ALTHASH
EDUCATION

CYBERSECURITY A KEY NECESSITY TO THE ADVANCEMENT OF BLOCKCHAIN AND CRYPTOCURRENCY

BY

ALOKAM CHIAMAKA PRINCE
AJIBOYE AYOMIKUN
DAVID OJO
IKWA FRANCIS
GOODNESS NWACHUKWU

NIGERIA

A CAPSTONE PROJECT
SUBMITTED TO THE FACULTY OF BLOCKCHAIN STUDIES AND ARTIFICIAL INTELLIGENCE
AT THE ALTHASH UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE COLLEGIATE OF SCIENCE IN DECENTRALIZED APPLICATIONS

CHICAGO, ILLINOIS

ABSTRACT

Cybersecurity in simple terms means the security of the cyberspace, however the blockchain space which is a welcomed development is not left out In the need to be incorporated with cybersecurity, in recent times we have heard of several exchanges been hacked and people's funds stolen…this and many other reasons are the need for which this work tends to address the objective while proposing in the work ”CYBERSECURITY A KEY NECESSITY TO THE ADVANCEMENT OF BLOCKCHAIN AND CRYPTOCURRENCY"

TABLE OF CONTENT

CHAPTER ONE

(INTRODUCTION)

What is Cybersecurity?

Cybersecurity refers to the practice of protecting computer systems, networks, and sensitive data from unauthorized access, theft, damage, or disruption. It encompasses a range of technologies, processes, and practices designed to safeguard information and prevent it from being compromised in any way. Cybersecurity is crucial in today's digital world, where cyber threats are constantly evolving and becoming more sophisticated.

CHAPTER TWO

(STATEMENT OF PROBLEM)

Challenges problems of non application of cyber security in blockchain

The non-application of cyber security in blockchain can pose several challenges, some of which are:

1. Theft of cryptocurrencies: Blockchain technology is commonly used for storing and transferring cryptocurrencies. If cyber security measures are not implemented correctly, hackers can exploit vulnerabilities in the blockchain network to steal cryptocurrencies from users' wallets. This can lead to financial losses for individuals and organizations.

2. Smart contract vulnerabilities: Smart contracts are self-executing agreements that run on the blockchain network. If these contracts are not designed securely or are not audited properly, they can contain vulnerabilities that can be exploited by hackers. This can lead to the loss of funds or sensitive data.

3. Network attacks: Blockchain networks are susceptible to various types of network attacks, including Distributed Denial of Service (DDoS) attacks and 51% attacks. A DDoS attack can overload the network with traffic, causing it to slow down or even crash. A 51% attack occurs when a group of miners controls more than 50% of the network's computing power, enabling them to manipulate transactions or even reverse them.

4. Lack of regulatory compliance: Blockchain technology and cryptocurrencies are largely unregulated in many countries. However, there are some jurisdictions that have begun to regulate these technologies. Failure to comply with regulatory requirements can result in legal action, fines, or other penalties.

Overall, the non-application of cyber security in blockchain can lead to significant financial losses, reputational damage, and legal consequences. It is important for individuals and organizations to implement appropriate cyber security measures to protect their blockchain assets and data.

CHAPTER THREE

(STATEMENT OF SOLUTION)

Importance of Cybersecurity in Blockchain

Blockchain technology is a decentralized, distributed ledger that allows users to securely record, store, and transfer data without the need for intermediaries. It is a revolutionary technology that has the potential to transform various industries, including finance, healthcare, and supply chain management. However, the same characteristics that make blockchain so powerful also make it vulnerable to cyber attacks.

One of the key benefits of blockchain technology is its ability to provide data immutability and transparency. However, this also means that once data is added to the blockchain, it cannot be altered or deleted. Therefore, if a cyber attack is successful in compromising the integrity of the blockchain, the consequences can be severe.

Another threat to blockchain is the risk of 51% attacks. In a blockchain network, consensus is achieved through a process called mining, where nodes compete to solve cryptographic puzzles. If one entity controls more than 50% of the network's computing power, they can potentially rewrite the blockchain's transaction history and double-spend coins.

NOTE:

- the 51% attack scenario isnt general for all approaches (ie the HTMLcoin is PoS and PoW, so even if you have a 51% of PoW strength you did need 67% of stake volume as well to rly attack also. when all existing PoW miners act legit you need the same amount plus an additional 1% which means 102% of the existing miners strengths, in case of HTMLcoin you did need to hold 67% of the staking volume as well) But yes BTC is for a 51% attack you did need 102% of the existing computational power only.

