Eldi-Naseni Journal of Digital Innovation And Contemporary Research In Science, Engineering and Technology (ENJDICRSET) ISSN: 3093-0626 VOL.1 ISSUE 1, December, 2025. available online at www.eldi.org.ng/publication/VOL1_ISSUE

EFFECTIVE SECURITY OF CYBERSPACE USING BLOCKCHAIN TECHNOLOGY TECHNIQUE

[1]Odachi Gabriel Nwabuonu and [2]Belodachi Kenechukwu
Sports University of Nigeria, Idumuje Ugboko, Delta State and Group Head, Digital Innovation, Fidelity Bank of Nigeria Plc, Lagos.
Odachygab@gmail.com and gabriel.odachi@uniniger.edu.ng

Abstract:

As the society is gradually becoming an information-based entity providing, to a very large extent, both public and commercial digital services to the people, Cyber Security risks are becoming more and more commonplace, despite various cyber security measures put in place to check cyber-attacks. The growing impact of cyber-attacks calls for new, creative and innovative solutions so as to mitigate the threats and inherent risks – hence the adoption of Blockchain Technology Approach. The main objective of this paper is to adopt a paradigm shift in cybercrime control as cyber-attacks have defied traditional method. The methodology adopted for this work include creation of decentralized database managed by multiple participants, recording of transactions with an immutable cryptographic signature called a hash, consensus mechanism and smart contract.

Key Words: Cryptographic, hash, blockcain, paradigm, cyberspace, consensus and smart, contract

I. Introduction

As the society is gradually becoming an information-based service culture providing, to a very large extent, both public and commercial digital services to citizens, Cyber Security risks are becoming more and more commonplace. Owing to its complexity, in terms of policies and technologies, Cyber Security is one of the major challenges of the contemporary world (Cyber Magazine , 2021). Risks which were once considered less likely to occur are now appearing all the more regularly. This trend shows the new forms of instruments and methods being used in attacks, as well as ever-increasing vulnerabilities and the higher motivation of the attackers. The growing impact of cyber-attacks calls for new, creative and innovative solutions so as to mitigate the threats and inherent risks.

Cyber Security spending has increased exponentially in the past decade, with no signs of slowing down. Worldwide, organizations plan to allocate more money running to trillion of dollars to protect themselves from online threats, according to one industry report.

Despite that staggering investment, criminal hackers are still exploiting both publicly known and unknown vulnerabilities, and intercepting devices, applications, and network communications. It was calculated that about 6 billion confidential files were stolen between 2017 and 2018(Shelke, 2023). In November, 2023 alone 13 countries recorded cyber-attacks and 24 industries were affected. Specific cyber-attacks on critical infrastructures and assets are enormous.

Cyber-attacks have continued to wreak havoc across all industries in 2024, resulting in substantial disruption to organizations and critical services. As with previous years, vast quantities of personal data have been stolen by hackers, often sold to other malicious actors or used to extort victims. (Coker, 2024)

These sophisticated assaults often outwit traditional security methods, including authentication, key management, cryptography, and privacy challenges. With a large percentage of employees

working from home- a work method rejuvenated by coronavirus pandemic, vulnerabilities are growing in new ways and cyber-attacks are growing in geometric progression.

In view of the above, it has become necessary for a paradigm shift from the traditional approach to cyber security to a new and dynamic method taking care of the vulnerabilities exploited by cyber criminals.

The current emerging paradigm for this decade could be the connected world of computing relying on blockchain cryptography (Swan, 2015).With revolutionary potential equal to that of the Internet, blockchain technology could be deployed and adopted much more quickly than the Internet was, given the network effects of current widespread global Internet and cellular connectivity.

Most blockchain solutions offer an immutable and enduring record of a transaction as it is hard for any trusted or untrusted source to change or modify. This presents a completely new level of security, privacy, and trust to our online world. A variety of uses, protocols, and standards make up the current blockchain ecosystem (Dhillon V., Metcalf D. and Hooper M. 2017).

