Venom

Venom Blockchain

WhitePaper

Venom Foundation
March 14th, 2023
Al Sarab Tower, ADGM, Abu Dhabi, UAE

Table of Contents

Abstract 3

1. Overview 4
1.1. Scalability 4
1.2. Security 4
1.3. Regulation 4
1.4. Adoption 5
1.5. Interoperability 5

2. Dynamic Sharding Protocol 5
2.1. Shardchain 5
2.2. Split and merge events 7

3. Workchains 8
3.1. Masterchain 8
3.2. Basechain 8

4. Consensus protocol 9
4.1. Election 10
4.2. Block Generation 10
4.3. Consensus 10
4.4. Message Passing Protocol 11

5. Virtual Machine 11
5.1. Account 11
5.2. Actor model 13
5.3. Messages 13
5.4. Message types 14
5.5. Transactions 15

6. Threaded Solidity (T-Sol) 17

7. The Venom blockchain 18
7.1. The Venom Ecosystem 18
7.2. Participants 19
7.3. Basics of token economics 19
7.4. Features 21

8. The Target market 22
8.1. Proof of Reserves mechanisms 23
8.2. CBDC 23
8.3. CBDC-backed stablecoin 23
8.4. Trade finance 23
8.5. Finance for the unbanked and micro transactions 24
8.6. Community driven blockchain 24

9. Governance 24
9.1. Infrastructure Governance 25
9.2. Resources governance 25
Grants 25
Bug Bounty Program 25

10. Launch Roadmap 26
Stage 0. PoA Launch 26
Stage 1. PoS and Governance 26
Stage 2. Workchains and Interoperability 26

Disclaimer 27

Abstract

As Venom Foundation, we recognize that the emergence of blockchain technology has ushered in a new era for social and financial services. With its decentralized nature, blockchain offers efficient solutions for better transparency and accountability, improved financial inclusion, digital identity, and personal data protection. This technology's transparency and security are expected to enhance accessibility and reduce censorship, which could positively impact billions of people globally.

However, despite the many advantages of blockchain technology, it is yet to see widespread adoption in the mainstream market due to several reasons, including scalability issues, regulatory uncertainty, and insufficient understanding of the technology among the public.

At the same time, regulated markets are subject to strict rules and regulations by government authorities and financial regulators. These rules protect consumers, ensure market stability, and prevent fraudulent activities. On the other hand, regulated markets and traditional economic systems are subject to bureaucratic processes and lack transparency and openness. They also face challenges such as slow innovation, accessibility, and high fees.

Our vision at the Venom Foundation is to foster the widespread adoption of blockchain technology in regulated markets while adhering to regulatory requirements. We believe that blockchain technology can provide a more transparent, secure, and efficient alternative to traditional financial systems, and we want to help overcome the challenges that prevent its mass adoption. We believe that we can achieve this vision while maintaining the principles of decentralization that are fundamental to blockchain technology.

Our mission is to promote blockchain technology's widespread adoption by offering innovative technologies and framework that adheres to the rule of law and creates a secure environment for a broad range of users, from retail customers to institutions and sovereign nations.

To achieve our vision of fostering the widespread adoption of blockchain technology in regulated markets while maintaining decentralization and regulatory compliance, we will focus on the following key areas:

Research and Development: We will support research and development in blockchain technology to address scalability, security, and interoperability issues. We will promote the development of best practices and standards for the blockchain industry to ensure that the technology adheres to regulatory requirements.

Partnerships and Collaboration: We will collaborate with developers, financial institutions, and other stakeholders to promote the adoption of blockchain technology. We will work to establish partnerships and build bridges between the traditional financial sector and the blockchain industry to foster innovation and create new opportunities.

Governance and Transparency: We will ensure that the Venom Foundation operates with the highest standards of governance and transparency. We will establish clear policies and procedures for the management of funds and the governance of the organization. We will provide regular reports on our activities and financial performance to our stakeholders.

The foundation is committed to upholding the highest governance standards and proud to be the first blockchain company licensed by the Abu Dhabi Global Market (ADGM) and compliant with international laws.

This whitepaper outlines the Venom blockchain's features, capabilities, and potential use cases for the platform. We also highlight its advantages over other blockchain solutions, and we are excited to bring our vision to life.

1. Overview

By launching the Venom blockchain, we aim to create a safe place for everyone to build their blockchain-based solutions and conduct transactions securely and efficiently.

The Venom blockchain is designed to handle the scalability issues and poor user experience that currently hinder the mass adoption of decentralized applications. It addresses challenges such as slow block confirmations, high transaction fees, and low scalability to ensure a seamless user experience.

1.1. Scalability

One of the significant issues for blockchain technology is its limited ability to process a high volume of transactions per second. This is especially important for public blockchains such as the Venom blockchain, which must simultaneously process transactions from many actors. The current architecture of most blockchain networks cannot process the high volume of transactions required for mainstream use.

The Venom blockchain has an impressive ability for vertical scalability through its use of the Dynamic Sharding Protocol [2]. This protocol allows the network to adapt to changes in load by splitting or merging shardchains as needed, improving overall performance and achieving high transaction throughput. Each shardchain processes a specific range of contract addresses and transactions, allowing for parallel execution of transactions between groups of validators.

Furthermore, Workchains [3] enable the creation of separate blockchains for various applications, allowing the network to cater to the specific needs of different industries and applications. This strategy allows for horizontal scalability by distributing the workload across multiple specialized blockchains, each with its validator sets. With its high scalability and flexibility, the Venom blockchain is enabled to achieve exciting transaction speed, is well- positioned to allow blockchain technology's mass adoption, and provides efficient solutions for various industries.

1.2. Security

Despite the impressive results in performance, the Venom blockchain retains security and decentralization. It uses an advanced consensus mechanism [4] and a distributed network structure to maintain the decentralization and security of the network.

The Venom Consensus Protocol [4] addresses security in the Venom blockchain by using the PoS consensus based on the Byzantine fault-tolerant consensus algorithm to ensure that the network can agree on the contents of a new block even if some participants are malicious. This helps to prevent attacks on the network and ensures the integrity of the blockchain.

Smart contracts, being self-executing and autonomous, require thorough auditing to ensure accuracy and security. Auditing is crucial for maintaining trust and stability in the blockchain ecosystem. Therefore, the Venom blockchain maintains partnerships with leading audit companies and, from the start, provides the opportunity to research and train engineers to audit a smart contract code written on the Venom blockchain.

1.3. Regulation

More than technical security is needed for mass adoption. As practice has shown, even projects with impressive technical results are at risk of collapse. A relatively nascent technology, blockchain has many questions surrounding its regulation. As a result, countries have taken different approaches to regulate blockchain and cryptocurrencies. At the Venom Foundation, we are dedicated to promoting the widespread adoption of blockchain technology by creating a framework that upholds the rule of law and ensures a safe environment for various users, including retail customers, institutions, and sovereign nations. We strive to maintain the highest governance standards. Furthermore, our ultimate objective is to transform the blockchain into a decentralized public platform accessible to everyone. By providing a platform that fosters innovation, inclusivity, and transparency, we can create new opportunities and value for individuals and businesses worldwide. The Venom Foundation is committed to driving the development of the blockchain ecosystem and contributing to its growth and evolution.

1.4. Adoption

Despite the potential benefits of blockchain, there has been slow adoption in industries. The Venom blockchain plans to achieve mass adoption by offering a framework that adheres to legal regulations in a secure environment for individual users, institutions, and governments. The architecture of the Venom blockchain can handle many transactions by designing its technology to support complex and simple services that can run on the blockchain. The Venom blockchain is able to involve a mass consumer in the market by offering core services, including payment systems, Central Bank Digital Currencies (CBDCs), stablecoins, and registry solutions. Regulation and decentralization come together to provide the best of both worlds at The Venom blockchain, creating a transparent environment in which it is secure for users to transact.

