NOTUS WHITEPAPER

DRAFT 1

Omer Goksoy [1] — Sahap Kurtaran [2] — Mehmet Kircal [3]

Abstract

This paper is the presentation of an architectural and design overview of Notus' initial release. In addition to a scalable and secure blockchain architecture, it includes a consensus structure based on Proof-of-Randomness (PoR), a synthesized hash algorithm, a variable nonce calculation structure. See the Token Economy Whitepaper for information on the native token economy.

Legal Disclaimer: Nothing in this White Paper constitutes a solicitation of an offer to acquire or a sale of any tokens. Notus releases this White Paper purely for public criticism and feedback. This paper contains preliminary information that could change at any time. This paper may also include "forward-looking statements."

1 — Introduction

Blockchain is a distributed Digital Ledger Technology (DLT) that consists of cryptographically secure blocks which connect to one another to store transaction data. With the release of the Bitcoin whitepaper by Satoshi Nakamoto on September 31, 2008, and the launch of the bitcoin network on January 3, 2009, blockchain technology entered our lives. As blockchain technology has entered our daily lives, numerous networks have begun to offer solutions in various forms for human use one by one. However, no platform has been able to create a network topology where the trilemma of decentralization, scalability, and security functions without any drawbacks.

Notus, a decentralized blockchain platform, addresses the trilemma of decentralization, scalability, and security differently. With a Proof of Randomness (PoR) consensus, a synthesized computation structure, and payment transactions, it quickly completes transactions by distributing next-generation Web3 solutions and transaction load around the network.

We created this paper to explain the Notus system's architectural layout and the methods used to create it. Even though the Notus created this architecture with every consideration, it is crucial to remember that this technology is still in its development.

2 — Principles

To achieve the ideals of blockchain, one should always keep innovation, experimentation, and development in mind. The architectural infrastructures that current and historical blockchain platforms use today are typically comparable. The primary guideline for maintaining technical advancements is the requirement to redesign new architectures in accordance with usage patterns.

The first foundations of the Notus architecture design is about Bitcoin. Notus proposes an alternative network structure with significant design improvements that comprise its architectural structure, taking into account the issues faced by other networks as well as the Bitcoin fundamental architecture.

The Notus design covers 6 principles.

— Scalability
— Low Carbon-Neutral
— Full Decentralization
— Simplicity
— Speed Transactions
— Secure

2.1 — Scalability

The inability of existing blockchain platforms to get past the transaction density barrier is one of their main issues. Based on this issue;

— Increasing the transaction density in a specific period.
— Limitation of transaction pools.
— Verifiers delay the confirmation of low-fee transactions as they favor high transaction costs when reacting to transactions.
— The network creates multiple blocks that are similar to one another as a result of validators competing with one another, lengthening the time it takes for each block to complete.
— Limit the number of transactions one can add to the architecture-derived block.

Notus introduces the transaction pool structure as a distributed transaction pool structure that incorporates all validators to address these issues faced by current networks. The unique transaction pools may include all transactions of the validators in addition to the main transaction pool.

Block generation can only take place for no more than 0.2 seconds. The primary purpose of keeping this time low is to consider the distribution time of transactions to all nodes. Additionally, it has a limitless transaction capacity while creating blocks, allowing for the insertion of transaction data to each block.

In order for scalability to function, each validator alternately works as a sizable team. Functioning in succession is the golden rule for validators working as a team. The way of validators' integration into the network is through using protocol-based authentication. The validator included in the network performs all the operations sequentially. Other validators validate these transactions and add them to the chain.

2.2 — Low Carbon-Neutral

Blockchain systems' high energy usage has an impact on climate change as well. With a synthesized computing method and a carbon-neutral blockchain architecture, Notus is dedicated to reducing users' and developers' carbon footprints without compromising sustainability. This revised structure has a security flaw due to the low difficulty level, but we fixed this flaw with a method created for the nonce calculation mechanism. Studying the developed designs and approaches is possible in the Notus architecture area.

2.3 — Full Decentralization

The concept of "Full Decentralization" is at the heart of Notus' goals. Our key objective is to maintain the decentralized nature of the entire process, from the transfer procedure through the decision mechanism. In this way, all Notus users will be able to share their transactions with whichever validators they choose directly.

2.4 — Simplicity

Web3 apps have proliferated thanks to Blockchain technology in response to various needs in industries including finance, insurance, digital identity, travel, health, games, music, and education, among others. With state-based development, Notus has streamlined the procedure by incorporating the smart contract process (Token, NFT, DApp) required for the creation of Web3 applications into the source code.

State-based development makes it possible for project developers to swiftly begin the project development process and reduce vulnerabilities while creating code.

