

A Review of Existing Cryptosystem, Challenges and Possible Adoption in Nigeria

Abdulkarim Oloyede
Research Fellow

*Department of Telecommunication Science/ Research and Development, NCC
University of Ilorin, Ilorin, Kwara State.*

Abstract -- The goal of this study is to examine the necessity for sensitive data/information security in society. With the widespread adoption of information security, people require a method to ensure that data/information remains confidential, authentic, and of high integrity. This research study investigates how the advancement of cryptography addresses this issue. Nonetheless, the use of cryptography in digital transactions has the potential to be a disruptive technology in our modern world. Some government organizations are concerned about this new technology because they believe spies, criminals, and hackers will exploit it because bitcoin is anonymous and there is no way for regulatory entities to monitor and balance it. This study examines the emergence of the cryptosystem, its benefits, and its disruptive features, particularly in cryptocurrencies.

Index Terms -- Bitcoin, Blockchain, Crypto-asset, Cryptography, Cryptocurrency, Cryptosystem, Decryption, Encryption.

I. INTRODUCTION

The importance of data security cannot be overstated in a world where sensitive and secret data must be kept private. This data can be financial, scientific, mathematical, medical, military, and so on. It is also critical that this information, which must be kept private from the broader public, is effectively managed in order to maintain its secrecy, integrity, and validity. Some data, if divulged or exposed to the incorrect source, can represent a threat to personal and national security. Different individuals must secure specific information in order to ensure that the interpretation of the information may only be done, altered, and processed between the sender and the authorized recipient. To secure such information, it gives rise to the use of cryptography keys in communication to encrypt and decrypt such information [1]. Encryption and decryption techniques have emerged as the immediate option for guaranteeing that sensitive information is safeguarded from unauthorized access. Cryptography is essentially the establishment of a secure means of transmitting information through the implementation of a set of algorithms and keys. The complexity of the set of algorithms used determines the difficulty of the encrypted communication. Simply, the more sophisticated the message's algorithm, the stronger the encryption process.

A cryptosystem, also known as a cipher system, is a scheme or structure that incorporates a sequence of algorithms that

transform plain-text to cipher-text in order to securely encrypt and decrypt messages. In order to keep data secure, a cryptosystem integrates and implements methods for key generation, encryption, and decryption processes. The term "cryptosystem" is derived from the phrase "Cryptographic System," which refers to a computer system that employs cryptography, a method of protecting information and communication by encoding it in such a way that only those who are intended to read, manipulate, and process it may do so. The most substantial part of a cryptosystem is the encryption keys, which render the message, information, or data value unreadable and unbreakable by an unauthorized reader but only by the intended recipients of the content. These keys form the word 'Krypto,' which means "secret" or "concealed" in Greek .

Cryptography techniques were first used in ancient times, according to historical records. This foundation has since formed the cornerstone for modern methods and algorithms utilized in data encryption and decryption in our modern technological environment. This system's earliest forms may be traced back to Roman and Egyptian civilizations. The usage of 'Hieroglyph' was the first known indication of cryptography. The Egyptians employed hieroglyphics to express written texts over 4000 years ago [2]. Caesar Shift Cipher [3] is another early kind of cryptography. This form was called after Julius Caesar, who used letter shifting techniques to preserve military information and send signals to his generals on the battlefield, particularly during World War II (WW2). The Caesar Shift Cipher works by shifting the letters of a message by an agreed number (usually three), and the recipient shifts the letters back by the same number to decipher the message. However, Cipher had the difficulty of being readily translated and broken down the frequency of letter [4], and once these letters are broken down, they become obsolete to the public. The algorithms used a few years ago were limited to shifting and rearranging the 26 letters within the alphabets [5], but modern algorithms are not limited to these letters alone, as more powerful and complex algorithms are being built by technologists today to ensure that the message encrypted is virtually unbreakable by unauthorized recipients. Cryptologists (Scientists who explore different ways to safeguard and ensure the confidentiality, integrity, and validity of information) [6] are developing more strong solutions as the world evolves.

Cryptography is used in a variety of ways to secure communication, end-to-end encryption, data storage, password storage, digital currency transactions, and so on. It has a wide area of applications in daily life, including authentication/digital signatures, time stamping, electronic money, email communication, social media accounts, and cryptocurrency technology, which is the focus of this research.