Cybersecurity is crucial for the advancement of blockchain and cryptocurrencies because it helps to mitigate these risks and ensure the integrity and security of the blockchain. Some of the key benefits of cybersecurity in blockchain include:

a) Protection against hacks and cyber attacks: Cybersecurity measures such as encryption, multi-factor authentication, and firewalls can help to prevent unauthorized access to the blockchain and protect against cyber attacks.

b) Ensuring data integrity: Cybersecurity measures can help to prevent data tampering and ensure the integrity of the blockchain.

c) Maintaining network availability: Cybersecurity measures can help to prevent denial-of-service attacks, which can disrupt the availability of the blockchain network.

d) Protecting user privacy: Cybersecurity measures can help to protect the anonymity and privacy of blockchain users.

CHAPTER FOUR

Effective Use of Cybersecurity

To effectively use cybersecurity in blockchain, it is important to implement a comprehensive cybersecurity strategy that includes the following:

a) Risk assessment: Conduct a thorough risk assessment to identify potential threats and vulnerabilities in the blockchain network.

b) Security controls: Implement appropriate security controls such as encryption, multi-factor authentication, and firewalls to protect against cyber attacks.

c) Regular testing and monitoring: Regularly test and monitor the blockchain network to identify and address any security vulnerabilities.

d) Incident response plan: Develop an incident response plan to quickly and effectively respond to any security incidents or breaches.

e) User education and awareness: Educate users on cybersecurity best practices and raise awareness of the potential risks and threats associated with blockchain and cryptocurrencies.

f) Compliance with regulations: Ensure compliance with relevant regulations and standards such as the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS).

CHAPTER FIVE

Unique features of cybersecurity in blockchain

Blockchain technology has brought about a paradigm shift in the way we think about data storage and security. Unlike traditional databases, which rely on central authorities to manage and secure data, blockchain networks are decentralized and distributed, which makes them inherently more secure. However, there are still unique cybersecurity challenges that must be addressed in order to keep blockchain networks safe and secure.

1. Distributed network architecture

One of the most unique features of blockchain technology is its distributed network architecture. Instead of relying on a single central authority to manage and secure data, blockchain networks are made up of a decentralized network of nodes that work together to verify and validate transactions. This distributed architecture makes it more difficult for

hackers to attack the network, as they would need to compromise a large number of nodes in order to gain control of the network.

2. Immutable ledger

Another unique feature of blockchain technology is its immutable ledger. Once a transaction has been recorded on the blockchain, it cannot be altered or deleted. This makes it difficult for hackers to manipulate data on the network, as any attempt to tamper with the ledger would be immediately detected by other nodes on the network. This also means that data stored on the blockchain is highly resistant to data loss or corruption.

3. Smart contracts

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code.

They are a unique feature of blockchain technology that allows for automated and trustless transactions to occur. However, smart contracts can also introduce new cybersecurity risks, as they are vulnerable to coding errors and exploits. If a smart contract is not properly coded and audited, it can be vulnerable to hacking attempts, which can result in significant financial losses.

4. Public and private keys

In blockchain networks, users are identified by public and private keys, which are used to sign transactions and prove ownership of assets. Public keys are visible to everyone on the network, while private keys are kept secret and used to sign transactions. If a user's private key is compromised, their assets can be stolen or transferred without their knowledge or consent. It is therefore essential for users to keep their private keys secure and not

share them with anyone.

5. Consensus mechanisms

Consensus mechanisms are used in blockchain networks to ensure that all nodes on the network agree on the state of the ledger. There are several different consensus mechanisms used in blockchain networks, including proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS). Each consensus mechanism has its own unique cybersecurity risks and vulnerabilities that must be addressed in order to keep the network secure.

CHAPTER SIX

How cybersecurity solve real-time problems in blockchain

Cybersecurity plays a critical role in ensuring the safety and integrity of blockchain networks. By implementing robust security measures, developers and users can help to prevent hacking attempts, data breaches, and other cybersecurity threats. In this article, we will explore how cybersecurity can solve real-time problems in blockchain networks.

1. Preventing 51% attacks

One of the most significant cybersecurity threats facing blockchain networks is the 51% attack. This occurs when a single entity or group of entities gains control of 51% or more of the computing power on a blockchain network. With this level of control, they can manipulate transactions and potentially double-spend coins. To prevent 51% attacks, blockchain networks can implement consensus mechanisms that require a certain level of computing power to participate in the validation process. Additionally, regular audits and testing can help to identify vulnerabilities that could be exploited by malicious actors.