2.5 — Speed Transactions

Today, Visa claims it can accommodate 1,700 transactions per second and 24,000 TPS [01], while Mastercard believes it can support 5,000 transactions. This competition for scalability and transaction speed is the grand race of the blockchain. The goal of Notus, on the other hand, is to give users the ability to do more transactions per second swiftly and effortlessly. With a distinct computational framework and block architecture, Notus asserts that it can make this claim. The remainder of this paper contains further in-depth information.

2.6 — Secure

Due to its decentralized nature and consensus-based structure, blockchain technology produces cryptographic data structures with built-in security measures. Despite having a different architecture than the current blockchain network topology, Notus has not compromised security. Instead, it has created a fast and secure network structure by redesigning the Nonce computing architecture.

3 — Overview

Notus is a scalable and fast modular chain. It acknowledges that a layered approach to network architecture is always the best way to fully realize the potential of blockchain technology. It adopts that a structurally multi-layered solution can resolve many dilemmas facing the blockchain community. Notus has always backed efforts to use innovation, experimentation, and development to strengthen the connection between blockchain and the real world. These features set Notus apart from existing networks with a dynamic, harmonic, and modular structure. This will allow for novel behaviors among network-based apps and aid in determining the technological course that blockchain technology will take in the future.

3.1 — Timestamp

The timestamp proves that the data must have existed at the time to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it [02]. Nodes in Notus connect with one another via the Network Time Protocol (NTP) and get precise UTC information. Then,

using the time information they have received, all nodes synchronize. This timestamp step is subject to further processing.

3.2 — Data Availability

Data availability entails the node that created the block broadcasting all transaction data within the block and other nodes validating (making available). As in current blockchain networks, we process transactions in blocks and append to the chain. Each node in the network checks a new block proposal against the information in the preceding blocks, confirms it, and adds it to its own chain. Nodes in the network ignore this transaction and do not include it in the chain when they recognize that the new block has an error. Nodes defend against counterfeit block assaults in this way. Additionally, Notus permits light nodes to conduct verification duties when they store block digests on the network. In doing so, it raises the network's security level and protects it from malicious users.

3.3 — Consistency

The efficient and consistent operation of the blockchain is the process by which any confirmation of transaction and consensus reached by several nodes. Notus uses Proof of Randomness (PoR) and Proof of Stake to achieve consensus (PoS). All nodes have a random queue to process transactions in a Proof of Randomness (PoR) consensus, and they are free to validate and add transactions to the network following the approval. Additionally, this procedure is on repeat at predetermined intervals, strengthening the network's defense against attacks.

3.4 — Verification

Bitcoin records the blocks it produces as binary. Meanwhile Notus stores the blocks it generates as a JSON object. To determine the block hash, Notus splits the JSON object into three aspects: block, info, and data. The method and hash algorithm selection is in the nonce parameter in the info parameter, and each component gets generated independently.

Production of a signature of these nonce calculations is after the conclusion of the info, block, and data nonce calculations. The last variable in the hash parameter holds the newly formed signature. Creation of the block signature is also through using this variable.

Notus includes the following seven parameters to generate the hash of each block.

- **Info:** includes details about the block. This data includes the block's version number, block type, block ID, line number, and nonce mechanism (Sliding calculation, Skip calculation, Hash method, Difficulty level).
- **Keeper:** Unencrypted or encrypted raw data, including transactions saved in the block, is stored.
- **Hash:** The parameter holds the hashes of objects as blocks, data, and info.
- **Validator:** It is the parameter that keeps the information of the validator that makes the nonce calculations.
- **Nonce:** It is the parameter that holds the nonce values of the segmented structure.
- **HashPrevBlock:** It is the parameter that holds the ID and summary of the previous block. There are 192+90=282 bytes.
- **Sign:** The parameter holds the summary of all JSON objects.

Notus uses all the parameters in the JSON object incrementally when creating the block signature. These parameters verify whether the block is valid or not.

3.5 — Censorship

A node that joins the network delivers its information to the other nodes first. Afterwards, it begins to monitor for information coming from other nodes. Synch of the nodes before sorting is through using randomization. The leader node in this ranking is qualified to conduct the transaction. If the chosen leader node does not respond, backup nodes, nodes 2 and 3 will take control. Once the transaction is complete, the node chosen as the leader broadcasts it to the network. Other nodes examine the block structure and confirm its accuracy. We select a new leader node once the allotted amount of time has passed and update the ranking once more. As a result, during each block generation, we select a leader and two backup nodes. The action of the node selected as the leader in other nodes goes through checking and verification process. The other nodes will disregard any attempted incorrect or improper transactions made by the node selected as the leader, and the two backup nodes have permit to conduct transactions in their own right.

For info on the penalty mechanism nodes will use in the event of error, consult the consensus thread.

3.6 — Finality

Through providing validators with a random queue of actions in line with the mathematical procedure, Proof of Randomness (PoR) enables time-based role/task

allocation. All validators must submit their status signature within 0.2 seconds since the PoR consensus generates a queue. Depending on the network density, this time scenario may get worse. Each time a transaction is valid, the validator chosen as the leader in the ranking receives a vote from the whole network. Every validator keeps track of the situation and syncs with other validators. Finally, it controls to see if the newly formed block is still valid after the requisite wait.