1.5. Interoperability

Interoperability refers to the ability of different blockchain networks to communicate with each other and exchange information. The lack of interoperability has been one of the significant challenges facing the blockchain industry, hindering its widespread adoption. To address this challenge, the Venom blockchain uses a cross-chain communication protocol, it maintains interoperability between workchains. This allows for the exchange of data, assets, and value between workchains in the ecosystem without third-party bridges. The Venom blockchain's interoperability enables collaboration and innovation in the blockchain industry, providing new opportunities for businesses and individuals to benefit from the advantages of blockchain technology. In the next section, we are discussing some critical technologies used in the Venom blockchain, which enables us to achieve such ambitious goals.

2. Dynamic Sharding Protocol

Splitting and distributing a large database into smaller chunks, known as "shards," is a common practice used in database management. This approach, called database sharding, improves efficiency and scalability by distributing the database across multiple machines in parallel.

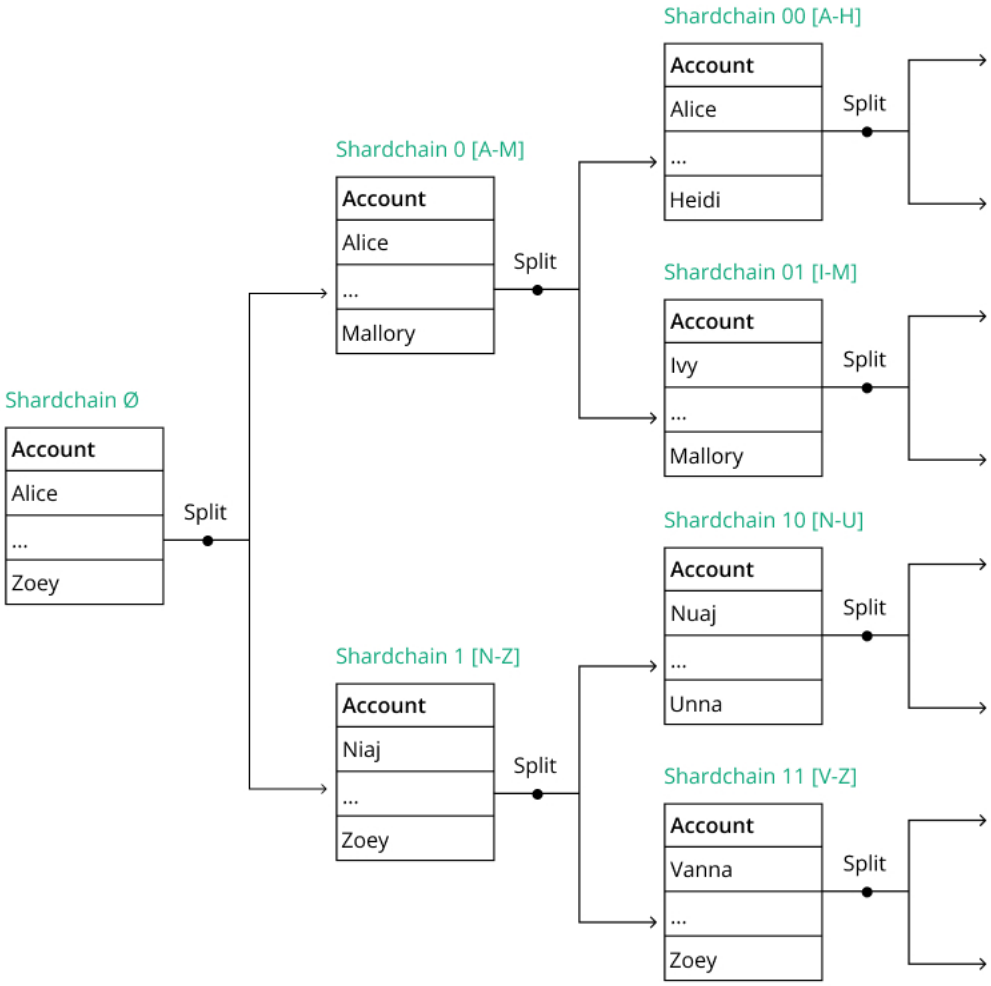
Similarly, in The Venom blockchain, sharding is used to split the execution of smart contracts into smaller threads, or "shards," which are then processed by different validator groups in parallel. Unlike database sharding, where the data is split and distributed across multiple machines, in computation sharding, the dataset remains common to all "shard validators," but they are responsible for executing different threads of the computation.

The Dynamic Sharding Protocol is a key feature of the Venom blockchain that is a solution that enables the network to dynamically adjust the number and size of shards to meet the needs of the current load.

2.1 Shardchain

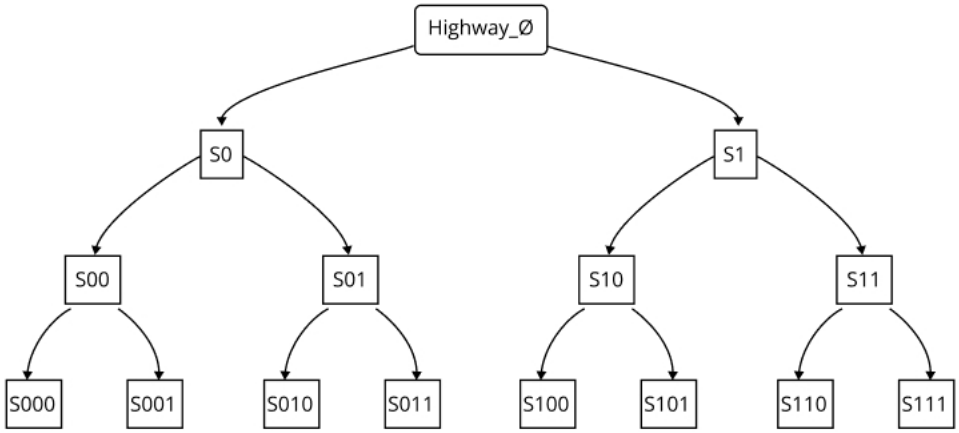
A shardchain is a smaller slice of a blockchain state responsible only for a subset of accounts defined by a binary prefix. Each range is validated by a group of validators responsible for processing a specific subset of transactions only for that range.

Initially, all transactions are processed by one group of validators belonging to a shardchain Ø. However, as the number of transactions increases and the shardchain becomes overloaded, the network triggers a split event in which the shardchain is divided into two shardchains. Then if the load on some shardchain is high, these shardchain may be further divided until the load is appropriately distributed. If the load on the network decreases, the network can trigger a "merge event" in which the shardchains are merged back into one shardchain.

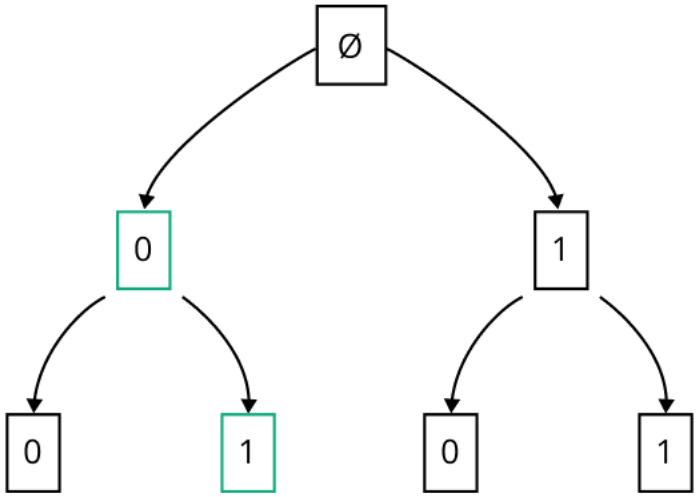


However, even though the state is divided into smaller chunks, each validator is aware of the entire state of the network in order to be able to switch and validate any shardchain dynamically. The main goal of sharding ensures distributed computation among validator groups.

