, it provides an effective network architecture for anonymous payment. Some blockchain-based cryptocurrency schemes allow users to conduct transactions without providing their own real credentials.

Benefits of Block-chain technology to the Financial Services Sector

Below is the summary of the ways in which block-chain technology and cryptocurrency benefits the Financial Services sector:

1. Costs Reduction
2. Faster Transactions
3. Improved Security (Mulders, P.F.A., 2019).
4. Improved Data Quality
5. Digital Currencies
6. Accountability
7. Compliance
8. Reduced Error Handling & Reconciliation

9. Increased Transparency
10. Ease of Money Transfers
11. Reduced Fraud Via Self Sovereign Identity

References

ABDELWAHED, I.M., Ramadan, N., and Hefny, H.A., (2020), *Cybersecurity Risks of Blockchain Technology, International Journal of Computer Applications (0975 – 8887), Volume 177 – No. 42, March 2020.*

ALANEZI, A.A., (2014). Development of an Orally Disintegrating Mini-Tablet (ODMTs) Containing Metoclopramide HCl to Enhance Patient Compliance. Master of Science Thesis. University of Toledo, 2014, http://rave.ohiolink.edu/etdc/view?acc_num=mco1417861431.

ATLAM, H. F., Walters, R. J., & Wills, G. B. (2018). Fog computing and the internet of things: A review. In *Big Data and Cognitive Computing*.https://doi.org/10.3390/bdcc2020010

BERMAN, D.S.; Buczak, A.L.; Chavis, J.S.; Corbett, C.L. A Survey of Deep Learning Methods for Cyber Security. *Information* **2019**, *10*, 122. https://doi.org/10.3390/info10040122

BRECESE,J., 2013. Research Note Money from Nothing: The Socioeconomic Implications of "Cyber--currencies".

BRINGAS, P.B., & Santos, I., (2010). Bayesian Networks for Network Intrusion Detection, Bayesian Network, Ahmed Rebai (Ed.), ISBN: 978-953-307-124-4, InTech, Available from: http://www.intechopen.com/books/bayesian-network/bayesian-networks-for-network-intrusion-detection.

DEMIR, N., & Dalkilic, G., (2017). Modified stacking ensemble approach to detect network intrusion, Turkish Journal of Electrical Engineering & Computer Sciences, Accepted/Published Online: 15.11.2017, http://journals.tubitak.gov.tr/elektrik/

. ELMAMY, S.B.,Mrabet, H., Gharbi, H.,, Jemai, A., & Trentesaux, D., (2020), *A Survey on the Usage of Blockchain Technology for Cyber-Threats in the Context of Industry 4.0, Journal of* Sustainability 2020, 12, 9179; doi:10.3390/su12219179; http://www.mdpi.com/journal/sustainability

GSMA. (2018). Mobile Economy 2018. *GSMA Intelligence*.

HALL, M. (2019). Chronic renal disease and antenatal care. In *Best Practice and Research: Clinical Obstetrics and Gynaecology*. https://doi.org/10.1016/j.bpobgyn.2018.10.002

HIGGINBOTTOM, K. (2018). *Emotional Intelligence Undervalued In The Hiring Process*. Forbes.

IDEBDOU, N., 2015. A Game of Coins: The Digitization of Money and the Regulation of Virtual Currencies.

LEWIS, R. E., & Heckman, R. J. (2006). Talent management: A critical review. *Human Resource Management Review*. https://doi.org/10.1016/j.hrmr.2006.03.001

MULDERS, P. F. A. (2019). Abstracts voorjaarsvergadering NVU, 16 en 17 mei 2019, Rotterdam. *Tijdschrift Voor Urologie*. https://doi.org/10.1007/s13629-019-0255-6

NATIONAL Institute of Standards and Technology, (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.

NIELSEN, R. (2015). CS651 Computer Systems Security Foundations 3d Imagination Cyber Security Management Plan, Technical Report January 2015, Los Alamos National Laboratory, USA.

PETER, G.R., Artur, P., & Peter, H.F., (2005). "A Pragmatic Research Philosophy for Applied Sport Psychology", Ph.D Dissertation, Kinesiology, Sport Studies and Physical Education Faculty Publications, 80, 2005, https://digitalcommons.brockport.edu/pes_facpub/80

STALLINGS, W., (2015). Operating System Stability. Accessed on 27th March, 2019. https://www.unf.edu/public/cop4610/ree/Notes/PPT/PPT8E/CH15-OS8e.pdf

TAMPI, M. M. (2019). MENAKAR PROGRESIVITAS TEKNOLOGI FINANSIAL (FINTECH) DALAM HUKUM BISNIS DI INDONESIA. *Era Hukum - Jurnal Ilmiah Ilmu Hukum*. https://doi.org/10.24912/erahukum.v16i2.4529

TRUONG, T.C; Diep, Q.B.; & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. Symmetry 2020, 12, 410.

SCHUESSLER, D.L., (2009), 'Beyond Content: How Teachers Manage Classrooms to Facilitate Intellectual Engagement for Disengaged Students',Theory Into Practice,48:2,114 — 121; DOI: 10.1080/00405840902776376; URL: http://dx.doi.org/10.1080/00405840902776376

KESSLER,J.B., & Hunt, A. (2019), "The Welfare Effects of Nudges: A Case Study of Energy Use Social Comparisons." *American Economic Journal: Applied Economics*, 11 (1): 236-76.DOI: 10.1257/app.20170328

DANHO & HABTE, (2019), Blockchain for Financial Inclusion and Mobile Financial Services: A study in sub-Saharan Africa[D], 2019.

KABANDA, G., (2020), Applied Business Informatics module Lecture Notes, University of Zimbabwe, 2020, https://gabrielkabanda.wixsite.com/professorgabrielkaba

NOWINSKI, W., & Kozma, M., 2017, "How Can Blockchain Technology Disrupt the Existing Business Models?," Entrepreneurial Business and Economics Review, Centre for Strategic and International Entrepreneurship at the Cracow University of Economics., vol. 5(3), pages 173-188.

Abdelwahab, S.A.M., W. S.E. Abdellatif , & A. M. Hamada, (2020) "Comparative Analysis of the Modified Perturb & Observe with Different MPPT Techniques for PV Grid Connected Systems," International Journal of Renewable Energy Research-IJRER, pp 156-164, Vol 10, No 1, 2020.

DANIEL, E., (2016), "The Usefulness of Qualitative and Quantitative Approaches and Methods in Researching Problem-Solving Ability in Science Education Curriculum", Journal of Education and Practice, http:// www.iiste.org, ISSN 2222-1735 (Paper) ISSN 2222-288X (Online), Vol.7, No.15, 2016, pp91-100.