4 — Architecture

Scalability, security, and fully decentralization are the three key issues with existing blockchain platforms that Notus architecture proposes various technical and architectural concepts and innovations to address. It suggests a modular blockchain architecture that makes it possible to use sidechains that are available to access by platforms in order to adapt to changing requirements. As a result, the main chain's density and traffic will decrease, and transactions will support the use of various features.

4.1 — Sidechains

Through the usage of sidechains, tokens and other digital assets from one blockchain is safe to use on another. Sidechains have the ability to improve the functioning and capabilities of blockchains.

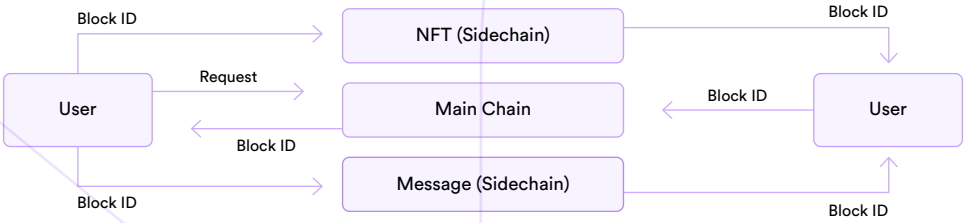
Similar to other blockchain networks, the Notus network has a sidechain mechanism that connects to the main blockchain in both directions. Contrary to other networks, Notus is not totally independent from the primary chain. The Notus architecture does not provide sidechains with their own nodes. All transactions are subject to control by main chain validators. Achieving consensus can be through using Notus consensus, and each network validator offers security. Transactions become final and immutable in 1-5 seconds thanks to the Notus consensus.

Here's how the side chains work, step by step.

— The user sends a request to the main chain and receives a block ID for the transaction from the main chain.
— It sends a transaction request to the sidechains with the block ID.
— The user receives the transaction confirmation information after the side chains transaction is complete.

In case of sending transaction query from the main chain to side chains:

— Sending a query from the main chain to the sidechain with the block ID.
— If the transaction is present and complete, sending the response that the transaction was successful.
— If there is no action, sending an error message. If the process is not complete, sending a continuation message.



Graphic I: *Sidechain Working Mechanism*

4.2 — Validators (NoVa)

The competitiveness of miners with one another is what drives traffic density in networks using the Proof of Work consensus mechanism. The intense competition among miners forces them to constantly upgrade their hardware. This issue has a solution in the form of a paradigm where miners operate sequentially within an algorithm and split the revenue generated by all of the network's nodes.

The validator task/role distribution design in the network as a solution to the scaling issue is one of the major advancements in the Notus architecture. These nodes, which uphold Notus's decentralized organization, have several role categories. When we generate reward blocks, we refer to these roles as "Miners," but once other nodes' transactions are valid, we refer to them as "Validators."

For creating empty blocks, validating and adding new transactions to the chain, and updating the blockchain, validators (NoVa) may receive a daily payment.

There are two different node types in Notus. These are;

I- Nodes/Validators (NoVa)

Represents nodes that fulfill the Notus-installed or -defined system requirements. Saving these nodes' IP addresses locally is possible by each node or included in the source

code of those nodes.addresses of these nodes can be embedded in the source code or stored by each node in the local nodes.

II- Archive Node

One can assign these nodes as both archivers and validators.

— **Full Node:** It represents the node type with a low system configuration that keeps all copies of blocks produced in the network but does not create new blocks.

— **Light Node:** It represents the type of node that holds all the block hashes generated in the network but does not create new blocks.

4.3 — Validator Queue

Each validator joining the Notus network must have a wallet address in order to verify transactions. The account to which the tokens earned as a result of the transactions upon validator's conducting and approving are available for transfer, which is subject to the determination of wallet address. It also establishes the sequence in which validators will work.

To ensure the effective running of the network, Notus has built it so that validators validate transactions in a sequential order.

These operations take place according to the following situation.

— Each validator shares its wallet address with other validators and requests wallet addresses from other validators.
— Converting all wallet addresses from the 58-number system to the 10-number system.
— Ordering all wallet addresses from smallest to largest.
— A newly added validator cannot trade for 2 rounds.
— The time allocated for each validator is 200 ms.
— If the validators do not complete the transaction within the allotted time, the other validators validate the block that the next validator will add to the chain for the current block.
— If active validators do not create blocks 3 times within the specified time, other validators exclude them from the network for 1 hour.

4.4 — Multiple Transaction Pools

Sent transactions which lack confirmation by the network gather in the Mempool. There is a pool of unconfirmed transactions that each node is aware of but which have not yet been added to the blockchain [3].