A blockchain is a type of database quite different from other databases such as an SQL, oracle, etc which have someone in charge who can change the entries. Blockchain is different because nobody is in charge of it. It is run by the people who use it – the participants. No single person can change the contents. Blockchain is the technology that drives the crypto currency security.

A blockchain is basically a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain is made up of a number of transactions. Every time a new transaction is made on the blockchain, a record of that transaction is added to every participant's ledger. The decentralized database managed by multiple participants is known as Distributed Ledger Technology (DLT). Blockchain is a type of Distributed Technology in which transactions are recorded with an immutable cryptographic signature called a hash

The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value (Tapscott and Tapscott, 2018)

Shelke (2023) contended that Blockchain offers a different path towards greater security, one that is less traveled and not nearly as hospitable to cybercriminals. This approach reduces vulnerabilities, provides strong encryption, and more effectively verifies data ownership and integrity. It can even eliminate the need for some passwords, which are frequently described as the weakest link in cyber security.

II. Methodology

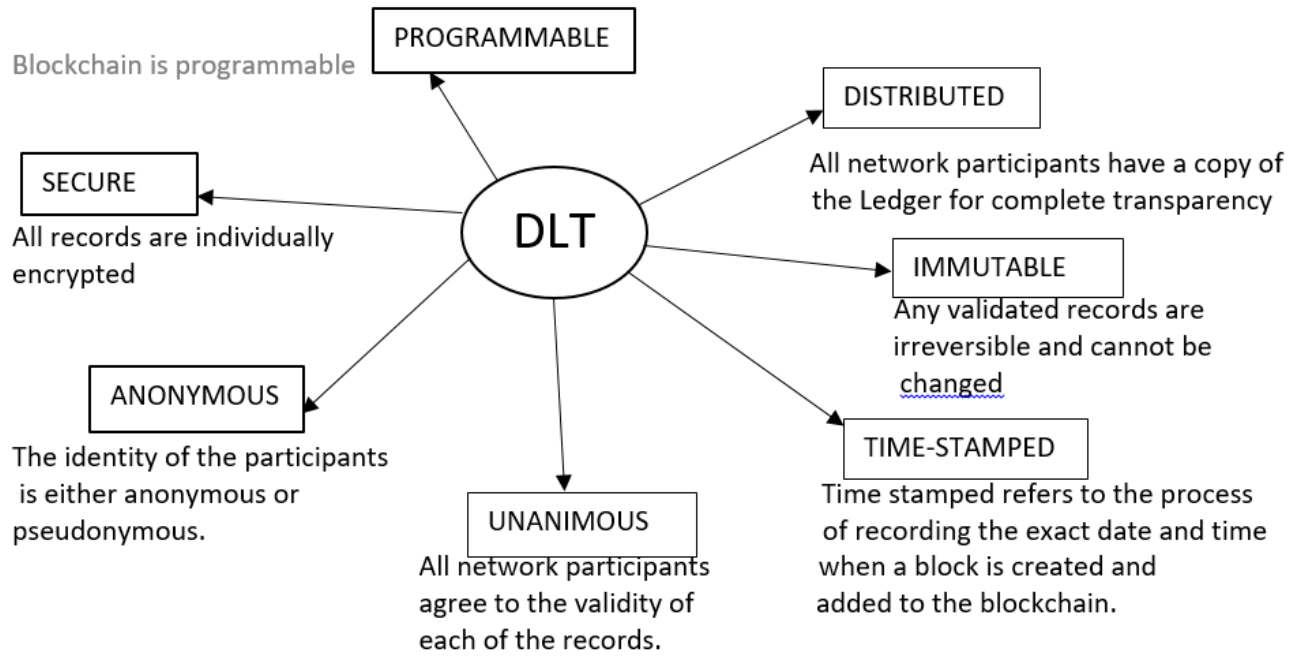
Blockchain technology employs a unique methodology that revolves around several key principles and processes. Understanding this methodology requires breaking it down into its fundamental components:

Distributed Ledger Technology (DLT)

At the core of blockchain is Distributed Ledger Technology, which allows data to be stored across multiple nodes in a network rather than being stored in a central location. Each participant in the network has access to the entire ledger, ensuring transparency and reducing the risk of data manipulation. This decentralization is crucial for enhancing security and trust among users.