The shardchains are determined by the binary prefix of the account's address. The shardchain prefix can have a length from 0 to 60 bits, and it can change dynamically. This prefix is a combination of binary digits corresponding to the path from the root node of the tree to the specific shardchain. That allows a validator to quickly determine the list of transactions that it should perform for the shardchain assigned to it.



Path to shardchain can be described as a binary tree:

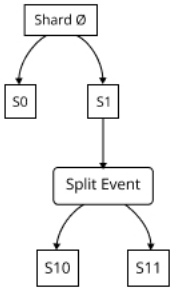


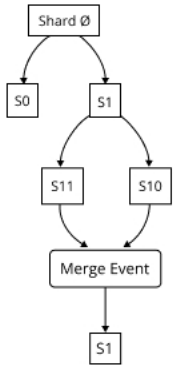
In this example, validators belonging to the 01 shardchain would be responsible for processing transactions of accounts with addresses that start with 01– the same for the other three shards in our tree: 00, 10, and 11. In this way, the tree covers the entire range of addresses.
Dynamic sharding in the Venom blockchain is a way to handle a large number of transactions by dividing the workload between multiple shardchains and achieving high transaction throughput by parallel processing. This approach allows the network to scale and effectively manage the increased load on the system.

2.2. Split and merge events

There are rules of management for split and merge events, which validator nodes follow.

Split event is announced several blocks in advance, first in the headers of the corresponding shardchain block and then in the masterchain block that refers to this shardchain block. If for 100 seconds (~50 blocks currently), the shardchain blocks are at least 90% full. Note that these values are configurable and may be tuned in Masterchain. This way, all parties concerned can prepare for the planned change and make necessary adjustments. A subset of validators [4] from a global set of validators is selected to be responsible for executing transactions for a specific range of addresses belonging to the shardchain. This subset is rotated, and they are known in advance so that every validator knows which shards it will need to validate. Finally, the split is committed into the shardchain block and is propagated to the masterchain block, updating the shard configuration of the network. A limited number of validators are selected to validate a single shard. When a shard is split into two shards, an additional group of validators is chosen from the overall validator set to ensure that performance and security are not compromised. This allows for more efficient use of resources and concurrent and parallel transaction processing, staying secure.





Merge event is determined by monitoring the sum of the sizes of the two blocks of sibling shardchains, and if, for 100 seconds (~50 blocks currently), this sum does not exceed 60% of the maximal block size, the validators will produce a block with a "want merge" flag. Note that these values are configurable and may be tuned in Masterchain. This flag tells the subset of validators responsible for the two shardchains to merge together into one shardchain. The validators will commit a "merge commit" flag in the headers of the blocks for their respective shardchains and then stop creating new blocks in the separate shardchains.The combined blocks and transactions from each of the two sibling shardchains are then used to create anew state for the merged shardchain. This allows the system to reduce the number of shardchains to match the current load, improve the efficiency and reduce costs associated with maintaining multiple shardchains.

3. Workchains

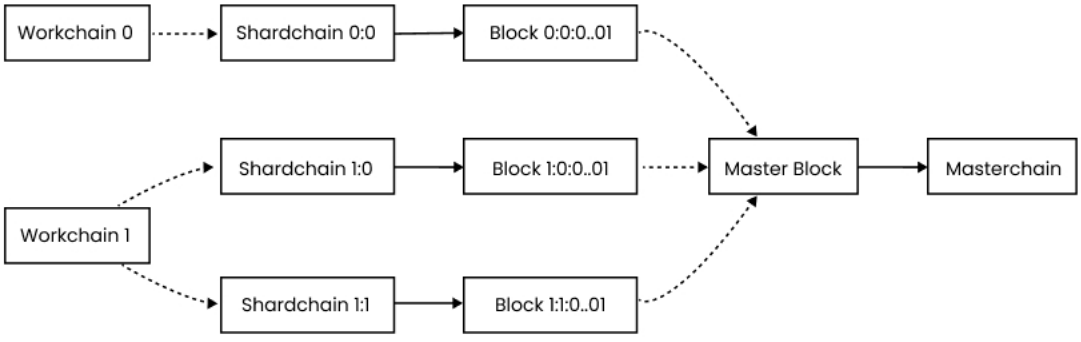
Different industries and use cases require varying security, compliance, and privacy levels. For example, a blockchain built for financial applications would require different levels of security than a blockchain built for gaming. It must implement advanced security features and meet regulatory compliance requirements such as KYC/AML and GDPR. At the same time, a blockchain built for gaming may placeless emphasis on security measures with faster transaction processing speeds and lower costs for the network. Different industries may have additional requirements for privacy. Each application has its unique needs and requirements. Creating separate blockchains for other use cases allows the network to cater to these particular needs and provide better solutions for various applications.
Workchains are specialized layer-1 blockchains that, on the one hand, can work independently and have their state transition function, virtual machine, cryptographic primitives, transaction or block structures, and native token. On the other hand, they have the property of interoperability that allows transferring assets between workchains. It is able to meet a wide range of blockchain use cases, such as CBDC and DeFi, NFT, and Gaming, among others. Workchains can take on different forms and implementations depending on the specific function they are meant to serve.
Public workchains: open to anyone to participate and build on;
Private workchains: intended for specific groups or organizations to use;
Consortium workchains: a collaboration between a group of entities.Each workchain can be customized to fit the specific needs and requirements of the application it hosts, providing greater flexibility for developers. Powered with the capability to customize their own commissions and set emission schemes, they will have complete control over their own economies.This approach allows for horizontal scalability, as the workload is distributed across multiple independent domain-specific blockchains with their specific validator set. Workchains can lead to better performance, faster transaction processing, and improved overall network efficiency.The Venom blockchain is designed as an open platform for developers to create and deploy their workchains to the Venom ecosystem.

3.1. Masterchain

The masterchain serves as the backbone of the Venom blockchain, providing a high level of security for all workchains connected to it. The masterchain validators are motivated to secure the network by staking their tokens. By being connected to the masterchain, workchains also benefit from this security, as the masterchain validators' efforts protect them.

A limited number of validators with the largest stakes are responsible for generating new masterchain blocks, even if a larger number of validators are running on the network. The rest of the validators will create new shardchain blocks, with each shardchain block being generated and validated by its group of validators. One validator may participate in several validator groups. More details about this subject are in the consensus [4] section.

In the Venom blockchain, the masterchain serves as a layer-0 chain, facilitating coordination and communication among workchains, shardchains, and accounts. It is responsible for the message [5.3]routing, maintaining the network configuration, and information about validators, their stakes, and election rounds. It stores and distributes the current shard configuration and the latest block hashes of each corresponding shardchain. Shardchains generate new blocks almost simultaneously, while a new block of the masterchain is generated roughly one second later as the masterchain block must include the hashes of the most recent blocks of all shardchains, which ensures that the blocks are finalized.



3.2. Basechain

At launch, The Venom blockchain consists of two networks: the Masterchain and the Basechain. The Basechain is the first layer-1 workchain for end-users, supporting dApps and serving as the platform for executing smart contracts. Both networks employ the Threaded Virtual Machine (TVM) for smart contract execution, with the Basechain offering lower storage and execution fees than the Masterchain.

4. Consensus protocol

In distributed systems, where multiple parties are involved, it is critical to ensure the security of an agreement process on specific aspects of the system, such as the current state, which transactions should be included in a block, and who will update the blockchain's state. Different parties may have various views of the same system or act maliciously or unreliable. Without consensus, conflicts and inconsistencies can lead to forks in the chain.