As a solution to the scalability issue, which is one of the major issues with blockchain platforms, the Notus architecture's main focus is task distribution design for validators in the network. Suggestion of the creation of several transaction pools is present as the most efficient solution to the bottleneck brought on by the scalability issues due to network density.

The working mechanism of multi-process pools is as follows:

— Signing transactions made through the wallet.
— Forwarding signed transactions to the personal pools of all validators.
— Transactions accumulate in validator pools.
— It scans the transaction pools of other validators, which are in the order of transactions from the validators.
— The next validator draws the transactions of other validators into its own pool.
— The validator, which creates a block and adds the transactions to the chain, notifies the validator of the status of the completed transactions.
— This process ensures continuity by following the same sequence.

Multiple Transaction Pools Benefits:

— Unlimited transaction skill
— Quick access to transactions by Miners/Verifiers
— Minimum network traffic density

4.5 — Complex Block Structure

The two sorts of blocks found in blockchain networks nowadays are smart contracts and payment transactions. Despite the fact that the entire network is set up to handle these blocks, this structure is unable to accommodate various needs at various levels. Upon the development of the Notus architecture, the purpose was to address the blockchain requirements of an online network with a single network while also supporting a closed network structure.

Each block in the Notus architecture can stand in for a particular kind of transaction. Albeit not necessary, this may be the case based on the specifics of the transaction.

For Instance;
— Block Number 1: Receive payment transactions,
— Block Number 2: It may include metadata where the NFT image is present,
— Block Number 3: It may include smart contracts,
— Block Number 4: It may include account security data etc.

In order to lessen Mainnet congestion, Notus intends to host files and other data documents on many sidechains.

The process of grouping transactions during block creation works as tracks:

— If the block type is the same, we use the maximum number of transactions to construct a block and add to the chain before the reaching time limit.
— Giving the transaction of the first kind priority when multiple transactions of various types assemble in the pool. The following transaction types are recorded in a single block within the allotted block production time and added to the chain if they are identical.
— Tracking this structure in order to examine the actions of other transaction types.

4.6 — State-Based Block Structure

Smart contracts and token transfers are the foundation of blockchain technology models. For the range of transactions that can be conducted using smart contracts, programming expertise is necessary. The weaknesses of written codes started to get worse every day as the use of smart contracts grew. Due to the Mixed Block architecture we created with Notus Network, adding block types to the chain that may cater to unique requirements offers advantages to the developer in terms of creation and to the user in terms of security. The token generation structure is the most prominent illustration of state-based block architecture. It is no longer necessary to form a contract in order to create tokens with “Zero Code” thanks to the straightforward interface given to the architecture for this structure.

4.7 — Summary-Based Block Structure

The supported summary-based block structure by the Notus architecture enables adding validators to the network quickly. The framework that consistently groups all chain transactions into a single block is known as knowledge blocks. This block structure enables

new validators to join the network easily and approve blocks as validators. The greatest amount of knowledge blocks that it can accumulate in a year is 365 due to keeping the knowledge blocks on a daily basis.

4.8 — Nonce Calculation

The nonce value is the figure that needs calculation for each block that after its addition to the blockchain. This value, with its determination by using the hash technique, ensures block validity. The nonce value protects content integrity because each block's calculation of it results in an accurate calculation. This makes sure that the "Collision" results won't have an impact on the hash algorithms.

The Notus architecture computes the nonce array rather than the nonce number. The Nonce array is formed in two different ways during calculation. We refer to these two methods as "Float Calculation" and "Jump Calculation," respectively.

In order to make block security more challenging, a novel structure was designed for the Nonce calculation mechanism. However, as we increase the level of difficulty, we use more CPU power, energy, and transaction time. It is possible to conduct block creation procedures without compromising security, with less CPU power, faster transaction times, and less energy consumption thanks to the "Float Calculation" and "Jump Calculation" structures created by Notus.

4.8.1 — Float Calculation

SHA-256 for the "Float Calculation" method; the calculation number of steps (N) values is calculated with the formula below.

N= Number of Steps
A = Hex Length of the Hash Algorithm
B = Difficulty Level Length

$$N = (A - B) + 1$$

```
00000AFA5F81323BFA0B92FE9D6EF2C6ADED1951079D86CF4D167E375665B04E
F0000006A0E269A08AB04D5E5E96F8E293F18E95039FE55ACD1148381D0498B3
B600000605A6D464D92E6130AF411CFDBCE8037389DACCE9785721E9DE65A984
48E4B50A.....................................................5573F82E
35C2C07198C213F04A8C9BB56113781044050900D79C7E2C09B67A68B00000CB
80AA7AC089EAB4F40770100D110001ED1A8C1A8325DB1C54C47A6C1048000008
39E9E66E6A6310F8C787204B7DBD937C26D1BD02BE32C358B9E98D606F000000
```

Example for Float Calculation;

Using the SHA-256 hash algorithm for the new block created:

Steps

For Step 1:	8325	For step (N-2)	3258
For Step 2:	7965	For step (N-1)	1542
For Step 3:	4862	For step (N)	9104
...	...	...	...