2. Protecting against smart contract vulnerabilities

Smart contracts are a powerful feature of blockchain technology, but they also introduce new cybersecurity risks. If a smart contract is not properly coded or audited, it can be vulnerable to hacking attempts, which can result in significant financial losses. To address this issue, developers can implement best practices for smart contract development, such as code reviews, testing, and auditing. Additionally, user education and awareness campaigns can help to prevent users from unknowingly engaging with malicious smart contracts.

3. Ensuring secure key management

In blockchain networks, users are identified by public and private keys, which are used to sign transactions and prove ownership of assets. If a user's private key is compromised, their assets can be stolen or transferred without their knowledge or consent. To prevent this, users must be educated on best practices for key management, such as keeping private keys secure and not sharing them with anyone. Additionally, blockchain networks can implement multi-factor authentication and other security measures to prevent unauthorized access to user accounts.

4. Protecting against DDoS attacks

Distributed denial of service (DDoS) attacks are a common cybersecurity threat facing blockchain networks. These attacks involve flooding a network with traffic to overwhelm servers and disrupt service. To prevent DDoS attacks, blockchain networks can implement measures such as rate limiting, traffic filtering, and load balancing.

Additionally, regular testing and auditing can help to identify vulnerabilities that could be exploited by attackers.

5. Ensuring secure network communication

In a decentralized network like a blockchain, communication between nodes is critical for maintaining the integrity of the network. However, this communication can also be a vulnerability if it is not properly secured. To prevent attacks on network communication, blockchain networks can implement encryption and other security measures to protect data in transit. Additionally, regular security audits and testing can help to identify vulnerabilities that could be exploited by attackers.

CHAPTER SEVEN

MISSION VISION AND OBJECTIVS

Vision: Our vision is to become the leading provider of blockchain-based solutions that improve cybersecurity and online information encryption/cryptography in the cyber space. We aim to revolutionize the blockchain space by leveraging cybersecurity to enhance more secured blockchain activities and transactions.

Mission: Our mission is to develop and deliver a secure, efficient, and transparent blockchain platforms that leverages cybersecurity to enhance information and transactions traceability. We strive to provide a solution that addresses the challenges faced by the CRYPTOCURRENCY and blockchain users while adhering to ethical and legal requirements.

Goals: Our primary goal is to develop a minimum viable product (MVP) of the blockchain-based platform within 12 months. We aim to test and validate the MVP with various developers and smart contract coders to gather feedback for further improvements. Additionally, we aim to develop a scalable and modular platform that can be customized to meet the specific needs of developers and stakeholders. We also aim to ensure ethical and legal compliance with relevant regulations,and provide ongoing support and maintenance to ensure the platform's stability, reliability, and security.

Objectives: To achieve our goals, we have identified the following objectives:

- Identify the key requirements and challenges of the blockchain technology related to cybersecurity and transaction encryption.
- Design a blockchain-based solution that meets these requirements and addresses the challenges of cybersecurity.

- Develop and deploy the MVP of the platform using agile methodologies to ensure efficiency and flexibility.
- Test and validate the MVP with blockchain developers, and gather feedback for further improvements.
- Implement features and functionality based on user feedback and market demand to ensure the platform is relevant and meets the changing needs of the blockchain industry.
- Ensure ethical and legal compliance with relevant regulations, to ensure the privacy and security of peoples funds,transactions and data in the blockchain space.
- Provide ongoing support and maintenance to ensure the platform's stability, reliability, and security.
- Continuously improve the platform based on user feedback and emerging technologies, to ensure that the platform remains at the forefront of innovation and is always providing the best solutions for the blockchain innovators.

By focusing on these objectives, we believe that we can achieve our goals and mission of developing a secure, efficient, and transparent platform that leverages cybersecurity to enhance blockchain innovations and and transactions in the blockchain technology. We are committed to delivering a solution that improves CRYPTOCURRENCY trading and custody outcomes and transactions efficiency/security while adhering to ethical and legal requirements.

CHAPTER EIGHT

(TOKEN NAME)

The token name **"ACFNI"** for **"APPLIED CYBERSECURITY FINANCIAL NETWORK INITIATIVE"** is a suitable and relevant name for the proposed capstone project for several reasons.

