

**A REPORT
ON
PRODUCT & ECOSYSTEM DEVELOPMENT
LEAD INTERN**

Submitted by,

Mr. Mohammed Faizan - 20211CCS0041

Under the guidance of,

Dr. N Syed Siraj Ahmed

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING (CYBER SECURITY)

At



PRESIDENCY UNIVERSITY

BENGALURU

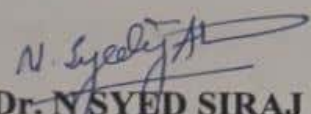
MAY 2025

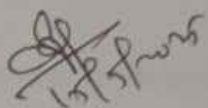
PRESIDENCY UNIVERSITY

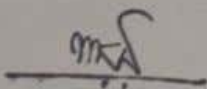
PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

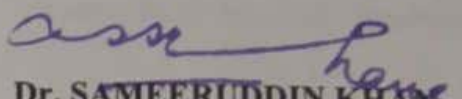
CERTIFICATE

This is to certify that the Internship report “**PRODUCT AND ECOSYSTEM DEVELOPMENT LEAD INTERN**” being submitted by “**MOHAMMED FAIZAN**” bearing roll number “**20211CCS0041**” in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in **Computer Science and Engineering (Cyber Security)** is a bonafide work carried out under my supervision.


Dr. N. SYED SIRAJ AHMED
Associate Professor
PSIS
Presidency University


Dr. S. P. ANANDRAJ
Professor & HoD
PSCS
Presidency University


Dr. MYDHILI NAIR
Associate Dean
PSCS
Presidency University


Dr. SAMEERUDDIN KHAN
Pro-Vice Chancellor - Engineering
Dean – PSCS / PSIS
Presidency University

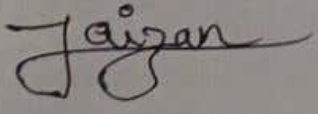
PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

I hereby declare that the work, which is being presented in the report entitled “**PRODUCT & ECOSYSTEM DEVELOPMENT LEAD**” in partial fulfillment for the award of Degree of **Bachelor of Technology in Computer Science and Engineering (Cyber Security)**, is a record of my own investigations carried under the guidance of **DR. N SYED SIRAJ AHMED, Associate Professor, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

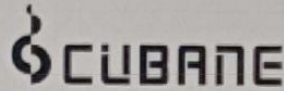
I have not submitted the matter presented in this report anywhere for the award of any other Degree.

<p>MOHAMMED FAIZAN 20211CCS0041</p> 	<p>Name, Roll No and Signature of the Student</p>
---	--

INTERNSHIP COMPLETION CERTIFICATE

Website : <https://cubane.space/>

Address :
A-131, Prem Nagar-II,
Delhi, India - 110041



(A PRODUCT OF JITOSHI TECHNOLOGY PRIVATE LIMITED)

Date : 5th May 2025

CERTIFICATE OF INTERNSHIP

This is to certify that **Mr. Mohammed Faizan** has successfully completed his internship at **Jitoshi Technology Pvt. Ltd.**, serving as a **Product & Ecosystem Development Lead Intern** from **1st February 2025 to 3rd May 2025**.

During his internship, he contributed to the development of our product **Cubane**, with his major project focused on the ongoing research and documentation of our proprietary **Cubic Consensus Mechanism (CCCM)**. This work involved exploring technologies such as **FHE, zk-STARKs, PoET, and PoS**. In addition, he worked as part of a collaborative team on tasks including writing and deploying the **CUBS Token smart contract**, and forming strategic technology partnerships with companies such as **Paycio, Insight Genesis, Decatron, Meet Finance, and 0xTeam Space**.

He showed strong initiative, technical skills, and a clear understanding of blockchain systems, making valuable contributions to our development efforts.

We appreciate his efforts and wish him success in all his future endeavors.

For JITOSHI TECHNOLOGY PVT LTD

Director

Jitesh Kumar Thakur
CEO, Jitoshi Technology Pvt. Ltd.

Email : info@cubane.space

Phone : +91 81788 01839

ABSTRACT

This internship report provides a comprehensive overview of the three-month internship undertaken at **Jitoshi Technology Private Limited**, focusing on its flagship blockchain project, **Cubane**. As a Product and Ecosystem Development Intern, I was actively involved in understanding and documenting the **Cubane Cubic Consensus Mechanism (CCCM)**—a unique, modular Layer-1 blockchain protocol designed to offer high levels of scalability, privacy, and decentralization. Throughout my internship, I worked on a number of areas like learning about the technical architecture of CCCM, becoming familiar with privacy-focused tools like **zkSNARKs** and **zkSTARKs**, and contributing to system enhancements. I was also part of a collaborative team which worked on tasks such as writing and deployment of CUBS Token smart contract, and forming strategic partnerships with tech companies.

The report I worked on looks at how Cubane's consensus mechanism uses zero-knowledge proofs and a step by step process starting with initiation, then proof generation, validation, and finally compression to create a modern blockchain setup tailored for SaaS and enterprise needs. I gained knowledge about the design of transactions, node voting, block validation utilising timestamps, and the application of cryptographic proofs by examining the literature, various methodologies including previous research of Cubane

This internship helped me connect what I've learned in university with real-world applications. It gave me hands-on experience with blockchain, cryptographic systems, and a learning of working with a team on complex projects.

ACKNOWLEDGEMENTS

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin Khan**, Pro-VC - Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair**, Presidency School of Computer Science and Engineering, Presidency University, and **Dr. S. P Anandraj**, Head of the Department, Presidency School of Computer Science and Engineering, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. N Syed Siraj Ahmed**, Associate Professor and Reviewer **Dr. Nagaraja S.R.**, Associate Professor, Presidency School of Computer Science and Engineering, Presidency University for their inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the internship work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 Internship/University Project Coordinator **Mr. Md Ziaur Rahman** and **Dr. Sampath A K**, department Project Coordinators **Dr. Sharmasth Vali Y.** and Git hub coordinator **Mr. Muthuraj**.