The result list will be combined with a separator. A value such as # can be used as a separator.

#8325 #7965 #4862 ....#3258 #1542 #9104

Graphic 2: Example for Float Calculation

4.8.2 — Jump Calculation

Since SHA-256 uses the "Jump Calculation" method, it is possible to determine the calculation number of steps (N) values using the formula below.

N= Number of Steps
A = Hex Length of the Hash Algorithm
B = Difficulty Level Length

$$N = \text{Ceil}\,(A - B)$$

```
00000AFA5F81323BFA0B92FE9D6EF2C6ADED1951079D86CF4D167E375665B04E
69A0F0000006A0E28AB04D5E5E96F8E293F18E95039FE55ACD1148381D0498B3
84E94DE65B900000605A6D464D92E6130AF411CFDBCE8037389DACCE9785721A
48E4B50A.....................................................557382E
98C213F04A8C9BB56113781044050900D79C7E2C09B67A8B00000CB35C2C0E17
7AC089EAB4F40770100D110001ED1A8C1A8325DB1C54C47A6C14800000880EAA
39E9E66E6A6310F8C787204B7DBD937C26D1BD02BE32C358B9E98D606F000000
```

Example for Jump Calculation;

Steps

For Step 1:	8325	For step (N-2)	3258
For Step 2:	7965	For step (N-1)	1542
For Step 3:	4862	For step (N)	9104
...	...	...	...

The result list will be combined with a separator. A value such as # can be used as a separator.

#8325 #7965 #4862 .... #3258 #1542 #9104

Graphic 3: Example for Jump Calculation

4.8.3 — Variable Nonce Calculation

The methods employed in the Notus architecture's nonce calculation have a design in a way that their structure can change depending on the network's density. The goal is to quickly reduce the network density in this way. The Nonce computation employs the Float Calculation and Jump Calculation discussed above.

5 — Network

Similar to other blockchain platforms, Notus is a decentralized data community that joins forces to store, manage, and distribute data, information, and transaction records among nodes. All nodes linked to the network share their CPU, memory, and storage space evenly throughout the entire platform to create the Notus blockchain. On this platform, developers can create, distribute, and execute Web3 apps (DApps) that can operate decentralized with smart contracts.

The Notus architecture has a node sorting mechanism to generate a Proof-of-Randomness (PoR) sequence that provides read consistency and a verifiable time state. While creating this ranking, a leader and backup nodes selection is complete. In order to maximize throughput, the leader manages the queued transactions, creates the block, and adds it to the chain. This allows other nodes in the network to process the block without interruption. With nodes referred to as verifiers, it exchanges the accepted block and the final state signature. Validators examine, validate, and add the shared block to the chain. Each node adds their own signature to the block they approve and verify before publishing it to the network. Publications that support a consensus algorithm need voting.

5.1 — Consensus

In the blockchain network, consensus is the dialogue that makes sure all confirmed nodes arrive to the same conclusions. At least 51% of the nodes in the network must agree for there to be a consensus. Proof-of-Randomness and Proof-of-Stake are two separate consensus techniques that Notus employs.

5.1.1 — Proof of Randomness (PoR)

The Notus architecture uses a Proof-of-Randomness consensus method to secure the network. PoR uses randomness to conduct block verification. At specific times, the network's all confirmed validators gather in a queue. There is a leader and backup node selected to validate the block throughout each interval. The network's leader verifies

transactions before sending them on to other nodes. More nodes verify the block's accuracy when added to the chain. You can review the Validator's sorting system 4.3.

The Notus architecture combines Proof-of-Randomness and Proof-of-Stake consensus. As a result, the network is both faster and safer.

Benefits of Proof-of-Randomness:

- High energy efficiency
- Fast and secure network structure
- Fully decentralized
- Low carbon-neutral
- Low hardware requirement
- Have the chance to establish more nodes with a fixed staking rate

5.1.2 — Proof of Stake (PoS)

Proof-of-Stake (PoS) is the consensus method that for utilization alongside Proof-of-Randomness in the Notus architecture. To become a validator on the Notus network, the Notus token is sent as a stake to a smart contract on the network. Unlike other blockchain networks, the Notus network requires validators to stake a certain amount of Notus tokens. The Notus token put as collateral makes guarantee that validators face penalty for dishonest or negligent behavior (for efficient and reliable operation of the Network).

Instead of using stake amounts to determine reward distribution, the Notus design relies on daily transactions confirmed by validators. Only the staked status protects the network from attackers.