Firstly, the token name emphasizes the financial aspect of the project, indicating that it aims to develop a solution that is not only efficient but also cost-effective. The name "Financial Network" suggests that the platform will facilitate secure and efficient financial transactions in the blockchain space

Secondly, the name "Applied" indicates that the project aims to develop a practical solution that can be implemented in real-world scenarios, rather than just a theoretical concept. This aligns with the project's objective of creating a blockchain technology which is born out of cybersecurity

Lastly, the name "financial network initiative" indicates that the platform will provide a secure and efficient network for managing blockchain data. This aligns with the project's goal of developing a solution that enhances patient secured blockchain operations and transactions traceability through cybersecurity, two critical aspects that require secure and efficient data management.

The token name "ACFNI" effectively communicates the project's focus on creating a secure, efficient, and cost-effective means of carrying out blockchain transactions

CHAPTER NINE

(TOKEN TICKER)

ACFNI - As a student presenting my capstone project, I have decided to use the token ticker "ACFNI". The acronym stands for "Applied Cybersecurity Financial Network Initiative". I believe that this token ticker accurately reflects the purpose of my project, which is to leverage blockchain technology to create a secure, efficient, and transparent platform for managing secured blockchain operations and transactions through cybersecurity.

The token ticker "ACFNI" emphasizes our commitment to building a {trust/service/credentials} network that can enhance data management and fund security in the blockchain space, ultimately leading to fewer or no blockchain wallets or exchanges hacking. We believe that this token ticker will help to differentiate our project from others in the blockchain and cyber space, while also conveying our vision and mission to potential investors and stakeholders.

CHAPTER TEN

(TOKEN MAXIMUM SUPPLY)

500, 000, 000, ACFNI: As per the recommendation, a minimum of 500 million tokens is recommended to reach a larg audience. In addition, the project's goal is to create a secure, efficient, and transparent platform for managing blockchain data and transactions, specifically related to transactions traceability and funds security. The platform will cater to a vast and complex blockchain industry, with numerous stakeholders, such as developers, regulators, and CRYPTOCURRENCY traders.

A larger token supply of 500,000,000, ACFNI tokens would provide sufficient room for broader adoption and greater liquidity, which is important for achieving the project's long-term goals. It will allow more users to participate in the platform, improving its usability and efficiency. The large token supply also ensures that the platform can scale to meet the growing demand of the Cybersecurity proofed blockchain technology over time.

Moreover, the large token supply provides ample room for token distribution, incentivization, and rewards, which can further drive adoption and engagement with the platform. It can also enable the project to create a sustainable ecosystem with active participation from all stakeholders.

The size of 500,000,000,ACFNI tokens is justified based on the project's goal of creating a secure, efficient, and transparent platform for managing blockchain operations,data's and transactions, the recommendation for a minimum of 500 million tokens to reach a broader audience, and the need for a large token supply to support broader adoption, liquidity, and ecosystem building

CHAPTER ELEVEN

(BUDGET ALLOCATION)

- 40% - Project Development
- 25% - Team Salary
- 15% - Marketing
- 19% - Bounty
- 10% - Faucets and giveaways to reward community members

The budget figures proposed for a blockchain project are justifiable based on the following considerations:

1. Project Development: Allocating 40% of the budget to project development is essential as it covers the research, development, and implementation of the project. Blockchain technology is complex and requires significant expertise, time, and effort to develop and implement successfully. A considerable portion of the budget must be allocated to this area to ensure that the project is developed to the highest standards.

2. Team Salary: Allocating 25% of the budget to the team's salary is vital as it ensures that the project is supported by a talented and dedicated team that can drive its success. Blockchain development requires specialized skills, and attracting and retaining top talent can be expensive. Allocating a significant portion of the budget to team salaries ensures that the project has the necessary resources to attract and retain the best talent.

3. Marketing: Allocating 15% of the budget to marketing is critical to ensure that the token gains sufficient exposure to reach the target audience. Effective marketing strategies are essential for driving adoption and building a strong community around the project. Allocating enough budget to promote the token through various channels, including social media, advertising, and public relations, will ensure that the project is visible and reaches the intended audience.

4. Bounty: Allocating 10% of the budget to bounty programs can help incentivize community participation, encourage community engagement, and drive adoption. Bounty programs can reward community members for contributing to the project's development, such as bug reporting, testing, and translations, among others. This allocation will help attract and retain a vibrant and active community around the project.
5. Faucets and giveaways: Allocating 10% of the budget to faucets and giveaways to reward community members is an excellent way to incentivize community participation and drive adoption. By providing community members with incentives, such as free tokens or access to unique features, the project can create a strong community that is loyal and committed to its success.