This research is organized as follows: Section I gives an introduction of the topic of discussion, Section II provides the Literature Review, Section III discusses the methodology used in carrying out this research, Section VI looks at the components of cryptosystem, Section V discusses the method of encryption in cryptosystem, Section VI shows how cryptosystem is applicable to cryptocurrency technology and Section VII further shows how disruptive this technology can be in digital economy. Finally, a possible solution is recommended.

II. LITERATURE REVIEW

Related works on this research topic have been completed; some of the published works on related topics are reviewed as follows:

In [7] Tuncay on the research topic “Important of cryptography in information security”, looked at how encryption and decryption techniques must be enhanced in order to provide the maximum level of security to authorized users. Strong cryptography, according to the study, is required to protect information in our digital environment against criminal activities and frauds. In his research, he also claimed that contemporary cryptography is required to offer security and digital keys to ensure that information sent between the sender and intended receiver in cyberspace remains intact and protected.

The broad adoption of cryptography is a necessary result of the information revolution, according to research “Overview of cryptography” carried out by Claret in [8]. The paper explained how the introduction of cryptography as a mechanism of ensuring the privacy of conversations and transactions ignited a hot policy discussion, with some government agencies attempting to limit the use of data encryption out of fear that criminals and spies would exploit the technology. The paper went on to discuss the benefits and drawbacks of encryption systems for society, as well as how abuse needs regulation.

Hassan et al. in [9], the work “Overview of Efficient Symmetric Cryptography: Dynamic vs Static Approaches” showed how existing cryptography algorithms suffer from various implementation flaws and are vulnerable to new types of severe attacks. Furthermore, their complexity makes them unsuitable for modern low-cost devices, and if deployed, they would have a severe impact on system performance and may undermine system security. To address these constraints, the study presented suggestions for the design of future (dynamic) cryptographic algorithms as well as highlighted future research problems, difficulties, and directions. As Using dynamic key-dependent substitution and diffusion primitives with maximum

cryptography performance might provide improved resistance against modern attacks.

Sheping Zhai et al [10], introduced the main applications of cryptography in the cryptocurrency known as blockchain in their research "Research on the application of cryptography on blockchain," analysed the existing problems of insecure digital transactions, simplified blockchain technology starting with blockchain infrastructure, and looked at how cryptography technology was introduced. The paper demonstrated that digital encryption is used throughout the cryptocurrency and is at the heart of the blockchain system. The paper further emphasized that cryptography research is essential for the growth of blockchain and predicts the future research direction of cryptocurrency technology.

According to Kadena et al. in [11], their research "Security Issues in Blockchain(ed) World" looked into the technological, risk, and security challenges of blockchain. The paper examined cryptocurrency technology in the context of financial crime, which poses a threat to national and international security; it focused on national security and how it is affected by criminal use of cryptocurrencies; and it elaborated on the lack of standards and mechanisms in connection with illegal activities, particularly money-laundering and terrorism financing. The paper advocated for the use of fuzzy approaches for security analysis and testing, as well as GDPR compliance for better data protection in the chain. They came to the conclusion that a collaboration of responsible organizations from many sectors is required, as well as an assessment of potential methods in which perpetrators can exploit additional applications. The convergence of terrorism and cybercrime should be examined, and appropriate preventive measures should be implemented.

III. METHODOLOGY

This research was carried out through critical analysis of related research papers, articles, reports, and journals related in the fields of cryptography and cryptocurrency technology. The resources used for the research were chosen based on their proximity to and relevance to the topic of discussion. For this topic, no real practical experiment was carried out. The research methodologies employed may contain mistakes related to the information source of the research papers utilized as case studies.

IV. COMPONENTS OF CRYPTOSYSTEM

As researched, Cryptosystem is the complete system that combines the algorithms for key generation, encryption and decryption techniques. This system is made of components such as Plain-text, Encryption algorithm, Cipher-text, Decryption algorithm, Encryption key and Decryption key [12]. The relationship between these components and flow of information is shown in Fig. 1

A. Plain text

This is the raw data, message or information that needs to be protected from unauthorized users. It can also be referred to as any readable data that can be read and interpreted by humans or machines.

B. Encryption Algorithm

This is the mathematical algorithm that takes Plain-text as an input and convert it to cipher-text which is the encrypted message/data. It takes in two inputs (the Plain-text and the Encryption key) to produce a cipher-text.