5.2 — Virtual Machine

An effective, separate replica of the real machine is what we mean by a virtual machine [04]. The EVM is a simple stack-based architecture. The word size of the machine (and thus the size of stack items) is 256-bit. The Keccak256 hashing algorithm and elliptic-curve computations were possible thanks to this decision. The memory model is a simple word-addressed byte array. The stack has a maximum size of 1024 [05].

Today, one can benefit from EVM to construct smart contracts (Ethereum Virtual Machine). This has a few benefits. The simplicity of conversion and execution for 1-byte Opcode instruction sets is one of these advantages (Assembly). The Solidity programming language has a drawback in that there aren't many developers and specialists using it, and

the fact that it frequently leads to hacking issues plainly demonstrates the necessity for a new programming language and framework.

Given the scale of the community and its simplicity, Notus suggests using the popular JavaScript programming language to create smart contracts. The intention is to add new commands to enable EVM and produce a Double-Opcode Notus Virtual Machine.

5.3 — NFT / Reliable NFT

NFTs, in our opinion at Notus, are more than just decorative components. We assume that NFTs actually contain a variety of digital assets, such as documents, audio, video, and photos, despite their limited use case. The fact that one can simply replicate and recreate digital content on other platforms using third-party integration solutions is the major issue we see in all of the existing NFT efforts.

The addition of a state-based NFT sidechain is a new structure to the Notus architecture. This state-based system will allow for the encrypted storage of digital files. In this manner, the NFT will only be visible to the owner, while a copy of the NFT will be visible to others. The NFT ecosystem, which includes audio, video, music, and contracts, among other things, is extensively available for use and this process is simple to manage due to this security layer provided by Notus.

One illustration is the Mona Lisa by Leonardo Da Vinci, which is on display at the Louvre. In practically all museums, replicas are on display in place of the originals. The real work keeps concealing its presence even if people damage or steal the imitation. As a result, managing the museum is simpler and less problematic.

5.4 — Wallet

The simplest way for users to experience blockchain is through wallets. Given the ability to use these wallets, users can transact on the blockchain using digital signatures. Users conduct these transactions by signing with their private keys (Public and Private Key).

Notus architecture has developed two different features for safer wallet usage and experience. These are:

5.4.1 — Heritage-Based Wallet

The issue of forgetting the wallet's private key or seed words is one of the main issues that has emerged with the adoption of the blockchain. Assumption is that about

one million Bitcoins are not available for obtaining even in Bitcoin, which has a supply of only twenty-one million, since wallet owners forget or lose their passwords. The "Heritage-Based System" is an additional feature created for wallets with "Complex Block Architecture" and "State-Based Block Architecture," which are the primary carriers of the Notus Network design.

The mechanism of operation of this feature is as follows.

Owners of wallets consent to the transfer of their assets to another wallet (either a friend's wallet address or their own wallet address) within a predetermined time frame. It can automatically transfer all of its assets to the wallet with permission to inherit at the conclusion of this time frame. The wallet owners can make sure that all of the assets in their accounts are available for transfer to the wallet to which they are entitled to inherit, even if they have lost their passwords.

One can use the Heritage-Based wallet for different purposes.

- Using as a bequest or donation of assets to private or corporate organizations in real terms.
- Using for the certainty of the payment of the debt for future debt payments.
- Offering a more secure payment infrastructure, it can enable people to act more comfortably and without hesitating.

For Instance;

- Suppose John owns a wallet on the Notus network.
- John chooses a different wallet as heir for the assets in his Notus wallet.
- John chooses the date on which system will transfer the assets in his wallet to the heir wallet.
- Even if John has forgotten the password of his wallet by the date he determined, system will still transfer his assets.
- John can use all his assets as he wishes by reaching the heir's wallet or transferring them to the person he chooses as heir.

5.4.2 — Time-Based Cold Wallet

Notus has made a secure wallet structure known as "Time-Based Wallet" available in addition to the new architecture it has created. Your Time-Based Wallet secures and locks all of the assets inside until the date you designate. Even if hostile individuals gain access to your wallet and know the private key of your account, they are unable to conduct

any transactions with the wallet prior to the date you select. You can have extremely safe wallets by utilizing the Time-Based Wallet and Heritage-Based Wallet features simultaneously.

When attempting to utilize Time-Based Wallet, you will get a warning to create a password that must have at least 8 characters and no more than 32. When you connect into your account, which is under lock on the wallet opening date, you must use the password you created in order to complete the first transaction. This extra layer of security increases the security of the contents of your wallet.

5.5 — Transaction Fee

Each transaction broadcast on the Notus network must pay a fee due to expense of fraud and abuse detection. Transaction costs vary based on the type of network operation being performed. Transfers of tokens will cost a set amount. However, for various activities (NFT storage, message transmission, etc.), determination will be through using a mathematical formula based on the transaction's data size. These transaction fees, which have a long-term lock, are transferred to the multi-signature community wallet in consideration of the Notus token market position. The release of locked tokens will be at predetermined rates decided upon by the community.