The primary goal of the consensus protocol is to provide a mechanism for all the parties involved in the network to reach an agreement on the current state of the blockchain and to ensure that all the transactions included in a block are valid and that the blockchain state is updated consistently and securely on all levels (shardchains, workchains, and masterchain).

The Venom blockchain utilizes a Proof of Stake (PoS) consensus mechanism with The Byzantine fault-tolerant (BFT) algorithm to reach a consensus agreement between validators.

The validator maintains the network's security by staking its VENOM tokens and committing to participate in consensus with other validators. The validator plays an essential role in maintaining the network's security through staking Venom tokens and actively participating in the consensus rounds with other validators. The validator proposes candidate blocks and votes on blocks proposed by other validators.

Participants with minimum VENOM can participate in the validation process through delegated staking pools. This mechanism allows network participants to delegate their stake to other participants or organizations who will serve as validators. Token holders can stake their tokens in specific validators — the more tokens staked in a validator, the more weight it carries in the consensus voting process. It gives token holders a say in who becomes a validator by choosing which validator candidates to delegate their stake. This helps to ensure that the validator set is representative of the interests and goals of the broader community.

There are three main types of validator sets:

Overall validator set. The weight-sorted validator list of all validators chosen to participate in the validation process.
Masterchain validator set. The list of validators with the largest stake is chosen from the overall validator set.
Shardchain validator set. The group of validators chosen from the overall validator set maintains block processing for a specific shardchain.

The protocol uses a round-robin role transfer system where validators take turns generating blocks to prevent a single group from monopolizing consensus. The consensus algorithm is executed by each shard using its group of validators.

The protocol proceeds through a series of rounds, each with a set of validator nodes responsible for proposing, validating, and committing blocks. If a proposed block receives approval from 2/3 of the validator nodes, it commits to the blockchain. If the proposed block does not receive approval in a specific time, it is skipped, and the next round begins.

Consensus algorithms can be broadly divided into two classes: those that allow for the creation of multiple chains at the same time (forks) and those that do not allow for forks. In other words, a consensus may have probabilistic or deterministic finality.

Deterministic finality refers to the idea that once a transaction has been committed in a block and added to the blockchain, it is considered final and cannot be reversed. This is important for the security and integrity of the network, as it ensures that transactions cannot be altered once they have been recorded on the blockchain. For example, in the context of Bitcoin, a transaction is considered to be final only in probabilistic nature. The transaction's reverse probability decreases as more blocks are added to the chain after it.

The Venom Consensus Protocol belongs to the deterministic finality class of algorithms. It ensures the finality of transactions at the commitment stage. Using a BFT makes it almost improbable for forks to occur, as they can only happen in the event of incorrect behavior by a majority of validators.

Components

The consensus protocol can be decomposed into several distinct components, each responsible for a specific protocol aspect:

1. **Election:** A selection of the overall validator set;
2. **Block Generation:** A creation and verification of blocks;
3. **Consensus:** A reaching consensus;
4. **Message Passing Protocol:** A passaging messages between validators.

4.1. Election

First, the consensus protocol must determine which participants are eligible to serve as validators through the election process. The smart contract implements a proof of stake-based election algorithm for selecting a weight-sorted validator list, where the stake determines the weight.

The election contract uses various factors to select validators, including the validator's stake size, the min/max number of validators allowed, the min/max stake size, and the maximum difference between the largest and smallest validator stakes. This accounting for these factors helps to ensure network security by maximizing the stake amount and the number of active validators.

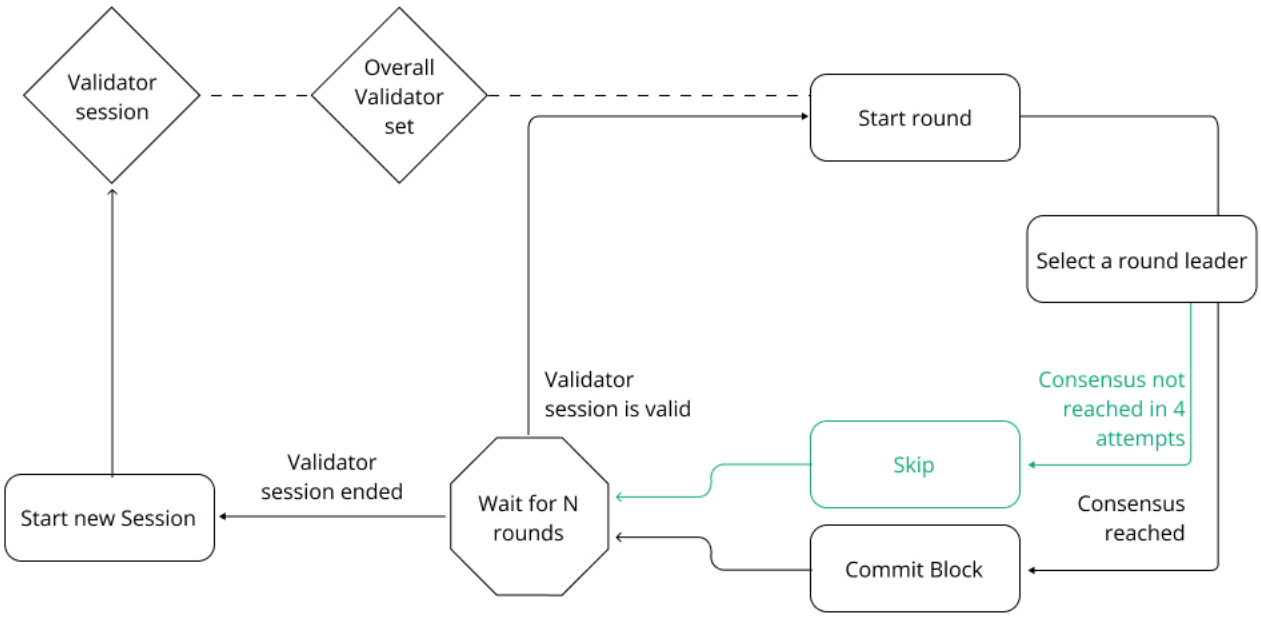
The election process gives the overall validator set to start the validator session. The selected validator set generates blocs by following the consensus algorithm during the validator session.

The Validator Session

The Validator Session goes through several rounds of block generation. During block generation rounds, the validator executes the consensus algorithm [4.3], resulting in committing the elected block to the blockchain.

Validators will have several attempts to commit a valid block to the network before it is considered a failure, and the process must start over with new lead validators. During each attempt, a limited number of validators can propose a block for consideration by the rest of the network.

If a validator misses their turn or produces an invalid block, they may be punished by having their stake slashed.



4.2. Block Generation

Before a validator proposes a block to the network, it must first collect and ensure that the block is well-formed and valid according to the block generation rules. These rules include the size of the block, the volume of transactions that can be included in a block, the time between blocks, the block header and transaction format, etc. The block generation component is ensured for creating and validating new blocks in a blockchain network.

4.3. Consensus

Byzantine Fault Tolerant (BFT) algorithm is part of the block generation round and is responsible for reaching an agreement on block production.

The consensus process includes several stages of reaching an agreement:

1.Candidate block generation: Validators, which have block generation priority for the round, generate a new candidate block. The candidate is sent to the Approve phase to other validator nodes as soon as the candidate is generated.

2. Candidate block approval: The candidate block is collected and checked for corruption by each validator node. If a block is approved, it is signed for approval by each validator and broadcast to the network. A block is considered approved by a node when it receives more than 2/3 of the approval messages and goes to the Vote phase.

3. Voting attempts: Several voting attempts are carried out, each with a time limit. The lead validator for the attempt selects a candidate block for voting, and other nodes are notified. Each validator node then sets a block to vote for according to the leader validator's a proposed block. A validator is not required to vote for the proposed block and can choose a different one, but a priority block is preferred due to speed performance. If any approved block receives more than 2/3 of the total validator weights during the voting process, it becomes the candidate for signing (pre-commit block). If two attempts propose different pre-commit blocks, the latest one prevails.