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

MOHAMMED FAIZAN

LIST OF TABLES

Sl. No.	Table Name	Table Caption	Page No.
1	Table 2.4.1	List of Papers referred for Literature Survey.	5

LIST OF FIGURES

Sl. No.	Figure Name	Caption	Page No.
1	Figure 7.2.1	Gantt Chart	21

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	I
	ACKNOWLEDGMENT	ii

1.	INTRODUCTION	1
	1.1 GENERAL	1
	1.2 INTERNSHIP CONTEXT	2
2.	LITERATURE REVIEW	3
	2.1 Emerging Consensus Models in Blockchain	3
	2.2 The Role of Privacy in Blockchain: ZKPs and FHE	3
	2.3 The Need for Modular, Scalable, and Secure Infrastructure	4
	2.4 Conclusion	4
3.	RESEARCH GAPS OF EXISTING METHODS	11
	3.1 Limitations of Traditional Consensus Mechanisms	11
	3.2 Gaps in Privacy and Confidentiality	11
	3.3 Lack of Modularity and Adaptability in Blockchain Design	12
	3.4 Summary	12
4.	PROPOSED METHODOLOGY	13
	4.1 Overview of Cubane Cubic Consensus Mechanism (CCCM)	13
	4.2 Layered Architecture of CCCM	13

	4.2.1 Transaction Layer (Transaction Nodes)	13
	4.2.2 Privacy Layer (ZK Layer)	13
	4.2.3 Validation Layer	14
	4.2.4 zkCompression Layer	14
	4.3 Key Innovations of CCCM	15
	4.4 Summary	15
5.	OBJECTIVES	16
	5.1 Technical Objectives	16
	5.2 Research-Oriented Objectives	16
	5.3 Product & Ecosystem Objectives	16
	5.4 Strategic Alignment Objective	17
6.	SYSTEM DESIGN AND IMPLEMENTATION	18
	6.1 Overview of the CCCM Architecture	18
	6.2 Transaction Node Layer	18
	6.3 ZK Layer Implementation	18
	6.4 Validation Layer Architecture	19
	6.5 zKCompression Layer Design	19
	6.6 Reward Mechanism Integration	20
	6.7 Implementation Summary	20
7.	TIMELINE FOR EXECUTION OF PROJECT(GANTT CHART)	21

	7.1 Project Timeline Overview	21
	7.2 Gantt Chart	21
8.	OUTCOMES	23
	8.1 Technical Outcomes	23
	8.2 Strategic and Ecosystem Contributions	23
	8.3 Personal and Professional Growth	24
	8.4 Summary	24
9.	RESULTS AND DISCUSSIONS	25
	9.1 Technical Results	25
	9.2 Discussion on Challenges and Solutions	25
	9.3 Validation of Results	26
	9.4 Alignment with Internship Objectives	26
	9.5 Summary	26
10.	CONCLUSION	27
	REFERENCES	28
	APPENDIX A : PSEUDOCODE	30
	APPENDIX B : SCREENSHOTS	31
	APPENDIX C : ENCLOSURES	35
	SUSTAINABLE DEVELOPMENT GOALS	36

Chapter 1

INTRODUCTION

1.1 General

Cubane, a flagship product of *Jitoshi Technology Private Limited*, is revolutionizing the way businesses interact with decentralized technologies. Positioned as a SaaS-oriented Layer-1 blockchain platform, Cubane bridges the gap between enterprise software needs and blockchain capabilities. Unlike traditional blockchain networks, Cubane incorporates a modular, service-oriented model that caters to sector-specific challenges—particularly in insurance, media, and intellectual property rights (IPR).

At the core of Cubane lies the **Cubic Consensus Mechanism (CCCM)**, an advanced architectural innovation that facilitates parallel transaction processing. This mechanism integrates modern cryptographic standards such as **Fully Homomorphic Encryption (FHE)** and **Zero-Knowledge Proofs (ZKPs)** to provide both scalability and privacy. Cubane is capable of processing thousands of transactions per second with minimal latency, making it one of the most robust platforms in the decentralized space.

The platform also features a **no-code development environment** and **multi-language support**, making it accessible even to non-technical users. These attributes not only enhance user experience but also lower the barrier to entry for organizations looking to adopt blockchain technology.

1.2 Internship Context

This report covers the work I carried out during my internship at Jitoshi Technology Private Limited, where I worked as a **Product and Ecosystem Development Lead Intern** for Cubane. My role was versatile and involved both technical and strategic responsibilities. These included:

- Identifying and nurturing relationships with potential **partners, investors, and backers** to broaden Cubane's reach and ecosystem.

- Assisting in the **design and execution of community engagement strategies** to grow and retain the Cubane user base.
- Researching **emerging blockchain protocols, encryption standards, and development tools** relevant to Cubane's roadmap.
- Collaborating with the technical team to **conceptualize and implement optimized solutions** for product development challenges.
- Creating **technical documentation**, including FAQs, user guides, and internal development progress reports.
- Supporting the development and refinement of **user interfaces** for Cubane's ecosystem tools and applications.

This internship gave me a chance to work directly on the Cubane platform, which focuses on scalability, privacy, and ease of use while meeting the needs of real-world businesses.

Chapter 2

LITERATURE SURVEY

2.1 Emerging Consensus Models in Blockchain

Many consensus methods have emerged due to continuous development of blockchain technology, with the goal to maintain balance between decentralization, security, and performance. In early blockchains, techniques like **Proof of Work (PoW)** and **Proof of Stake (PoS)** were essential, but they are not suitable in high performance environments, particularly in **SaaS** ecosystems. These methods often rely on sequential processing and provide little privacy or scalability support, which can be problematic for businesses.

To address these challenges, **Cubane** has come up with the **Cubic Consensus Mechanism (CCCM)**, an approach built around parallel processing and modular components. CCCM's core consists of independent validation units called as **Cubes**, which handle transaction validation concurrently instead of sequentially. This approach is particularly relevant for distributed, cloud-based systems that look for speed, scalability and reliable synchronization. By incorporating Coordinator Nodes to maintain network coherence without sacrificing decentralization, **CCCM** positions itself as a forward looking solution in the realm of **Layer-1 blockchain protocols**.

2.2 The Role of Privacy in Blockchain: ZKPs and FHE

Many industries like in healthcare, law, finance etc that deal with sensitive data are starting to use blockchain. Because of this, keeping data private is more important than ever. Two protocols that help ensure data is secured are **Zero-Knowledge Proofs (ZKPs)** and **Fully Homomorphic Encryption (FHE)**.

Zero-Knowledge Proofs allows to prove something is true without sharing the actual data. For example, a platform like **Binance** could use ZKPs to confirm a user is over 18 without showing their ID to the government. This way, the user's age can be verified while keeping their personal details confidential. In **CCCM**, ZKPs help check transactions without exposing any sensitive data, which is useful for apps that handle user or company information.

Fully Homomorphic Encryption lets validators work with encrypted data without having to unlock it first. It used to be very slow, but recent improvements have made it more useful. Big tech companies like **Microsoft** and **IBM** are already testing it for safer cloud services. In CCCM, FHE adds more security by allowing encrypted data to be processed while still following privacy laws like GDPR.

2.3 The Need for Modular, Scalable, and Secure Infrastructure

Decentralized apps today require systems that are not only secure and transparent, but also flexible enough to keep up with fast changes. Traditional consensus methods aren't very flexible as they usually need big updates to keep up with new standards.

CCCM takes a different approach. It's built in a modular way, where different parts like transaction validators, storage, or encryption can be updated separately without affecting the whole system.