It is possible to use the unlocking and issuance of these tokens to build the Notus network or to finance initiatives that will be built on the Notus network. The community will decide when to go into lockdown.

5.6 — Block Rewards

Due to the CPU, bandwidth, and disk space that validators allocate for the network's dependable and effective functioning, Notus rewards all validators depending on their daily involvement in the system.

Empty Blocks are reward blocks that do not include any transactions but nonetheless maintain the network's security. In order to maintain security, production takes place every ten blocks. Determination of this block reward depends on the daily transaction volume since the validators process the transactions sequentially. Calculation and distribution of the daily unit transaction fee is based on how many transactions each validator processes that day. If they are under lock until the end of the designated time, the daily transaction reward for each validator in the network is subject to transfer to their wallets at the end of the day.

Calculation of the daily unit transaction cost is according to the following mathematical formula.

B = Daily Total Block Rewards
E = Daily Empty Block Amount
N = Daily New Block Generation
T = Daily Transaction Amount
R = Reward Amount per Transaction

$$R = B / (E+N+T)$$

For Example

B	20.000
E	10.000
N	15.000
T	100.000

R = 20.000 / (10.000 + 15.000 + 100.000)

R= 20.000 / 125.000

R= 0.16 NOTUS

The reward amount for a validator verifying 5.000 transactions per day:

Validator Reward = 5.000 x 0.16 NOTUS

Validator Reward = 800 NOTUS

— At the conclusion of the day, one of the randomly chosen NoVa (Validator) will receive the daily 25 empty block awards (without sharing).
— The distribution of block rewards will lock them for a month in wallets..

6 — Economy

The Notus Platform functions in accordance with the needs and goals of the community while taking into account the constraints of the economy. Notus intends to transfer resources to community and project creators over the short, medium, and long terms as part of certain programs in order to expand its presence and user base.

On decentralized platforms, assessment of a transaction cost takes place only when the program is in use, as opposed to the monthly or annual rental fees that are necessary for applications running in centralized networks. To preserve its effectiveness and functionality, the design of Notus Platform is in accordance with specific economic criteria.

6.1 — Notus Token

Notus Token is Notus Network's native asset that enables decentralized applications to interact with each other and perform transactions.

Notus Token Usage Status:

- Use for payment to the system to process transactions and store data.
- Become a part of the network by staking a certain amount of Notus Tokens and earning block rewards by running a validator (NoVa) node.
- Participate in Governance processes and contribute to the development and growth of the network by staking Notus Token.
- Get a Notus token grant by developing decentralized applications (dAPPs) on the network.

Read the token technical paper to learn more about Notus Token design.

6.2 — Staking

In blockchains backed by Proof of Stake (PoS) consensus, staking is the process of locking tokens to ensure the security of the network. For the service they render, holders of Staking Tokens receive additional Tokens (Due to the CPU, bandwidth, and disk capacity). The Notus network has a set number of stakes. Based on how well they trade each day, Notus network validators receive reward tokens. Tokens that are under lock for a predetermined amount of time will then to longer be under lock. You can review the validator reward system 5.6.

Through transferring their assets to authorized validators using the Notus Wallet, users who conduct transactions on the Notus network can receive staking rewards. The validators will have the last authority on the amount of money will be the award as a result of the delegation process. Validators and delegated wallets will both get daily automated distribution of staking rewards. Presenting the rewards will take place following the one-month lockout period.

The staking criteria will be as follows.

- To become a validator, one must stake 10,000 NOTUS permanently.
- Validators must also meet specified hardware criteria.
- Each validator can accept NOTUS delegations up to 10 times the maximum stake (10,000x10= 100,000 NOTUS).

- Each validator can set his own rates for the delegation award.
- Each validator will earn an extra ranking for the delegated tokens. This ranking right is directly proportional to the amount delegated. For instance; A node ranking with 5000 NOTUS delegate transactions gains 0.5 extra sortings compared to normal nodes.
- Validators have to distribute certain percentages (Minimum 20%) from the daily wildcard block reward to the users who perform delegate transactions.

  See "***https://docs.notus.network***" for hardware criteria.

Delegation:

- Users with NOTUS assets can delegate a minimum of 1000 NOTUS to their chosen node.
- The amount delegated must be 1000 and its multiples. (Example: 1000, 2000...5000, 8000 NOTUS etc).
- The delegated amount will give extra sorting when sorting transactions for the nodes.
- Users' rewards will have locked status for their wallets at the end of the day.
- Tokens staked for delegation will be under lock for a minimum of 1 month and a maximum of 1 year.

  See "***https://docs.notus.network***" for details of the delegation process.

To guarantee effective and regular network operation, Notus must take various safeguards. Each block that is created is also sent to other network nodes. The nodes that execute the incorrect transaction are not allowed including performing any other transactions in the network under the following system upon noticing that the content of the transmitted block has wrong modification on purpose.