4. Block committing: The signing begins as soon as a round attempt yields a pre-committed block. The validator that gets the pre-committed block in the current round signs it and broadcasts it to other validators. When a particular validator receives more than 2/3 signatures from other validators, it switches to the next round, and commits the signed block to the blockchain. If no block is committed in the current round, the round is considered failed, and the process moves to the next round.

4.4. Message Passing Protocol

The message-passing protocol is the network-layer protocol used for communication and coordination among the validator nodes in the network. Validators use it to broadcast messages containing candidate blocks, approvals, votes, and signed blocks to other nodes in the network. It is also used to synchronize the validator session state among the nodes in the network. The message-passing protocol does not implement the consensus algorithm itself. However, it serves as a means of communication and coordination for the validator session higher-level component responsible for making decisions related to the consensus process.

Note messages discussed in this section are not the same messages which accounts send to each other. Messages of this protocol are network-layer messages and don't have on-chain representation.

The Message Passing Protocol gives a way to synchronize the chain's state and communicate to reach a consensus agreement.

5. Virtual Machine

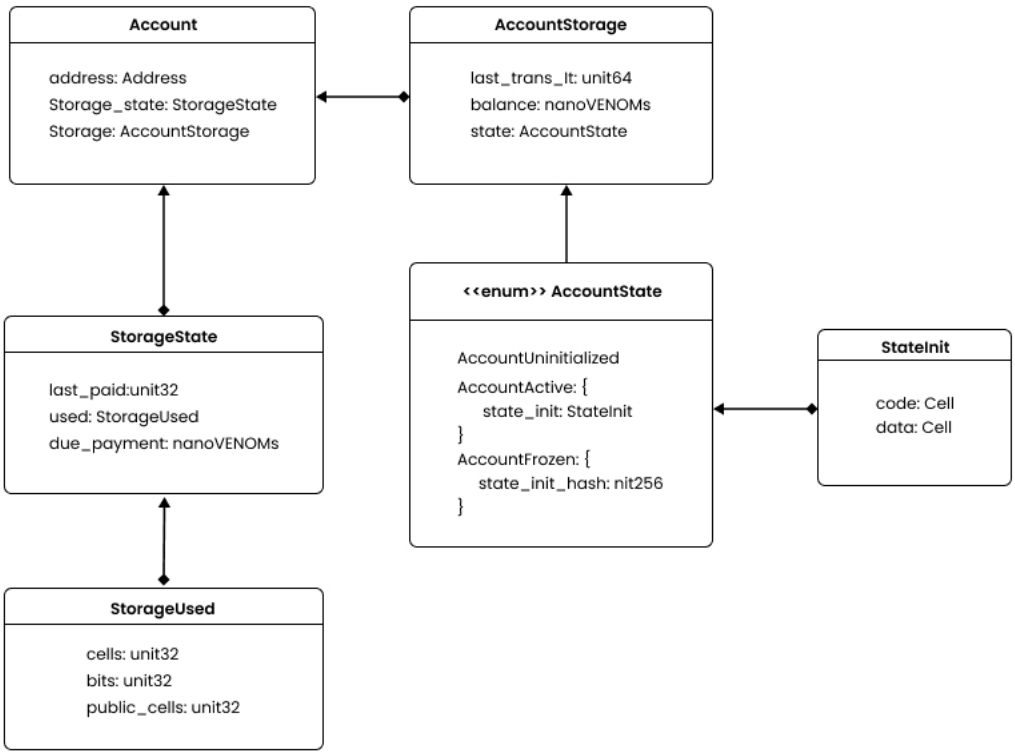
The Venom blockchain provides a way for smart contracts to be executed on TVM (Threaded VirtualMachine), a Turing complete machine on the basis of its ability to execution of machine- level instructions. Note Threaded Virtual Machine is used to execute smart-contract code in the masterchain and basechain[9]. Other workchains on the Venom blockchain may use other virtual machines instead of the TVM (e.g.,EVM).By design, TVM has an asynchronous model of communication between accounts. Each account can only affect the state of another account only by sending a message.

5.1.Account

An account on a blockchain serves as a unique identifier for a user, with a corresponding address, balance, and the ability to transfer funds and call smart contracts. It can also refer to a smart contract with behavior (code) for changing data storage.There is no distinction between accounts and smart contracts in the Venom blockchain. Every account is a smart contract with code, and there is no concept of an externally-owned account (owned by key pair) in the traditional sense. All accounts can hold a balance, perform code, and call each other. This approach is called Account abstraction and allows for authentication through other means beyond external ownership.Since every account in the Venom blockchain is a smart contract, the contract's code can include any authentication logic necessary to verify a user's identity. The flexibility of smart contract code allows for a wide range of authentication options beyond traditional private key ownership.

Account structure

Account's structure is composed of three main components: Address, StorageState, and AccountStorage



Account (smart contract) uses its address (Address) as the entry point for incoming messages and a unique identifier for its storage, which holds data such as the balance and state. It contains two parts: the first is the identifier of the workchain where an account is deployed (masterchain = -1; basechain = 0;),and the second is the hash of the initial code and data of the smart contract.hash(init_code, init_data)The storage state (StorageState) serves the purpose to fee calculation [5.5]. It contains information about how much data is placed in the contract storage.The account storage (AccountStorage) contains information about the account's balance, the last transaction made, and the current state of the account. The state can be "Uninitialized," "Active," or"Frozen."The Active state indicates that a smart contract was initialized, and code and data are present in an account's state. A smart contract's code and persistent data are stored together as part of its persistent state. In the Uninitialized state, the account does not have any code or data associated with it and is essentially empty. The Frozen state means that the account has been frozen, and the account's code and data are sealed by a hash.

Initialization

A smart contract can be deployed by sending an external message [5.3] containing the code and initial data of a future account to the network. Before sending that message, the sender should increase a balance of an account address of the deployable contract.The deterministic derivation of an account address is a crucial aspect of distributed programming in TVM[5.2], as it enables participants to calculate the same address given the same inputs independently. This allows for the pre-calculation of an address before deploying a smart contract on the network, for example, enabling the transfer of tokens to a non-deployed contract.Another smart contract also can initiate the deployment of a new smart contract by sending an internal deploy message [5.3].

Upgradability

The original idea behind smart contracts is that they are self-executing contracts with the terms of the agreement written directly into code. The agreements and the code contained therein exist in a state that can not be altered. However, the immutability of smart contracts can also be a problem if errors are discovered in the code or if the contract needs to be updated to reflect changes in the real world. The upgradability of smart contracts allows for the improvement and maintenance of smart contract functionality over time.
For example, Ethereum has attempted to address the problem of upgrading smart contracts by separating a contract's storage and logic into different parts. It requires building complex systems contracts and involves tricks with DELEGATECALL instruction.

Modern smart contract platforms, such as NEAR, Solana, and the Venom blockchain, use virtual machines that allow you to achieve upgradability through the use of the upgrade method on contracts.TVM allows for updating smart contracts by using the SETCODE instruction, which enables the setting ofa contract's code even after it has been deployed. This feature makes it more straightforward for developers to incorporate upgradability into their smart contracts, as compared to the EVM. The update process is performed by sending an internal or external message to the target address, making it a public and transparent process like any other transaction on the network.

5.2. Actor mode

The Actor model is a mathematical model of concurrent computation that is often used in distributed systems and in programming languages such as Erlang. It is a way of organizing and structuring the behavior of concurrent processes or actors in a distributed system.

In this model, an account of the Venom blockchain can be thought of as an actor. Like the actor, the account has a unique address, can send and receive messages, change its state, change its behavior (upgradability), and even spawn other accounts (initialization).