This kind of flexibility is especially useful for SaaS platforms, where updates happen often and security needs change over time. By combining this modular setup with tools like **Fully Homomorphic Encryption (FHE)** and **Zero-Knowledge Proofs (ZKP)**, CCCM ensures user privacy and stay compliant with rules, all while allowing room for growth and innovation.

2.4 Conclusion

The combination of CCCM, ZKPs, and FHE in blockchain is a forward-thinking approach in solving the limitations of traditional consensus models. As more industries move towards decentralized solutions that require speed, privacy, and adaptability, bringing these technologies together is becoming important. Together, they offer a solid foundation for creating secure, compliant, and user-focused SaaS ecosystems that are built to last.

2.4.1 List of Papers referred for Literature Survey.

Paper Title	Authors	Takeaway from Paper	Limitation	Year
Zerocash: Decentralized Anonymous Payments from Bitcoin	Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers and Eran Tromer	Demonstrate d use of zkSNARKs for anonymous transactions in blockchain.	Complex setup; trusted setup required.	2014
Scalable, Transparent, and Post-Quantum Secure Computational Integrity	Eli Ben- Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev	Introduced zkSTARKs as scalable, trustless, and quantum- resistant ZKPs.	Large proof sizes increase bandwidth.	2018

Zero-Knowledge Proofs: An Overview	Nir Bitansky and Omer Paneth	Comprehensive explanation of ZKPs and their cryptographic applications.	Highly theoretical; lacks implementation examples.	2021
Zether: Towards Privacy in Smart Contracts	Benedikt Bünz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh	Applied ZKPs to smart contracts to ensure transaction confidentiality.	Still experimental; not widely adopted.	2020
Homomorphic Encryption for Arithmetic of Approximate Numbers	Jung Hee Cheon, Andrey Kim, Miran Kim, and Yongsoo Song	Made FHE practical for real-world arithmetic operations.	Less accurate than exact computation methods.	2017

TFHE: Fast Fully Homomorphic Encryption over the Torus	Ilaria Chillotti, Nicolas Gama, Mariya Georgieva and Malika Izabach`ene	Achieved practical FHE performance using torus-based encryption.	Still not efficient for large-scale SaaS systems.	2020
CryptoNets: Applying Neural Networks to Encrypted Data	Pengtao Xie, Misha Bilenko, Tom Finley, Ran Gilad-Bachrach, Kristin Lauter and Michael Naehrig	Showed how FHE can be used to run ML models on encrypted data.	Applicable mainly to static, fixed models.	2016
Fully Homomorphic Encryption Using Ideal Lattices	Craig Gentry	Pioneered fully homomorphic encryption allowing computation on ciphertexts.	Computationally heavy; impractical for real-time use.	2009

Algorand: Scaling Byzantine Agreements	Yossi Gilad, Rotem Hemo, Silvio Micali and Georgios Vlachos	Proposed a BFT consensus with high throughput and low latency.	Assumes honest majority; vulnerable if assumptions break.	2017
PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake	Sunny King and Scott Nadal	First implementation of PoS to replace energy-intensive PoW.	Early PoS model lacks slashing or penalization.	2012
A Better Method to Analyze Blockchain Consistency	Lucianna Kiffer, Rajmohan Rajaraman, and Abhi Shelat	Provided analytical models to measure blockchain consistency.	Focuses more on performance metrics than cryptography.	2018
A Secure Sharding Protocol for Open Blockchains	Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert and Prateek Saxena	Introduced a secure sharding design to improve blockchain scalability.	Requires high synchronization overhead.	2016

<p>Zerocoin: Anonymous Distributed E- Cash from Bitcoin</p>	<p>Ian Miers, Christina Garman, Matthew Green and Aviel D. Rubin</p>	<p>Proposed privacy layer for Bitcoin using ZK proofs.</p>	<p>High overhead and poor scalability.</p>	<p>2013</p>
<p>Hyperledger Fabric: A Distributed Operating System</p>	<p>Androulaki et al.</p>	<p>Showed a modular architecture for enterprise blockchain services</p>	<p>Not suitable for open/public blockchain networks.</p>	<p>2018</p>
<p>An Overview of Blockchain Technology</p>	<p>Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen and Huaimin Wang</p>	<p>Summarized blockchain architecture, consensus, and challenges.</p>	<p>Lacks focus on newer consensus like CCCM.</p>	<p>2017</p>
<p>RapidChain: Scaling Blockchain via Full Sharding</p>	<p>Mahdi Zamani, Mahnush Movahedi and Mariana Raykova</p>	<p>Presented a fully sharded blockchain for high throughput.</p>	<p>Complex synchroniza tion and coordination needed.</p>	<p>2018</p>

A Taxonomy of Blockchain-Based Systems	Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch and Len Bass	Provided classification for different blockchain architectures.	Focused more on typology than implementation.	2017
Ethereum: A Secure Decentralized Ledger	Gavin Wood	Defined Ethereum architecture and smart contract functionality.	Monolithic design not optimized for modular scaling.	2014
Thunderella: Blockchains with Optimistic Instant Confirmation	Rafael Pass and Elaine Shi	Proposed hybrid PoW/BFT model for fast transaction confirmation.	Optimistic design assumes network is often honest.	2017
The Honey Badger of BFT Protocols	Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi and Dawn Song	Proposed hybrid PoW/BFT model for fast transaction confirmation.	Optimistic design assumes network is often honest.	2017

Chapter 3

RESEARCH GAPS OF EXISTING METHODS

3.1 Limitations of Traditional Consensus Mechanisms

Traditional consensus methods like **Proof of Work (PoW)** and **Proof of Stake (PoS)** have played a key role in the development of blockchain technology. But when it comes to high performance, privacy focused environments like SaaS platforms, they often fall short due to their built-in limitations.

- **PoW** is computationally intensive, energy-inefficient, and suffers from scalability issues due to its sequential validation process.
- **PoS**, while more energy-efficient, often introduces centralization risks and lacks sufficient transaction throughput for enterprise-grade applications.
- Neither PoW nor PoS inherently provides **privacy-preserving features**, which are crucial for applications involving sensitive user data.

These limitations highlight the need for advanced consensus mechanisms that address both **performance** and **privacy** challenges.

3.2 Gaps in Privacy and Confidentiality

As concerns about data protection continue to rise particularly in sensitive sectors like healthcare, finance, legal etc, privacy has become a necessity for decentralized systems. Yet, existing blockchain solutions fall short when it comes to delivering strong privacy protections.

- Most existing blockchains store transaction data in plaintext, making it visible to all network participants.
- Technologies like zkSNARKs and other Zero-Knowledge Proofs (ZKPs) are becoming more popular, but their complexity and high computational requirements often make them hard to use widely.
- **Fully Homomorphic Encryption (FHE)** offers a promising alternative by allowing computation on encrypted data, but it remains underutilized due to performance constraints and the lack of integration with modular systems.