In other words, Distributed Ledger Technology (DLT) is a system that allows multiple participants to access, validate, and update records in a shared database without the need for a central authority. This technology enables simultaneous access to data across a network of computers, known as nodes, each of which maintains its own copy of the ledger. The primary purpose of DLT is to enhance transparency, security, and efficiency in data management.

Properties of Distributed Ledger Technology (DLT)



Source: Adapted from Euromoney Learning, 2020)

Figure 1: Properties of Distributed Ledger Technology

III. Data Structuring in Blocks

Data are organized into blocks on blockchain. Each block contains a set of transactions or records, along with a unique cryptographic hash of the previous block, creating a chain of blocks (hence the name “blockchain”). This structure ensures that once data is added to the blockchain, it cannot be altered without changing all subsequent blocks, thereby maintaining integrity.

Fig 2: Blocks of data

Cryptographic Security
Blockchain uses advanced cryptographic techniques to secure data. Each transaction is encrypted and linked to previous transactions through hashing algorithms (such as SHA-256). This encryption ensures that only authorized users can access or modify their own data while keeping other information secure from unauthorized access.

Consensus Mechanisms
To validate new transactions and add them to the blockchain, consensus mechanisms are employed. These mechanisms ensure that all participants agree on the validity of transactions before they are recorded. Common consensus algorithms include Proof of Work (PoW), used by Bitcoin, and Proof of Stake (PoS), which is becoming increasingly popular due to its energy efficiency.
Proof of Work (PoW) - In PoW, miners compete to solve complex mathematical problems; the first to solve it gets to add a new block and is rewarded with cryptocurrency. Proof of Stake (PoS): In PoS, validators are chosen based on the number of coins they hold and are willing to "stake" as collateral.

Smart Contracts
A Smart Contract is not a written contract on paper of the traditional kind, nor is it simply an online contract. It is described as "smart" because it can do more than both of these paradigms, in the same way that a "smart phone" can do more than just making calls. It takes the form of computer code on a Distributed Ledger Technology (which can be a Blockchain but can also be another type of DLT such as Corda) and *executes itself* upon receipt of electronic data inputs. It effects an action on a DLT in a manner comparable to a formula in the cell of an Excel spreadsheet—it adjusts itself or transfers payment or other assets, monitors stock levels, or effects other actions automatically because that is what it is programmed to do (Corrales, Fenwick, Haapio, 2019)
In other words, Smart contracts are self-executing contracts with terms directly written into code on the blockchain. They automatically enforce and execute agreements when predetermined conditions are met, eliminating the need for intermediaries and increasing efficiency.

Ethereum is a decentralized global software platform that operates on blockchain technology. It enables the creation and execution of smart contracts—self-executing contracts with the terms of the agreement directly written into code. This functionality allows participants to transact without needing a trusted central authority, making it a significant advancement in blockchain technology.
The Ethereum blockchain consists of two main layers: the consensus layer and the execution layer. The consensus layer is responsible for validating transactions and maintaining the integrity of the blockchain, while the execution layer processes smart contracts and executes their code. This separation allows for greater efficiency and scalability within the network.