C. Cipher-text

This is the unreadable, unbreakable and encrypted version of plain-text after transformation. This can be series of letters or numbers which humans or machines cannot make any sense of unless it is been decrypt back to the original plain-text

D. Decryption Algorithm

This is the mathematical algorithm that takes Cipher-text as the input received and decrypt it into plain-text which is the decrypt message/data. It takes in two input (the cipher-text and decryption key) to produce a plain-text.

E. Encryption key

This is typically random of strings or codes the sender uses to compute the cipher-text from a plain-text. These keys are created with algorithms in order to ensure that the information is unreadable and unpredictable. The complexity of encryption keys constructed for a message will determine the harder it will be decoding such message.

F. Decryption key

This is a set of strings or codes the intended recipient of a message uses to convert cipher-text to plain-text.

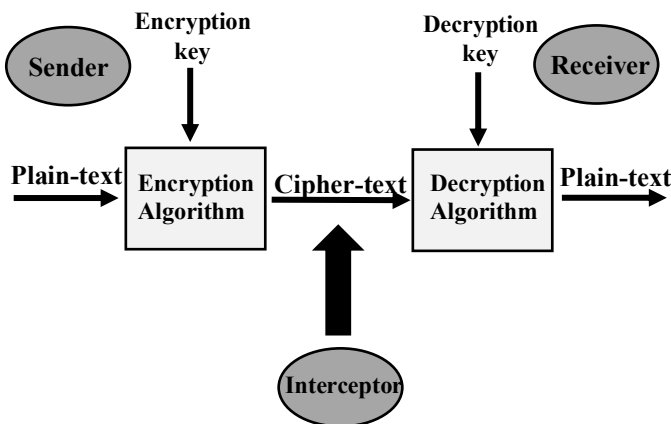


Figure 1: Components of Cryptosystem

V. METHOD OF ENCRYPTION IN CRYPTOSYSTEM

The method by which a cryptosystem encrypts and decrypts data/messages transferred from the sender to the intended receiver, as well as the type of encryption key used in the message, are used to classify cryptosystems. There are two types of cryptosystems: symmetric key and asymmetric key. Cryptosystem.

A. Symmetric Cryptosystem

This is an encryption algorithm that uses only a key (a secret key) to encrypt and decrypt message [9]. This type of encryption allows the sender to use a unique password during encryption process and the same password will be used to decrypt the message by the intended recipient. Once anyone has the secret key the message is encrypted with, the decrypting will be done with the same key. This implies that the secret key must be shared with trusted and authorize people because if spies or hackers getting hold of the secret means they can decrypt all the messages the person is trying to protect and secure. Symmetric encryption is useful to protect messages between parties with already shared keys. Fig 2 shows how secret key is been used for encryption and decryption in symmetric encryption.

Some examples of symmetric encryption algorithms include: Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA), Blowfish (Drop-in replacement for DES or IDEA) etc.

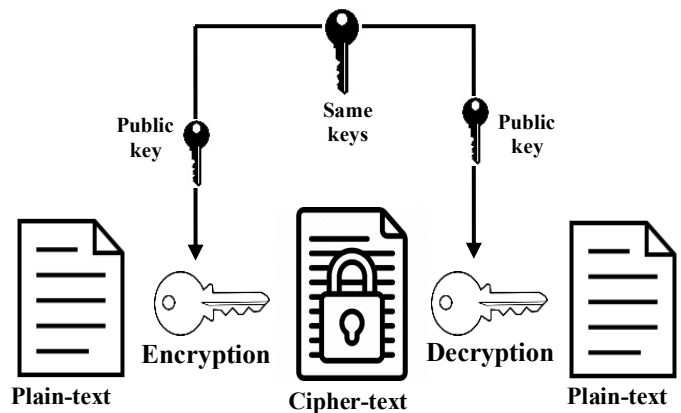


Fig. 2 Symmetric Encryption

B. Asymmetric Cryptosystem

This is also known as Public Key Encryption Method [12]. It uses two separate keys (public and private keys) to encrypt and decrypt data. To protect the message, the sender uses public key to encrypt the message and the corresponding private key to decrypt at the receiver's end. The public key is open to everyone. This means anyone can access the encrypted message but it will be in form of cipher-text which means it cannot be decrypt until the private key known to the authorized people who have access to the message is used to decrypt it. The public key can be given freely to everyone and anyone but the private key is only known to the owners of the message [9]. Asymmetric encryption is considered a more secure way of protecting information than symmetric encryption because it uses two keys, one for encryption and the other for decryption as shown in Fig. 3 which makes the data more secured and less vulnerable to unintended recipient. However, this method of encryption consumes more processing power than symmetric encryption during the encryption and decryption process. [8]