These challenges point to a major gap in research towards finding effective ways to build privacy preserving features into blockchain consensus systems that can scale for real-world applications.

3.3 Lack of Modularity and Adaptability in Blockchain Design

Most existing Layer-1 blockchains are built as all-in-one systems, where things like consensus, data storage, transaction checks, and app logic are all connected and handled together. This setup creates several problems:

- Difficulty in upgrading or replacing individual components without impacting the entire network.
- Poor adaptability to emerging technologies or evolving enterprise needs.
- Limited support for **customization**, which is essential for SaaS platforms that need custom features such as micropayments, subscription models, or regulatory compliance layers.

Whereas, Newer mechanisms like Cubane's CCCM take a different approach by breaking things into different segments like consensus, validation, and storage that can be improved or upgraded on their own.

3.4 Summary

The existing blockchain platforms are facing significant challenges in **scalability**, **privacy**, and **adaptability**. Traditional consensus mechanisms are unable to meet the demands of enterprise SaaS platforms, while privacy-enhancing technologies like ZKPs and FHE are still evolving in terms of usability and efficiency. Moreover, the lack of modular architecture in most blockchains limits flexibility and innovation. These gaps create a clear opportunity for next-generation solutions such as CCCM to reshape the future of Web3.

Chapter 4

PROPOSED METHODOLOGY

4.1 Overview of Cubane Cubic Consensus Mechanism (CCCM)

The Cubane Cubic Consensus Mechanism (CCCM) introduces a layered, modular approach for achieving scalable, secure, and privacy-preserving blockchain consensus. It is designed specifically for SaaS environments. CCCM employs a four-layer architecture that decouples the various elements of consensus which are **transaction initiation**, **privacy preservation**, **validation**, and **compression** into independent, efficiently orchestrated systems.

4.2 Layered Architecture of CCCM

4.2.1 Transaction Layer (Transaction Nodes)

The CCCM transaction layer begins at the Transaction Node, where a transaction request is initiated. This node utilizes the Dynamic Resource Allocation Layer (DRAL) to manage computational load. DRAL dynamically allocates compute resources based on the complexity of each transaction. The unused compute is utilized by the Member Node in Cube (MNCU) for network scaling. Once validated, transactions are forwarded to the ZK Layer for privacy validation.

4.2.2 Privacy Layer (ZK Layer)

The ZK Layer is responsible for generating Zero-Knowledge Proofs (ZKPs) using zkSTARKs. These proofs validate transaction integrity without revealing sensitive data. Transactions are batch-processed, timestamped using PoET and HTLC, and routed through a randomization algorithm into shards. A comparison of zkSTARKs and zkSNARKs confirms zkSTARKs as the optimal choice due to their scalability, transparency, and resistance to quantum attacks.

Key components in the ZK Layer:

- **Coordinator Node:** Oversees fair task distribution and consistency.
- **Proof Generation Nodes (PGNs):** Generate zk-proofs in parallel for scalability.
- **Batch Aggregation Node:** Aggregates and compresses multiple zk-proofs for final validation.

- **Synchronization Layer:** Ensures consistency, fault tolerance, and seamless communication using Gossip protocols and Merkle trees.

4.2.3 Validation Layer

Once proofs reach the Validation Layer, shards and cubes are formed to validate ZKPs. Each cube comprises a **Leader Node (LDN)** and multiple **Member Nodes (MNs)**. The LDN validates the ZKPs using a Tick Algorithm to verify timestamps and transaction integrity. The result is broadcast to MNs, which use Proof of Stake (PoS) to reach consensus. Once validated, proofs move to the **zkCompression Layer**.

Key components include:

- **Randomization Algorithm:** Ensures fair zk-proof distribution.
- **Cube Organizer Algorithm:** Assigns nodes into cubes.
- **LDN & MN Structure:** Implements a leader-member validation model with dynamic resource allocation.

4.2.4 zkCompression Layer

The final layer compresses validated transactions using **Merkle Trees** and recursive **zk-proofs**. This process generates a single, compact cryptographic hash for on-chain storage, while complete metadata remains off-chain for auditability.

Steps involved:

- **Merkle Tree Construction:** Represents all zk-proofs in a batch.
- **Recursive zk-Proofs:** Minimizes storage overhead.
- **Hash Generation:** Creates final on-chain block hash.
- **Reward Distribution:** Allocates staking and validation rewards to LDNs and MNs.

4.3 Key Innovations of CCCM

- **Modular architecture:** Allows independent upgrades of layers.
- **Parallelization:** High throughput is achieved via distributed PGNs and validation cubes.
- **Privacy-preserving consensus:** zkSTARKs and FHE integration for secure data handling.
- **Scalability and decentralization:** Designed to support high-frequency SaaS transaction models.

4.4 Summary

CCCM is a strong, flexible, and privacy-first upgrade to older blockchains. By using separate layers and advanced encryption, it solves common problems in today's blockchains and makes it easier to build secure SaaS apps on decentralized networks.

Chapter 5

OBJECTIVES

5.1 Technical Objectives

The primary goal of the internship was to understand and contribute to the development of the **Cubane Cubic Consensus Mechanism (CCCM)**. This involved exploring its layered architecture which included the **Transaction Layer**, **ZK Layer**, **Validation Layer**, and **zkCompression Layer** and assisting in the documentation and analysis of each component. A key focus was placed on **evaluating and implementing zkSTARKs**, which offer scalable, privacy-preserving proof generation suitable for high-performance blockchains.

5.2 Research-Oriented Objectives

Another major objective was to perform a **comparative study of Zero-Knowledge Proofs**, primarily zkSNARKs and zkSTARKs, to determine their suitability within CCCM. This research extended to understanding **Fully Homomorphic Encryption (FHE)** and other cryptographic standards relevant to privacy-focused blockchain infrastructure. The findings were used to support informed decision-making in the implementation of privacy mechanisms within the Cubane architecture.

5.3 Product & Ecosystem Objectives

As part of the role, the internship also focused on enhancing Cubane's **ecosystem** through community outreach, investor engagement strategies, and contributing to platform documentation. We worked on improving the design of user interfaces, FAQs, and learning materials to make sure the platform is easy to use and understand for everyone including non-technical audience.

5.4 Strategic Alignment Objectives

In alignment with Cubane's long term vision, the internship aimed to ensure that all contributions supported the **scalability, privacy, and adaptability** of the platform. By adopting a modular and future-ready development approach, the work contributed towards the long-term goal of making Cubane a trusted infrastructure for decentralized applications in industries such as Insurance, Digital IP, and SaaS.