This model emphasizes the concept of message-passing concurrency, which allows for the isolation and parallelism of actors. As a result, it provides a way to handle the complexity of concurrent and distributed systems by breaking them down into simpler components that can be composed to form more complex systems.

TVM utilizes the actor model to handle interactions between accounts, which is different from how EVM-based networks operate. In EVM, transactions are executed one by one, and each must be completed before the next one can start. From the actor model's perspective, the way transactions are processed in EVM-based networks could be more efficient. This is because all smart contracts on the network are united into one state and can be considered as a single actor within the system, while only external actors (user, web service, any off-chain actor) are considered separate actors. High demand from external actors leads to delays and increases the cost of maintaining a network.

In contrast, the Venom blockchain uses an asynchronous communication model, where a message is away for a sender to initiate an action on an account (smart contract) and potentially change its state. Messages are sent to accounts and contain instructions for the execution of a smart contract. Theoretically, each account can operate independently and interact with external actors separately from other accounts. However, to improve efficiency, accounts are grouped into shards as part of the dynamic sharding protocol [2].

This approach allows contracts to execute in an asynchronous mode, where threads of execution can run in parallel and participants don't know about the current state of each other. TVM does not need to wait for calls between contracts located in different shards to be processed so long as no dependencies link those contracts.

5.3. Messages

It is possible to determine the following roles of interacting actors in the Venom blockchain:

An external actor is an actor without an internal representation in TVM interacting with the Venom blockchain network (e.g., validator node, wallet, etc.). Since there is no internal representation of an external actor, it does not have an on-chain address; accordingly, messages from it don't have a sender. Typically, an external actor has a key pair that signs messages and sends them to the network's internal actors (accounts).

However, an external actor can also be any off-chain service, such as an API, web service, or oracles, that interacts with the network by sending unsigned messages to internal actors if the logic of the smart contract allows it.

An internal actor is an account that exists at the TVM level. It can process incoming messages, modify its internal state, and generate outgoing messages resulting from the processing.

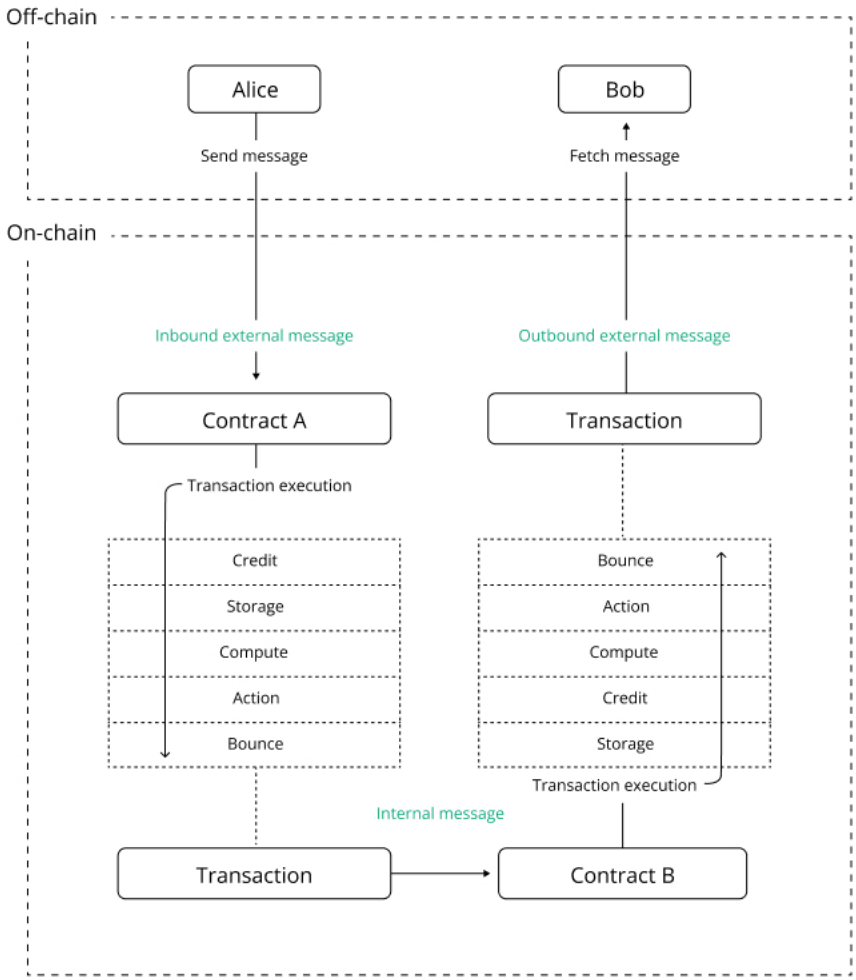
5.4. Message types

External Inbound messages are sent from external actors to internal actors.
Example: Oracle sends a price rate to a smart contract. Another one is The user with a keypair sends a message to the wallet account to transfer funds.

Internal Inbound/Outbound messages are sent between internal actors (accounts) within the blockchain.
Example: As a result of the external inbound message, the wallet account changes its balance and sends an internal message to the other wallet account.

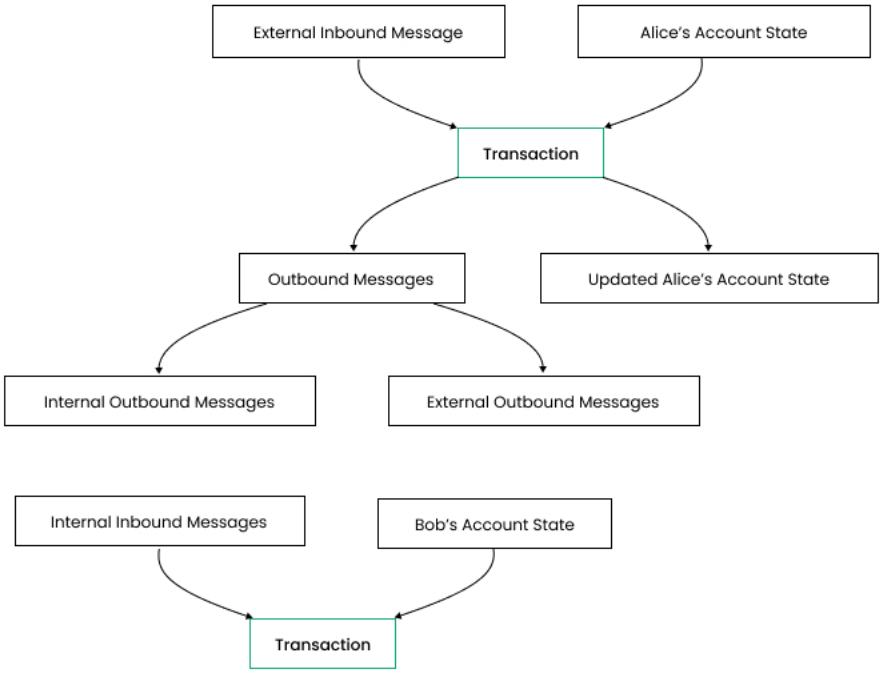
An account can send up to 255 internal messages to other smart contracts within one transaction. This constraint can be addressed by using a recursive pattern of sending messages to itself, which allows for efficiently batching more actions. Still, it will be split into multiple transactions and doesn't require additional external messages.

External Outbound messages, also known as "events," are produced by internal actors and can be subscribed to by external actors.
Example: The wallet account emits the event about receiving funds, and the external service catches it.



5.5. Transactions

A transaction is a direct result of the processing of exactly one inbound message by a recipient account code. When an inbound message is received by an account, it leads to the computation of the account's new state and the possibility of generating one or more outbound messages with the account serving as the source. The inbound message and the previous state of the account serve as inputs for the transaction, while the generated outbound messages and the next state of the account serve as outputs. This relation can be represented as a Directed Acyclic Graph (DAG).