Some examples of asymmetric encryption include: Rivest Standard Adieman (RSA), Digital Signature Standard (DSS). Elliptical Curve Cryptography (ECC), TLS/SSL protocol, etc.

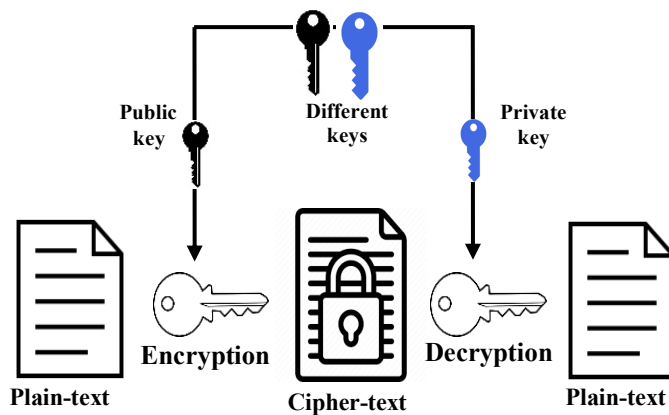


Fig. 3 Asymmetric Encryption

VI. APPLICATION OF CRYPTOSYSTEM TO CRYPTOCURRENCY

The word ‘Cryptocurrency’ is the combination of the word ‘cryptography’ and ‘currency’. The Advanced Oxford dictionary simply defines it as ‘a digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than a centralized authority’.

In current world, this corresponds to the concept of digital transactions using cryptography and encryption keys. Cryptocurrencies make it simple to move funds between two people anywhere in the world without the participation of government agencies or central banks. The transfer of funds cannot be legally monitored by a third party in this manner. Instead, cryptography keys have been used to secure them. Cryptocurrencies rely on a technique known as public key cryptography to accomplish all of this. One of the fundamentals of cryptocurrency is asymmetric cryptography [10,13].

A user's wallet or account address in cryptocurrency has a public key, whereas the private key is known only to the owner of such account and is used to sign transactions. An address can be thought of as a bank account number as well as the recipient of cash. Fund transfers are performed with minimum processing fees, allowing consumers to avoid the high fees levied by banks and financial institutions. [13]

In recent years, cryptocurrency has seen tremendous success and expansion. This new technology [14], has become a source of enormous opportunity in the banking, economic, and financial fields. Aside from that, this technology has been a source of employment creation and an opportunity for IT companies to create value. As cryptocurrency continues to gain traction in the global economy, we should expect to see more career opportunities in this sector.

Furthermore, cryptocurrency allow wallet owners to remain entirely anonymous if they so desire.

As crypto-assets transfer does not require any sensitive/personal information aside from the number of virtual

wallets, i.e., the public keys, transactions can be done between two parties with the maximum anonymity and secrecy if they do not want to divulge their identities.

The creation of this system as a medium of exchange has also provided the masses with the opportunity to finally have access to a digital economy that is completely independent of laws imposed by governments, banks, or any other centralized/financial entity. As a result of this advancement, online communities are now relying on this framework to conduct virtual transactions among its members.

VII. CRYPTOCURRENCY AS A DISRUPTIVE CRYPTOSYSTEM TECHNOLOGY

While the introduction of cryptographic algorithms into cryptocurrencies looks to be secure in digital transactions, the lack of consistent and legitimate international standards throws a host of legal difficulties into the system. Many investors and governments interested in participating in this breakthrough technology are sometimes discouraged by the lack of a legal framework. Because cryptocurrency transactions are semi-anonymous and lack regulatory oversight, they are ideal for a wide range of illicit operations. This technology's decentralization component, which has been one of its achievements, may turn out to be one of its failures.