Chapter 6

SYSTEM DESIGN & IMPLEMENTATION

6.1 Overview of the CCCM Architecture

The Cubane Cubic Consensus Mechanism (CCCM) is designed as a four-layered, modular blockchain architecture to deliver **scalability, privacy, and consistency** for high-performance SaaS applications. Each layer—Transaction Node, ZK Layer, Validation Layer, and zkCompression Layer—performs specific roles in transaction processing, proof generation, and on-chain integration. This chapter describes the system design and implementation strategies used to realize these layers during the internship.

6.2 Transaction Node Layer

The **Transaction Node Layer** initiates transaction requests and dynamically allocates computational resources through the **Dynamic Resource Allocation Layer (DRAL)**. This ensures optimal CPU usage based on the complexity of incoming transactions.

After an initial resource check, the transaction request is validated and routed forward to the ZK Layer. The portion of unused compute from the Transaction Node acts as a Member Node within the Cube (MNCU), contributing to network-wide scalability.

6.3 ZK Layer Implementation

The **ZK Layer** is responsible for generating privacy-preserving **zkProofs (specifically zkSTARKs)** for validated transactions. These proofs are timestamped using a hybrid of **Proof of Elapsed Time (PoET)** and **Hash Time-Locked Contracts (HTLC)** mechanisms, ensuring sequencing and temporal integrity.

To scale zk-proof generation, the ZK Layer uses:

- **Coordinator Nodes** for batching and task distribution.
- **Proof Generation Nodes (PGNs)** to generate zkSTARKs in parallel.
- **Batch Aggregation Nodes** for consolidating multiple proofs into a single output.
- **A Synchronization Layer** using gossip protocols and Merkle Tree verification for consistency across nodes.

The system was implemented to batch transactions based on parameters like transaction complexity, network congestion, and time intervals. Batch processing improved proof generation throughput significantly.

6.4 Validation Layer Architecture

In the **Validation Layer**, zk-proofs are randomly assigned to **Shards**, where the **Cube Formation Algorithm** creates multiple validation units known as **Cubes**.

Each cube contains:

- A **Leader Node (LDN)** elected via Proof of Stake (PoS) and Randomization Algorithm.
- Multiple **Member Nodes (MNs)** responsible for verifying the leader's output.

The validation follows a two-step process:

- The **Leader Node** validates zk-proofs, verifies timestamps using a **Tick Algorithm**, and shares results.
- **Member Nodes** independently confirm the output. If consensus is reached, the transaction is marked valid and sent to the zkCompression Layer.

This leader-member model enables parallel processing which reduces latency and increases throughput.

6.5 zkCompression Layer Design

The **zkCompression Layer** is the final layer before on-chain storage. It aggregates and compresses validated zk-proofs using a multi-step algorithm involving:

- **Merkle Tree Construction** for proof hierarchy.
- **Recursive zkProofs** for compressing multiple proofs into a compact structure.
- **Cryptographic Hash Generation** to represent each batch.

Two outputs are generated:

- A **root hash** stored on-chain to serve as an immutable record.
- **Off-chain metadata** stored externally for auditing and verification purposes.

This layer ensures minimal on-chain data usage while maintaining verifiability and traceability.

6.6 Reward Mechanism Integration

Once a block is finalized in the zkCompression Layer, **rewards are distributed** to the Leader and Member Nodes of the cubes involved in the validation. These rewards are issued based on successful proof generation, validation accuracy, and uptime, aligning with the **staking-based incentive model**.

6.7 Implementation Summary

The layered design of CCCM allows modular development and testing of each functional component. Each layer is developed with a focus on scalability, fault tolerance, and cryptographic integrity. The integration of zkSTARKs and time-stamping protocols provides an innovative solution to existing blockchain limitations. This design of Cubane offers a decentralized yet enterprise-ready infrastructure for industries requiring privacy, performance, and adaptability.

Chapter-7

TIMELINE FOR EXECUTION OF PROJECT (GANTT CHART)

7.1 Project Timeline Overview

The internship lasted **12 weeks** and gave plenty of time to dive into both the technical and strategic sides of the **Cubane's Cubic Consensus Mechanism (CCCM)**. The project was structured step by step, starting with learning and research, then helping with development, writing documentation, and wrapping up with a final report.

7.2 Gantt Chart



Figure 7.2.1

The Gantt chart (Figure 7.2.1) shows a week by week breakdown of the tasks completed during the internship, from February 1 to May 3, 2025. It includes all major activities like research, studying the system's design, writing documentation, designing parts of the

CCCM, and building tech partnerships. Each task was planned and carried out in order, helping ensure steady progress and meaningful learning throughout the 12-week internship.

Chapter 8

OUTCOMES

8.1 Technical Outcomes

During the internship, I gained a solid understanding of the Cubane Cubic Consensus Mechanism (CCCM) and how its modular blockchain system works. By diving into research, analyzing the system, and helping with documentation, I was able to make meaningful technical contributions in several key areas such as

- A detailed comparative analysis of **zkSNARKs and zkSTARKs** was conducted to assess their suitability for Cubane’s privacy infrastructure, with a recommendation in favor of zkSTARKs based on scalability and transparency.
- The architecture and transaction flow of all four CCCM layers—**Transaction Node, ZK Layer, Validation Layer, and zkCompression Layer** were studied and documented.
- A mapping of **node roles and responsibilities**, including Proof Generation Nodes (PGNs), Coordinator Nodes, Leader Nodes, and Member Nodes, was created to support internal architecture documentation.
- The functionality of **dynamic batching, timestamp verification using PoET + HTLC, and Merkle-based compression techniques** were analyzed.

8.2 Strategic and Ecosystem Contributions

In addition to the technical contributions, the internship role also focused on ecosystem development :

- Framing of supporting material including **FAQs and flow diagrams** to improve onboarding and understanding of Cubane’s ecosystem tools.
- Participation in **community-building discussions** and internal meetings for ecosystem expansion and investor outreach strategies.

8.3 Personal and Professional Growth

This internship provided hands-on exposure to the **cryptography, blockchain design, and documentation**. Working closely with senior developers and product teams, I was able to avail the following:

- Improved research and analytical skills in complex topics such as zero-knowledge proofs and consensus protocols.
- Stronger technical writing and documentation abilities, especially in communicating layered systems to diverse audiences.
- A deeper appreciation of decentralized architecture and its implications for real-world applications in industries like finance, healthcare, and digital IP.

8.4 Summary

Overall, I was able to successfully meet the main goals of my internship, both technically and strategically. My work aligned with Cubane's long-term mission to build a secure, scalable, and flexible Layer-1 blockchain. The contributions I made are expected to support ongoing development, help with knowledge sharing, and contribute to community education as the Cubane continues to grow.