5.4.1. Transaction phases

A transaction is a multi-step process composed of several distinct phases, each with its specific purpose. Each phase is a logical step in the message execution and may either complete successfully or result in an error. If an error occurs, the next stage not be executed.

The purpose of **the credit phase** is to add the value of the received message to the account's balance. The value added to the account's balance is the entire value passed with the message for internal messages. And the value added for external messages is a constant amount of 10000 gas. The storage phase is responsible for collecting storage payments for the account state, which includes the smart contract code and data.

The storage phase is absent if the transaction is sent to deploy a new smart contract, which did not exist before. During this phase, the smart contract may be frozen if its balance is insufficient to pay the storage fee [5.5].

The computing phase is where the smart contract code is invoked inside an instance of TVM with appropriate parameters, including the inbound message and the account's persistent data. This phase terminates with an exit code, new persistent data, and an action list, which includes outbound messages to be sent. The processing phase may lead to creating a new account (uninitialized or active) or activating a previously uninitialized or frozen account. The gas payment, equal to the product of the gas price and the gas consumed, is exacted from the account balance.

The action phase is where the actions from the action list are performed if the smart contract is terminated successfully (with exit code 0 or 1). Suppose it is impossible to perform all the actions, for example, because of insufficient funds to transfer with an outbound message. In that case, the transaction is aborted, and the account state is rolled back.

The Bounce phase is triggered when a transaction is aborted, and the inbound message has its bounce flag set. This phase involves automatically generating an outbound message, with the bounce flag clear, and sending it back to the original sender. The value of the original inbound message, minus any gas payments and forwarding fees, is transferred to this generated message, which has an empty body.The execution of a transaction requires payment of various types of fees. Each kind of fee serves a purpose, such as incentivizing validators to maintain the correct operation of the network, perform transaction execution, and store contract data on their nodes. Also, it serves as a measure to restrict spamming and malicious attempts to slow down the network. Note an external message is not a value-bearing message. Only an internal message can transfer value between accounts and increase its balance in the credit phase, and only after that are all fee payments due from the account balance.

5.4.2. Transaction fees

Forward message fee

The External Inbound Message Fee is a fee not associated with any of the phases of transaction execution. This fee is incurred when a transaction is initiated by an external message, and it compensates the validator as a charge for forwarding the message.

$$lump\_price + bits * bit\_price + cells * cell\_price$$

The **bits** and **cells** values are derived from the tree of cells representing the message, with the root cell not being counted.

The **lump_price**, **bit_price**, and **cell_price** values are expressed in nanoVENOMs and found in the global configuration parameters and can only be changed by a vote of validators.

Storage fees

The storage fee is calculated based on an account's storage size measured in bytes and cells. It compensates the validator for maintaining and storing the account's data on the network.

$$(bits * bit\_storage\_price + cells * cell\_storage\_price) * \Delta$$

The **bits** and **cells** values represent the number of bits and cells in the storage state structure [5.1].

The **bit_storage_price** and **cell_storage_price** values are expressed in nanoVENOMs and found in the global configuration parameters.

Δ - the number of seconds since the previous due storage payment at the moment of the transaction.

The storage fee is charged whenever an account receives a message. If an account's balance is less than the storage fee, the account is frozen. The account can be unfrozen by passing a special message containing the code and data of the frozen account.

Gas fees

During the computing phase, a gas fee is charged for the computations performed by the smart contract code. The gas fee is intended to compensate the validators on the network for the computational resources they are using to execute the called smart contract code.

The gas fee is calculated according to the following formula:

$$gas\_fee := (10 + b) * gas\_price$$

b is the instruction length in bits.

gas_price determines the cost of each unit of gas in nanoVENOMs.

Gas fees are only applicable if the TVM compute phase is initialized for a transaction. If the compute phase is not initialized, these fees may be skipped.

Action fees

Action fees are used to pay for creating and routing internal and external outbound messages in the action phase. These fees are comprised of all costs for external outbound messages, the first fraction of fees for internal outbound messages. The second fraction of internal outbound message fees is sent with the internal message for further processing.

The calculation of action fees is as follows:

$$action\_fees := \sum_{i=1}^{n} external\_action\_fee_i + \sum_{i=1}^{m} internal\_action\_fee_i$$

The transaction will only succeed if the condition **(n + m) < 255** is met, where **n** and **m** represent the number of external and internal actions. Otherwise, the transaction will fail.

$$external\_action\_fee := msg\_forward\_fee$$

The first fraction of fees for the internal outbound messages is calculated by the formula:

$$internal\_action\_fee_a := msg\_forward\_fee * first\_frac$$

first_frac is expressed in nanoVENOMs and determines the fraction of the fee that the current set of validators receives.

The following formula determines the second fraction:

$$internal\_action\_fee_b := msg\_forward\_fee * second\_frac$$

second_frac is expressed in nanoVENOMs and determines the fraction of the remaining forward fee that intermediary validators receive.

A bounce message also is subject to the action fee as an internal outbound message. In all cases, the **msg_forward_fee** is calculated as the forward message fee [*].

6. Threaded Solidity (T-Sol)

Multiple high-level programming languages can be utilized in conjunction with the native "assembly "language on the TVM platform. One is T-Sol (Threaded Solidity): the asynchronous dialect of solidity programming language adapted to TVM's Actor Model.

The Actor Model is closely related to asynchronous programming, based on the same principles. Asynchronous programming is a paradigm based on non-blocking I/O and concurrency, where a program can perform other tasks while waiting for input or output operations to complete. As in the Venom blockchain, calls to accounts have non-blocking nature and can be executed concurrency by shards.

"Classic" Solidity, used in EVM-like blockchains, does not have built-in support for concurrency. Still, it has quickly gained popularity as the primary language for developing smart contracts on the Ethereum blockchain. Because of this popularity, many resources are available for learning Solidity, including tutorials, documentation, and example code.

The Venom blockchain utilizes T-Sol, a programming language designed explicitly for the TVM Actor Model, and uses the same syntax as the Solidity language. It provides built-in support for message-passing, state management, and creating, updating, and deleting actors (accounts). And the language is widely adopted by developers, making it easy to use and understand.

T-Sol supports several features to support the Actor model:
1.**Actor management:** Managing actors, including creating new actors and deleting existing ones;
2.**Message passing**: Message passing, such as sending messages to other actors and receiving messages from other actors;
3.**State management**: Managing the state of actors, including reading and modifying the state of an actor;
4.**Access control**: Functionality for access control, such as defining which actors can read or write to another actor's state;
5.**Interoperability**: Sending messages between actors on different shardchains and workchains as well;
6.**State isolation**: Actors should be isolated from each other so that the failure of one actor does not affect the execution of other actors.

7. The Venom blockchain

The Venom blockchain is a decentralized network built on innovative technology that provides fast, secure, and scalable solutions for various industries. The technology behind the Venom blockchain has been tested and proven in the real world, starting from R&D in 2017 and progressing to the first stable network called Everscale with a bandwidth of over 54,000 transactions in a close-to-live environment and4,000 in the mainnet. The community and core development teams have contributed to the network's improvement by implementing concepts, fixing errors, and enhancing security.

The Venom Foundation is a non-profit organization responsible for managing the development of the Venom blockchain and promoting its adoption. It seeks to bring new life to the Everscale-born technologies and core concepts by combining them with intelligent management and compliance. The foundation aims to facilitate the development of robust and decentralized networks that offers efficient solutions for various industries. It is committed to continuously improving the main network's functionality and security while ensuring compliance with international laws and regulations.

To achieve these goals, the Venom blockchain was created as a safe place where blockchain innovation can meet mass adoption. The Venom Foundation aims to create an ecosystem that supports the development of decentralized applications and solutions for various industries. This approach enables businesses and individuals to leverage the power of blockchain technology and achieve their goals more efficiently and cost-effectively.