With the growing popularity of the cryptocurrency market and the vast number of criminal activities, governments and other stakeholders around the world must pay closer attention. In recent years, the cryptocurrency market, which includes Bitcoin, has grown to \$500 billion; its applications range from transferring and moving funds to purchasing software, real estate, and even illegal substances [15]. The overall market value of the top 100 cryptocurrencies exceeded € 300 billion in early 2018. Meanwhile, the entire market capitalization of all cryptocurrencies is \$ 728 billion [16].

VIII. RECOMMENDATION

This paper recommends that legal environment favourable to cryptocurrency should be created. Creating regulatory bodies for this technology will authenticate legal transactions that will be carried. This will control the rate of fraud and illegal activities carried out in this decentralized system. This development will definitely allow the distribution of crypto-assets which are primal economic interest for countries wishing to perpetuate their financial attractiveness. In order to sustain the use of virtual currency legally in some countries, the standardization of legal bases governing cryptocurrencies is a necessity.

IX. CONCLUSION

The study looked at the concept of a cryptosystem, its evolution, and its use in cryptocurrency technology. It demonstrated the methods of encryption in a cryptosystem through examples. This study went on to discuss how Cryptocurrency is a disruptive technology in our modern society, which leads to its rejection by different authorities and

government bodies. Finally, a feasible solution on acceptance of cryptocurrencies for digital transactions was suggested.

X. REFERENCES

- [1] C. Bernstein "Cryptosystem" an article in *TechTarget* Available Online. <https://searchsecurity.techtarget.com/definition/cryptosystem> Date accessed 19th August, 2021.
- [2] M. K. Adomey "Introduction to Cryptography" in *Africert*, Vol.1, pp 5-20, Feb. 2017.
- [3] L. Dennis, G. Prichett "Cryptology: From Ceaser Ciphers to Public-Key Cryptosystems" in *The College Mathematics Journal* Vol. 18 pp 2-17, January, 1987.
- [4] A. Jain, R. Dedhia A. Patil "Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication" in *International Journal of Computer Applications* Vol. 129, pp 13, November, 2015.
- [5] A. Mishra "Enhancing Security of Caesar Cipher Using Different Methods" in *IJRET* Vol. 12 pp 1-6, 2013.
- [6] J. G. Simmons "Cryptology" *Encyclopedia Britannica*, Aug. 2016. Available Online. <https://www.britannica.com/topic/cryptology>. Date Accessed 19th 2021.
- [7] M. T. Gencoglu "Importance of Cryptography in Information Security" in *ISOR Journal of Computer Engineering (IOSR-JCE)* Vol. 21, pp 65-68, Feb. 2019.
- [8] N. A Claret "Overview of Cryptography" *IEEE* vol 1, pp 1-5, 2006
- [9] H. N. Noura, A. Chebab, R. Couturier "Overview of Efficient Symmetric Cryptography: Dynamic vs Static Approaches" in *IEEE* Vol 1, pp 1-6, June, 2020.
- [10] S. Zhai, Y. Yang, J. Li, C. Qui, J. Zhao "Research on the Application of Cryptography on Blockchain" in *Journal of Physics* Vol. 1168, PP 1-8, 2019.
- [11] E. Kadena, P. Holieza "Security Issues in Blockchain(ed) World" *IEEE* Vol 1, pp 211-214, June, 2020.
- [12] L. Ozturk, E. Sulungur "The Regulation Problem of cryptocurrencies" presented at *Global Conference on services and Retail management* [Florida, USA], June, 2019.
- [13] A. Alharbi and O. Sohaib, "Technology Readiness and Cryptocurrency Adoption: PLS-SEM and Deep Learning Neural Network Analysis," in *IEEE Access*, vol. 9, pp. 21388-21394, 2021.
- [14] M. Belotti, N. Bozic, G. Pujolle, S.A. Secchi, "Vaemecum on Blockchain Technologies: When, Which and How" *IEEE Commun. Surv. Tutorials*, Vol. 21, pp 3796–3838, 2019.
- [15] Creative Commons, "Cryptocurrencies and National Security," Council on Foreign Relations, 28 February 2018. [Online] Available: <https://www.cfr.org/backgrounder/cryptocurrencies-and-nationalsecurity> Date Accessed 05/09/2021.
- [16] R. M. Bratspies, "Cryptocurrency and the Myth of the Trustless Transaction," *SSRN*, pp. 1-48, 2018.