Chapter 9

RESULTS AND DISCUSSIONS

9.1 Technical Results

The internship gave me valuable technical insight into how a modular Layer-1 blockchain works. By exploring Cubane’s Cubic Consensus Mechanism (CCCM), I was able to achieve several key outcomes:

- The implementation and evaluation of zkSTARKs proved effective for batch processing of high-volume transactions while ensuring data privacy. This validated Cubane’s decision to move away from traditional zkSNARKs for scalability and transparency reasons.
- Each layer of the CCCM architecture—from Transaction Nodes to zkCompression—was broken down, documented, and critically analyzed. This layered study allowed a clear understanding of how CCCM enhances **parallelism, modularity, and privacy** simultaneously.

9.2 Discussion on Challenges and Solutions

While the internship journey was successful, several challenges were encountered:

- **High Complexity of zkSTARKs Implementation:**
zkSTARKs, while scalable, come with large proof sizes and significant computational costs. The solution involved introducing a **batch processing approach** and recommending **trusted environments** during early-stage implementation to offset computational load.
- **Node Synchronization and Data Integrity:**
With distributed Proof Generation Nodes (PGNs) and Coordinator Nodes, maintaining synchronization was a key concern. This was addressed through a **Gossip Protocol** and **Merkle Tree-based state verification**, which were studied and supported in the final architecture documentation.

- **Lack of Existing Frameworks for Modular Consensus:**

Because CCCM is a novel consensus mechanism, there was limited existing literature to rely on. Most concepts had to be approached from first principles and analyzed using Cubane's internal design logic. Collaborative discussions with the core development team helped overcome these limitations.

9.3 Validation of Results

Throughout the internship, conceptual understanding was backed by:

- Reviewing open-source implementations of privacy-preserving protocols.
- Creating documentation with references to real-world use cases in privacy-sensitive sectors like finance and healthcare.
- Ensuring that architectural recommendations align with the scalability and decentralization goals of Cubane.

9.4 Alignment with Internship Objectives

The results achieved were strongly aligned with the objectives set at the beginning of the internship. Technical contributions such as flowcharts, zkSTARKs documentation, and architectural analysis supported both product and ecosystem development. Furthermore, engagement in strategic and UI/UX-related discussions reinforced the holistic understanding of the platform from both engineering and product perspectives.

9.5 Summary

The internship delivered concrete technical results, strategic value, and learning outcomes. During the internship, I didn't just learn and evaluate the CCCM framework but also helped in improving it by offering recommendations. These efforts made my internship a valuable and rewarding experience.

Chapter 10

CONCLUSION

My internship at **Jitoshi Technology Private Limited**, where I worked on the **Cubane**, was an incredible experience that connected with what I had learned in theory to real-world applications in **blockchain development**. As a **Product and Ecosystem Development Lead Intern**, I had the chance to dive deep into the **Cubanes Cubic Consensus Mechanism (CCCM)**, modular **Layer-1 blockchain** built with a focus on **privacy, scalability, and decentralization**. I was able to contribute to ongoing research and documentation around CCCM, getting hands-on experience with advanced technologies like **Fully Homomorphic Encryption (FHE)**, **zk-STARKs**, **Proof of Elapsed Time (PoET)**, and **Proof of Stake (PoS)**.

In addition to the research side, I collaborated with a talented team on key initiatives, including writing and deploying the **CUBS Token** smart contract. I also played a part in building strategic tech partnerships with companies like **Paycio, Insight Genesis, Decatron, Meet Finance, and 0xTeam Space**, which gave me broader insight into the **blockchain ecosystem**.

This internship gave me a clearer understanding of **blockchain infrastructure** for **SaaS industries** and sharpened my skills in **research, cryptography, technical communication, and systems design**. Not only was I able to make a real impact on a live project in a rapidly evolving space, but it also brought me a step closer to my long-term goals in **blockchain** and **cyber security**.

REFERENCES

1. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized anonymous payments from Bitcoin. *IEEE Symposium on Security and Privacy*.
2. Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptology ePrint Archive*, 2018(46).
3. Bitansky, N., & Paneth, O. (2021). Zero-Knowledge Proofs: An Overview.
4. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., & Maxwell, G. (2020). Zether: Towards privacy in smart contracts. In *NDSS*.
5. Buterin, V. (2020). Blockchain privacy and scalability. *Ethereum Foundation Blog*.
6. Cheon, J. H., Kim, A., Kim, M., & Song, Y. (2017). Homomorphic encryption for arithmetic of approximate numbers. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 409–437). Springer.
7. Chillotti, I., Gama, N., Georgieva, M., & Izabachène, M. (2020). TFHE: Fast fully homomorphic encryption over the torus. *Journal of Cryptology*, 33(1), 34–91.
8. Dowlin, N., Gilad-Bachrach, R., Laine, K., Lauter, K., Naehrig, M., & Wernsing, J. (2016). CryptoNets: Applying neural networks to encrypted data with high throughput and accuracy. In *ICML*.
9. Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of computing* (pp. 169–178).
10. Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling Byzantine Agreements for Cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles* (pp. 51–68). ACM.
11. King, S., & Nadal, S. (2012). PPCoin: Peer-to-peer crypto-currency with proof-of-stake. Self-published whitepaper.
12. Kiffer, L., Rajaraman, R., & Shelat, A. (2018). A better method to analyze blockchain consistency. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 729–744).
13. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17–30).
14. Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). Zerocoin: Anonymous distributed e-cash from Bitcoin. In *IEEE Symposium on Security and Privacy* (pp. 397–411).
15. Miller, A., Xia, Y., Croman, K., Shi, E., & Song, D. (2016). The Honey Badger of BFT protocols. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 31–42).
16. Pass, R., & Shi, E. (2017). Thunderella: Blockchains with optimistic instant confirmation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 3–33). Springer.
17. Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*.
18. Wüst, K., & Gervais, A. (2018). Do you need a blockchain?. In *Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45–54). IEEE.
19. Xu, X., Weber, I., & Staples, M. (2017). A taxonomy of blockchain-based systems for architecture design. *IEEE Software*, 34(4), 70–77.

20. Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 931–948).
21. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data* (pp. 557–564). IEEE.
22. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018). Hyperledger Fabric: A distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference* (pp. 1–15).