The proposed budget allocation is justifiable as it considers the various aspects required for the successful development and implementation of a blockchain project. The allocation to project development, team salaries, marketing, bounty, and faucets and giveaways are crucial to ensure that the project is developed to the highest standards, has the best talent, gains sufficient exposure, and has a strong and active community.

CHAPTER TWELVE

(TOKEN SLOGAN)

"Securing blockchain technology, improving the future of money"

This slogan highlights the two main goals of the project: to create a secure technology for managing blockchain data and to improve operations by enhancing transactions traceability through cybersecurity. The word "Securing" emphasizes the importance of data security, while "improving the future of money" highlights the project's focus on improving financial outcomes through secured blockchain data/transaction management. Overall, the slogan communicates the project's commitment to creating a solution that benefits both the blockchain developers and blockchain users.

CHAPTER THIRTEEN

(TOKEN LAUNCH DATE)

Launch Date: October 17, 2025

The ACFNI token is expected to launch on October 17, 2025, based on the projected timeline for the development and testing of the blockchain-based platform. The project team plans to develop a minimum viable product (MVP) of the platform within 8 months, starting from october 17,2024.

Once the MVP is developed, the team will test and validate it with blockchain developers and blockchain users, and gather feedback for further improvements. This testing and validation process is expected to take around 3 months, which brings us to July 2025.

Based on the feedback received, the team will then work on developing a scalable and modular platform that can be customized to meet the specific needs of blockchain developers, users and stakeholders. This development process is expected to take around 4 months, which brings us to October 2025, the proposed launch date for the ACFNI token.

Launching the token in October 2025 will allow the project team to leverage the upcoming holiday season and end-of-year financial planning for blockchain developers, potentially increasing adoption and engagement with the platform. It also provides ample time for marketing and outreach efforts, ensuring that the project reaches its target audience and achieves its goals

CHAPTER FOURTEEN

(OTHER USE CASE OF THE TOKEN)

ACFNI **token can serve as a voting utility in a DAO (decentralized autonomous organization) by allowing token holders to participate in decision-making processes related to the development of tools for transparency and documentation facilities. Here's how it can work:**

1.ACFNI **Token holders are given voting rights proportional to the number of tokens they hold. This can be implemented through a smart contract on the blockchain.**

2. The ACFNI **DAO proposes potential projects related to transparency and documentation facilities, such as developing neat frontends, stats, and other gadgets. The DAO can also propose budgets for these projects.**

3.ACFNI **Token holders can then vote on which projects to pursue and how much funding to allocate to each project.**

4. Once the votes are tallied, the ACFNI **DAO can allocate resources to the projects that received the most votes and funding.**

5. As the projects are developed, they can be released to the public and the DAO can continue to gather feedback from the community through surveys and other mechanisms.

By using ACFNI **token as a voting utility, the DAO can ensure that decisions are made democratically and that token holders have a say in how resources are allocated. This can help build a community of users who are invested in the success of the DAO's projects and can lead to greater adoption of the tools and services developed by the DAO.**

CONCLUSION

cybersecurity is a key necessity for the advancement of blockchain and cryptocurrencies. Without effective cybersecurity measures in place, the potential risks and threats associated with blockchain and cryptocurrencies can compromise their integrity and security. It is important to implement a comprehensive cybersecurity strategy that includes risk assessment, security controls, regular testing and monitoring, incident response planning, user education and awareness

conclusively, while blockchain technology offers many unique security benefits, it also introduces new cybersecurity risks and challenges that must be addressed. To ensure the security of blockchain networks, it is essential for developers and users to understand these risks and take appropriate measures to mitigate them. This includes implementing best practices for smart contract development, keeping private keys secure, and regularly auditing the network for vulnerabilities. By doing so, we can help

TEAM OATH

We, the members of this team, pledge to work together with respect and integrity towards our common goals. We will communicate openly and honestly, listen actively, and support each other's ideas. We will hold ourselves accountable for our actions and decisions, and strive for excellence in everything we do. We will embrace diversity and inclusivity, recognizing that our differences make us stronger. We will always act with the best interests of the team in mind, putting aside personal agendas and egos. We commit to working tirelessly towards our shared vision, and to celebrating our successes together as a team.