- The first time a node commits an erroneous operation, it is subject to removal from the network for one hour.
- A node that commits an erroneous operation for the second time is subject to removal from the network for one day.
- The third time the node commits an error, it loses its staked tokens along with all the block rewards.

7 — Governance

Notus will contribute to the smooth operation of the global network of interconnected nodes. Each node must adapt and employ the latest architectural and resource management techniques. Only if all nodes consent to the updates containing the security patches that the architecture delivers to technical issues will this method function as intended. To ensure that the network functions properly and that the formed chains can continue without forking, each node needs upgrades.

The technical management mechanism should proceed as follows by the developers.

- To correct the faults in the architectural design.
- To prevent the backlog of transactions on the platform.
- Generating security updates against attack possibilities.
- Adding additional features required for new projects to run on the platform. It integrates updates and improvements made in the main source code into the platform. (GitHub etc.)

All choices made by the “Technical Management” to build the Notus network should cover the community’s interests and needs in mind. These choices should be in accordance with the network’s voting system that is currently in the development process as well as ideas and proposals from the developer community.

Resource management is the generic term for asset management, which includes regulations affecting token supply and value. The community’s preferences and the results of the polls will determine “Resource Management” on the Notus platform.

Resource Management rules should include the following considerations:

- The community should not lose their rights.
- Continuing the award programs effectively.
- Protection of validator rights.
- Making decisions as soon as possible while also taking the preservation of the token market value into consideration.

The Notus management mechanism will proceed as follows:

The Voting Round will take place in 3 stages.

— **Pre-Voting:** For the second round to proceed, securing 70% of the votes is necessary.
— **Applicability Voting:** Securing 51% of the votes is necessary for the third round.
— **Enactment:** Ensuring the majority of votes rate is necessary.

Voting Process:

— A minimum of 100 NOTUS is necessary to stake in order to vote.
— The staked amount is subject to removal from the wallet or locked in the wallet. (Until the cancellation of stake status)
— Following the stake transaction, the person receives the NFT of the vote in their wallet.
— Vote NFTs are acceptable for all voting. (Until the cancellation of stake status)
— In the case of cancellation of the stake, the wallet sends the NFT vote back to the original source.
— When the stake is broken, the wallet receives the staked amount back, but it is released after a week of lock.

Voting Offer Criteria:

— The above voting process are valid in order to submit a bid. However, a minimum of 100 NOTUS is necessary as a deposit in order to bid.
— Once the proposal gets enough votes, the amount received for the deposit will be released after 2 weeks of lock.
— In case the proposal does not receive enough votes, 100 NOTUS deposits are transferred to the treasury wallet, locked for a long time.
— Project development will utilize the tokens that have accrued in the Treasury wallet. (To be decided after the voting process)
— Invitations for validators are automatic during the entire voting process.

8 — Conclusion

Since blockchain technology is still in its early stages of development, there are always some unknowns associated with any new technology. This casts Notus, as well as current blockchain networks, in some doubt. For blockchain platforms like Notus, which allow decentralized processing and storage, it is possible to understand the state of uncertainty.

For instance, when we examined the evolution of the earliest mobile phones, we saw that they featured a keypad and a little screen. Nowadays, nearly all phones created as smart devices have a single screen and more sophisticated features. Here, user demands and design expectations have influenced technological development and given it its current shape.

It is impossible for the Notus platform to assert that it is faster than centralized structures when taking into account the time it takes for all nodes on the Notus network to execute transactions as well as the CPU power and storage space needs to store data. On the other hand, central structures are exempt from issues like access restrictions. However, considering the intricate architectural design of blockchain platforms, it is clear why the transaction fees needed for the transaction and storage are not less expensive than those of the centralized systems.

The administrative tasks gather in the hands of one or a small number of persons, which is the major drawback of modern centralized systems and makes it possible for the recorded transactions and data to be altered either voluntarily or accidentally. However, when we look at Bitcoin's original manifesto, we see that the emphasis on "Decentralization" has all but vanished, with the exception of a few mining pools today. Based on this reality, the Notus platform seeks to offer a platform where all miners and validators can collaborate, independent of the amount of processing power or currencies staked in the consensus architecture. Making sure that miners and validators are evenly represented in the network will be the key objective here.

References

[01] **Visa, "Transaction per Second"**
https://usa.visa.com/run-your-business/small-business-tools/retail.html

[02] **Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System"**
https://bitcoin.org/bitcoin.pdf

[03] **Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction"**
https://assets.press.princeton.edu/chapters/s2-10908.pdf

[04] **Gerald J. Popek, Robert P. Goldberg**
"Formal Requirements for Virtualizable Third Generation Architectures"
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.141.4815&rep=rep1&type=pdf

[05] **Dr. Gavin Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger"**
https://ethereum.github.io/yellowpaper/paper.pdf