APPENDIX-A

PSUEDOCODE

Function ProcessTransaction(transaction):

```
// Layer 1: Transaction Node
resources = DRAL_Allocate(transaction.complexity)
If resources < MIN_THRESHOLD:
    RejectTransaction("Insufficient resources")
EndIf
ForwardToZKLayer(transaction)

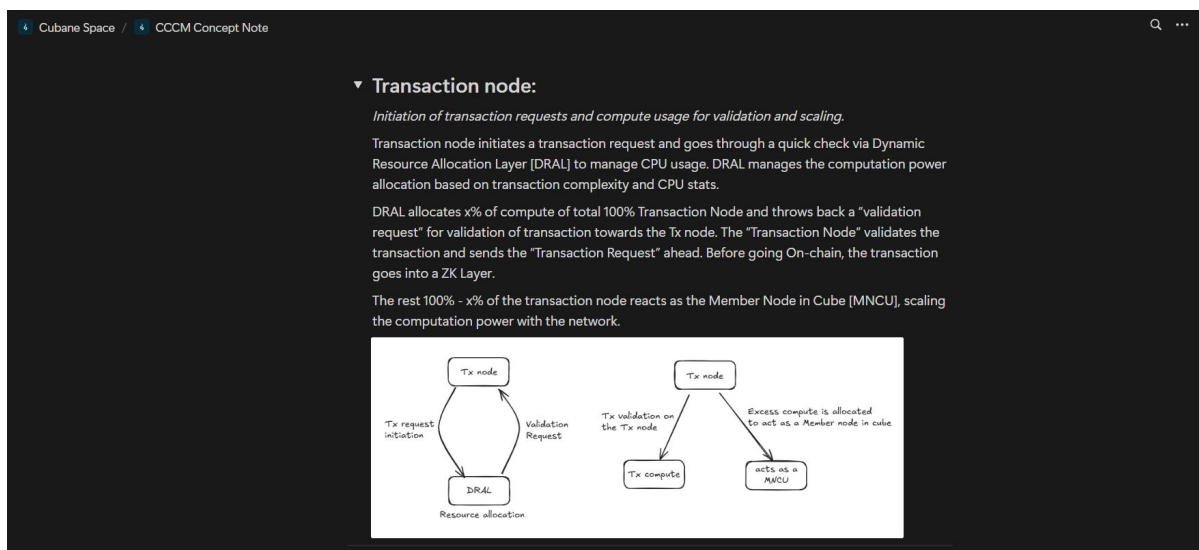
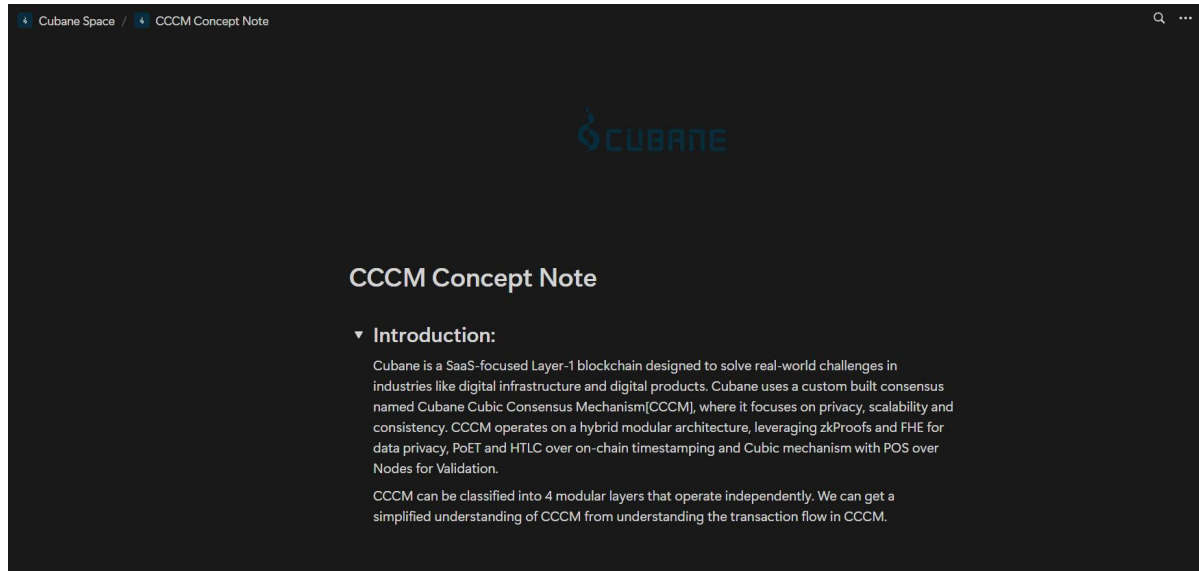
// Layer 2: ZK Layer - Proof Generation
proof = GenerateZKProof(transaction)
timestamp = GenerateTimestamp(transaction)
shardID = RandomShardAssignment()
ForwardToValidationLayer(proof, timestamp, shardID)

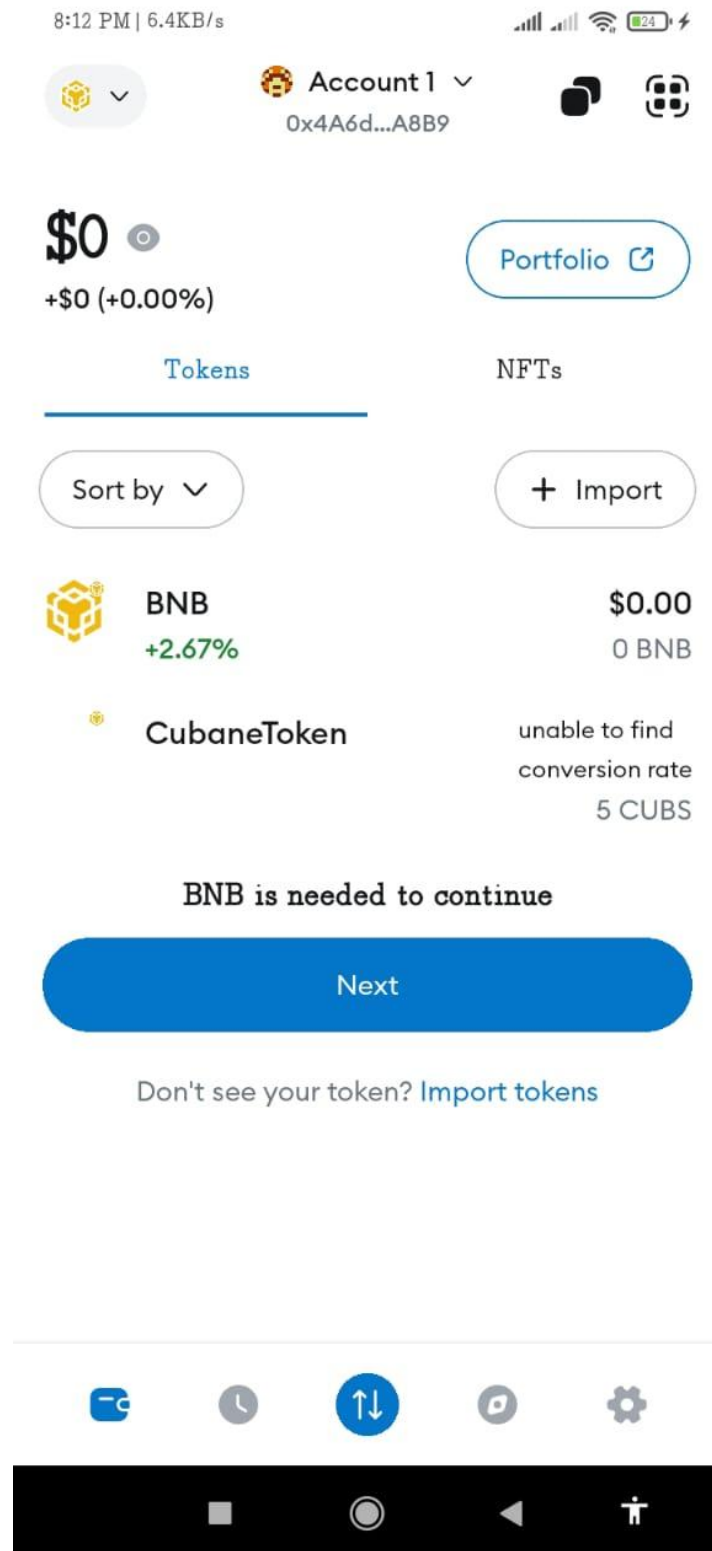
// Layer 3: Validation Layer
cube = FormValidationCube(shardID)
result = cube.LeaderNode.ValidateProof(proof, timestamp)
consensus = cube.MemberNodes.Verify(result)
If consensus == TRUE:
    ForwardToCompressionLayer(proof)
Else:
    RejectTransaction("Consensus failed")
EndIf

// Layer 4: zkCompression Layer
compressedBlock = CompressProof(proof)
StoreOnChain(compressedBlock.hash)
StoreOffChain(compressedBlock.metadata)
DistributeRewards(cube.LeaderNode, cube.MemberNodes)
EndFunction
```