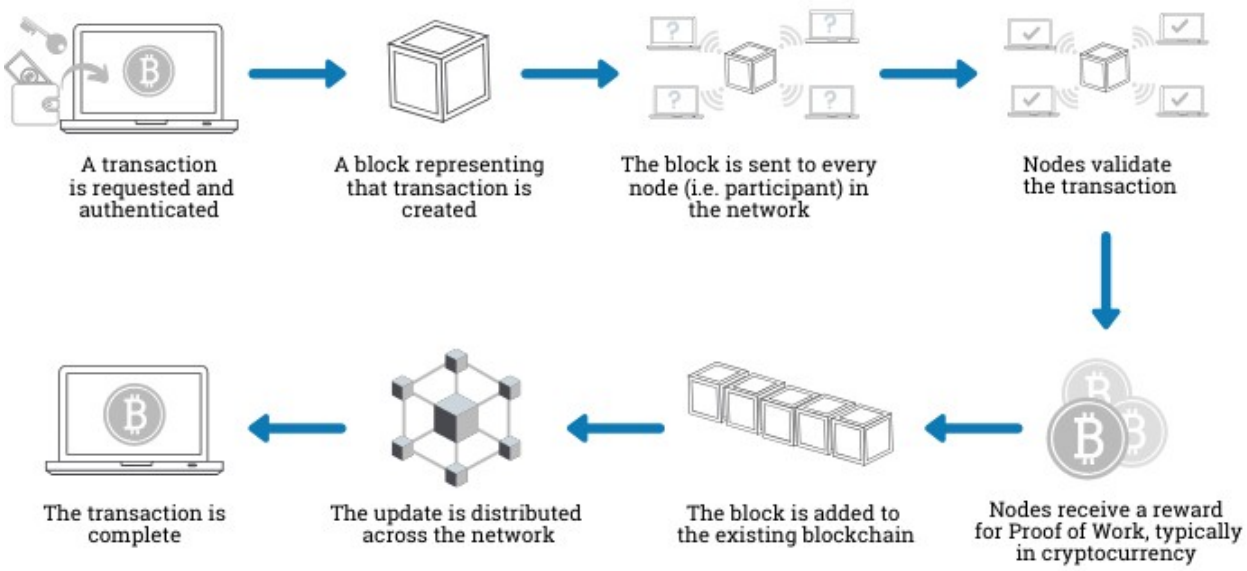
Transparency and Immutability
One of the most significant advantages of blockchain technology is its transparency; all transactions are recorded on a public ledger accessible by all participants in real-time. Additionally, once

information is added to the blockchain, it becomes immutable—meaning it cannot be changed or deleted—thus providing an auditable trail for all transactions. Immutability is one of the core characteristics of blockchain technology, referring to the property that once data has been recorded on a blockchain, it cannot be altered or deleted. This feature is achieved through cryptographic hashing and the structure of the blockchain itself. Each block in a blockchain contains a unique hash of the previous block, along with its own data and timestamp. This creates a chain of blocks that are linked together, making it extremely difficult to change any single block without altering all subsequent blocks.

Peer-to-Peer Network Architecture

Blockchain operates on a peer-to-peer network architecture where each participant (node) can communicate directly with others without needing an intermediary server. This architecture enhances resilience against failures or attacks since there is no single point of failure.

IV. How a Transaction Gets into a Blockchain with Reference to Bitcoin.



Source: (Euromoney learning, 2020)

Figure 3: How transactions get into the blockchain

The blockchain collects transaction information and enters it into a block, like a cell in a spreadsheet containing information. As soon as it is full, the information is run through an encrypted algorithm which creates a hexadecimal number called the hash. The hash is then entered into the following block header and encrypted with the other information in the block. This creates a series of blocks that are chained together.

Before a transaction is added to the blockchain it must be authenticated and authorized. Once the transaction is agreed between the users, it needs to be approved, or authorized, before it is added to

a block in the chain. Adding transaction to the blockchain will take the following processes as found in the diagram above.

In case of a public blockchain, the decision to add a transaction to the chain is made by consensus, meaning that the majority of "nodes" (or computers in the network) must agree that the transaction is valid. The people who own the computers in the network are motivated (rewarded) to verify transactions through a process known as 'proof of work'. Proof of Work requires the people who own the computers or the participants in the network to solve a complex mathematical problem to enable them add a block to the chain. Solving the problem is known as mining, and 'miners' are usually rewarded for their work in cryptocurrency. As more blocks are added to the chain, hacking becomes more difficult.