APPENDIX-B

SCREENSHOTS







Paycio

15,604 followers

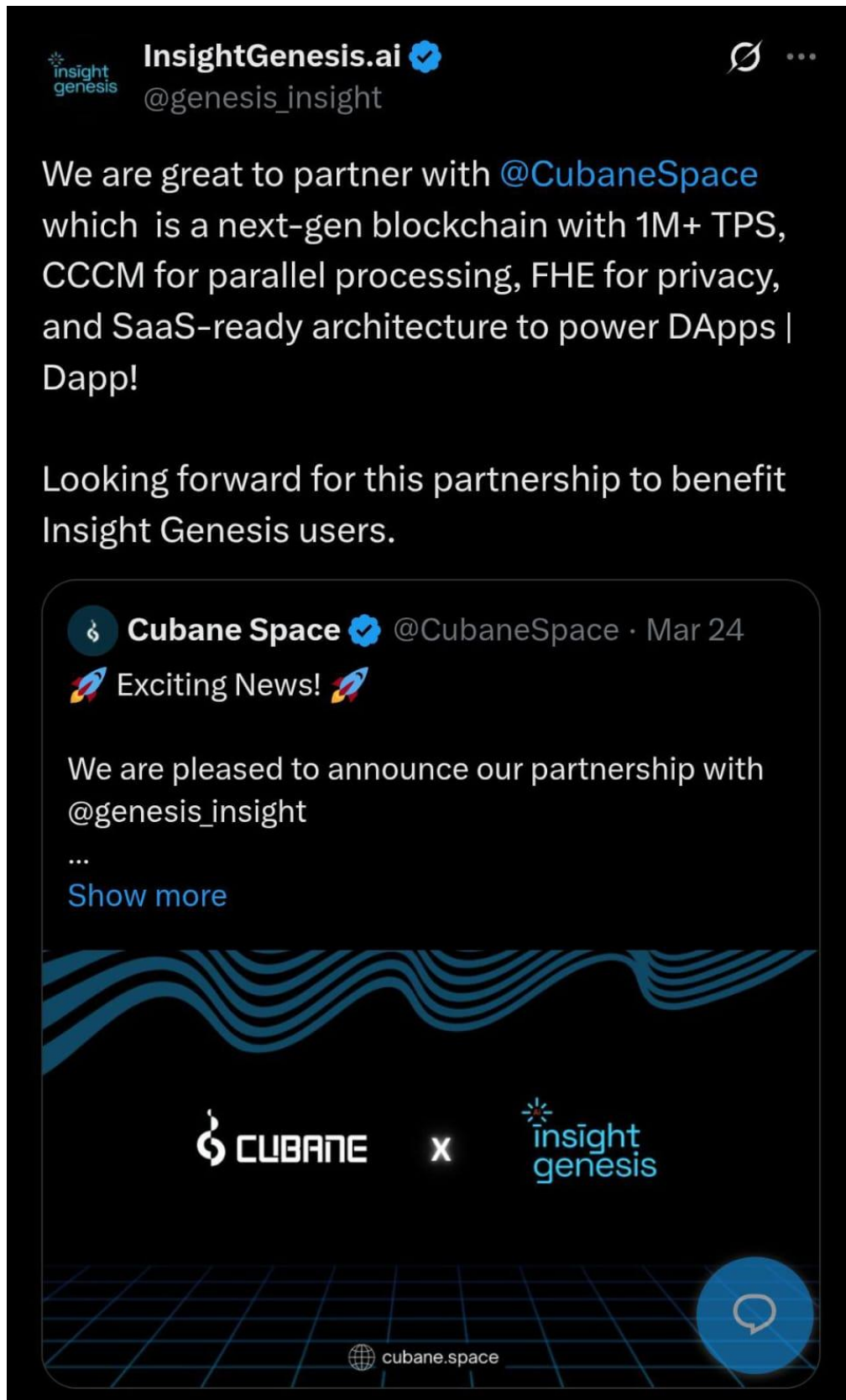
2mo • 🌐

In our quest for excellence, Paycio is proud to partner with an industry leader, Cubane. By integrating with Cubane's scalable Layer-1 blockchain, Paycio is set to enhance crypto payment transactions, driving innovation in the finance and healthcare sectors. Stay tuned for more updates as [#PaycioxCubane](#) leads the charge in transforming digital finance and blockchain adoption.

[Cubane™](#)


[#blockchaininnovation](#) [#cryptopayments](#) [#expertpartners](#)
[#growthpartnership](#)





APPENDIX-C

ENCLOSURES


Page 2 of 53 - Integrity Overview
Submission ID: rrcol-ic:13248696755





19% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.




Filtered from the Report

► Bibliography

Match Groups

- 
46 Not Cited or Quoted 19%
Matches with neither in-text citation nor quotation marks
- 
0 Missing Quotations 0%
Matches that are still very similar to source material
- 
0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 
0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 1.4%  Internet sources
- 1.0%  Publications
- 1.6%  Submitted works (Student Papers)


Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our systems algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.


Page 2 of 53 - Integrity Overview
Submission ID: rrcol-ic:13248696755

SUSTAINABLE DEVELOPMENT GOALS