V. Security Features of Blockchain Technology

The following Security features make blockchain tick. These security features are derived from blockchain methodology.

Decentralized storage - A decentralized system in blockchain technology makes it impossible for data theft in the network. Any tampering with a block will lead to rejection by the network community, reducing the chances of hacking into the network.

Cryptography Technique – Blockchain transaction records are encrypted, which make them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record which is not an easy task.

Smart Contract – Smart contracts are digital contracts stored on a blockchain that are automatically executed when predetermined terms and conditions are met. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

There is trust and transparency because there's no third party involved, and because encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit.

Time – Stamped - Blockchain-based time stamping is a method of verifying the exact time and date at which a certain digital event took place. A blockchain-based time stamping system can record timestamps on data, documents, and transactions, providing proof of their existence and state at a particular point in time. This form of time stamping uses cryptographic algorithms to provide a secure, verifiable, and tamper-proof timestamp. Blockchain's decentralized nature further ensures that these timestamps cannot be changed or manipulated by any single entity, thereby enhancing the integrity of the time stamped data.

Benefits of Using Blockchain in Cyber Security

Using Blockchain in Cyber Security has the following benefits

i. **Customer Trust:** Data transparency and privacy are achieved using blockchain. This helps to gain customer trust. It enables the data owners to manage and control their data securely.
ii. **Chance of Failure is Rare:** As discussed, blockchain technology is a decentralized system that offers more resilience than traditional systems. Thus, a single node failure does not affect the entire blockchain system.
iii. **Safe Data Transfers:** Public Key Infrastructure (PKI) is provided by blockchain technology which helps authenticate data during transfers. It makes for fast and secure transaction of data.
iv. **Smart Contracts** are the best examples that provide automatic execution of agreements between parties. This removes manipulation as there is no third party in any transaction
v. **Secure Data Storage and Processing:** The records under blockchain are immutable, transparent, and non-removable.
vi. **User Confidentiality:** Blockchain technology offers high user confidentiality using Cryptography to authenticate the users for accessing the data.

VI. Conclusion

The authors, by this article, have highlighted the need to explore other techniques rather than rely on the traditional methods of tackling cyber security. This is because, cyber security issues are approaching explosive dimension as no day passes without data breach or hacking news – current cyber security measures put in place notwithstanding. We need to give cyber criminals a very hot chase because of the enormous benefits we derive from cyberspace. Blockchain Technology has shown to a reasonable extent resilient to tampering. It is the security measure that drives crypto currency; for instance bitcoins can't be faked, hacked or double spent. This technology can be applied to other areas such as financial exchange, real estate management, voting system, healthcare record management, supply chain management, intellectual property protection, secure personal information management etc.

Blockchain is not projected here as a water-tight security measure for data and other critical assets in cyberspace, but it could be applied where best-fitted in addition to other cutting edge technologies that are cyber security oriented.

References

Coker J. (2024). Top 10 Cyber-Attacks of 2024. (https://www.infosecurity-magazine.com/news-features/top-cyber-attacks 2024/#:)Corrales M, Fenwick, M and Haapio H (2019). Legal Tech, Smart Contracts and Blockchain, Fukuoka City, Springer.Cyber Magazine (2021).The history of cyber security (https://cybermagazine.com/cyber-security/history-cybersecurity)

Dhillon V., Metcalf D. and Hooper M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You, Florida, Apress.

Euromoney Learning (2020). What is blockchain? (https://wwww. Euromoney.com/learning/blockchain-explained/what-is-blockchain)

Samreen N. F., Alalfi M. H. (2023). An empirical study on the complexity, security and maintainability of Ethereum-based decentralized applications (DApps), journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Shelke Y. (2023). Rethinking Cybersecurity Through Blockchain

https://www.infosys.com/insights/cyber-security/cybersecurity-blockchain.html
Swan, M (2015). Blockchain: Blueprint for a New Economy, Tokyo, O'Reilly Media, Inc.
Tapscott D. and Tapscott A. (2018). Blockchain Revolution, New York City, Penguin Random House