The foundation is dedicated to building a network that is user-friendly, accessible, and efficient. By providing the necessary tools and resources, the foundation aims to encourage developers and businesses to build decentralized networks (workchains) in the Venom network. The foundation fosters partnership sand collaborations with other blockchain projects, businesses, and organizations to promote adoption and drive innovation. The foundation believes working together can build a more decentralized, secure, and equitable future.

7.1. The Venom Ecosystem

To provide a seamless user experience and promote the adoption of blockchain technology, Venom blockchain offers a comprehensive ecosystem that includes various tools and services. These tools are designed to make it easy to interact with the blockchain and access its features. The Venom blockchain provides all the necessary products, such as wallets, explorers, a ready-made DeFi ecosystem, bridges, and developer tools. These technologies are combined into one ecosystem to use easily.

Here are some of the base components of the Venom ecosystem:

Venom Wallet is a secure, non-custodial wallet that allows users to securely store, send, and receive VENOM and other digital assets. It provides an intuitive user interface and enables users to manage their assets easily.

Venom Scanner is an explorer that allows users to track transactions and monitor the status of their transfers on the network. It provides real-time data on block production, transaction confirmation times, and other key metrics.

Venom Pools allow users to stake their VENOM tokens and earn rewards for helping to secure the network. Validators are responsible for confirming transactions and maintaining the integrity of the network, and stakers can earn a share of the block rewards for supporting this process.

In addition to these key components, the Venom ecosystem also includes a range of other products and tools that offer a seamless experience for users and developers alike. The Venom Foundation Developer Program attracts developers to build products to demonstrate the capabilities of the Venom blockchain from the start.

The Venom Foundation Developer Program has already supported several products in the Venom ecosystem, including:

Venom Bridge is a cross-chain platform enabling seamless asset transfer between blockchain networks.

The bridge platform features architecture designed not only for token transfers but also for any cross-chain data transfers, including NFTs, cross-chain smart contract calls, and even DAO execution of decisions performed in different networks.

The bridge is operated by a set of independent validators called relayers, monitoring all supported events coming to the bridge in all connected networks.

Web3World, is a decentralized exchange that allows users to trade digital assets without the need for intermediaries.

NFT Marketplace is a platform for buying, selling, and trading non-fungible tokens (NFTs) on the Venom blockchain.

All of these products were developed by third-party teams participating in the Developer Program, and they serve as examples of the possibilities for building on the Venom blockchain. The Venom Foundation continues to support the development of innovative and impactful applications and smart contracts on the network through the Developer Program and other initiatives.

Whether you are a developer looking to build on the Venom blockchain or a user looking for a secure and efficient way to manage your digital assets, the Venom ecosystem has something to offer. With a commitment to innovation, security, and user experience, the Venom ecosystem is poised to significantly impact the world of blockchain technology.

The Venom ecosystem continues to grow and evolve through partnerships with other industry leaders and innovative startups.

7.2. Participants

The Venom blockchain is a community-driven network that empowers its participants to shape the future of the ecosystem. The network's success depends on the engagement and contributions of its users, validators, and developers.

Users are at the core of the Venom blockchain, and their participation is essential to the network's success. By sending transactions and utilizing decentralized applications (dApps), users generate value and help to expand the network's capabilities. By participating in governance through voting and decision-making processes, users can shape the direction of the network.

Validators are essential to the security and functionality of blockchain networks. These participants are responsible for verifying and validating transactions and block-producing by a consensus mechanism that ensures the network's integrity. Validators are critical to maintaining the distributed nature of the blockchain, as they help to prevent fraudulent or malicious transactions from being added to the network. With validators, the Venom blockchain network is protected from attacks and struggles to maintain its decentralized nature. Therefore, validators play a critical role in supporting the growth and evolution of blockchain technology.

Developers are essential to the growth and evolution of the Venom blockchain. They create and launch products that leverage the network's capabilities and help to expand its functionality. By improving the protocol's codebase and developing new solutions, developers contribute to the network's long-term success and facilitate its adoption by a wider user base.

The Venom Foundation is also an important participant in the Venom blockchain ecosystem. As a non-profit organization responsible for managing the development of the network, the foundation commits to promoting its adoption and ensuring its compliance with international laws and regulations. By coordinating with users, validators, and developers, the foundation helps to facilitate the network's growth and evolution and ensure its long-term sustainability.

The Venom blockchain's success is driven by the engagement and contributions of its participants, including users, validators, and developers. The network's ability to provide value to these groups is essential to its continued growth and development.

7.3. Basics of token economics

7.3.1. The Venom token

The VENOM token is the primary currency used within the Venom blockchain. It is designed to act as a utility token that provides several essential functions within the ecosystem. One of its primary functions is to serve as a settlement method for participants within the network, enabling them to pay network fees and settle transactions using the VENOM token.

Also, The VENOM token is intended to perform several key functions in the network, including:

Incentivizing validators: The VENOM token rewards validators who contribute to maintaining the network's integrity. Validators receive a reward in VENOMs for each block they produce, encouraging them to act honestly and consistently. The block reward consists of an independent, configurable reward for each block and the transactions' fees [5.4.2] collected per block.

Protecting against Sibyl attacks: The network uses a Proof-of-Stake (PoS) mechanism [4] to safeguard against Sibyl attacks. Participants must stake their tokens to become validators, and the number of validators a participant can create is limited by the number of tokens they hold.

Delegated staking: Participants in the network can delegate their tokens to other participants who want to become validators. This process is referred to as "staking," It enables token holders to participate in the network's consensus mechanism by delegating their tokens to validators responsible for validating transactions and creating new blocks. By delegating tokens, the community can effectively control the list of validators and ensure that the network remains decentralized. This helps to prevent a small group of validators from having too much control over the network and potentially engaging in malicious behavior.

Governance: The network will introduce governance mechanisms, allowing participants to propose and vote for proposals using the VENOM token. This will help to decentralize decision-making and give control to the community.

The VENOM is subdivided into the smallest transferable units, called NanoVENOM.

Unit	Decimal Places	Conversion to NANO VENOM	Conversion to VENOM
NanoVENOM	0	1	0.0000000001
MicroVENOM	3	10^3	0.000001
MilliVENOM	6	10^6	0.001
VENOM	9	10^9	1

The VENOM token does not assign any form of ownership, such as shares, participation, or entitlements to profits, dividends, or investment returns.

7.3.2.Total supply

The Venom blockchain has an inflationary model, meaning no fixed maximum supply of tokens exists. However, the Venom Foundation is exploring ways to transition to a deflationary model.

One possible way to transition to a deflationary model is through part of the transaction fee burning (a crypto term for destroying). Fee burning permanently removes certain tokens from circulation by sending them to an address with no known private key, rendering them unusable.

This is not a final proposal. The transition to a deflationary model would require careful consideration and planning to avoid any negative impacts on the network's stability and sustainability. The Venom Foundation will continue to evaluate the network participant's behavior and explore the best approaches after launch to maintain a healthy and thriving ecosystem for all participants

7.3.3.Token Release

The Venom blockchain's initial supply of tokens for issue during the mainnet launch is 7,200,000,000VENOM. Of this initial supply, 15.5% (1.116B) is for unlock and immediately available, while 84.5%(6.084B) is under lock. The locked tokens include 10% (720 million) of the initial supply as a stake of the initial validators.

The projected annual inflation rate is ~1% (~72,000,000 VENOM)

Category	Allocation	VENOM	The Unlock Launch	Cliff	Linear Vesting
Community	22.0%	1,584,000,000	10.0%	6	90 Months Linear
Ecosystem	28.0%	2,016,000,000	10.0%	6	90 Months Linear
Foundation	15.0%	1,080,000,000	0%	24	72 Months Linear
Early Backers	7.5%	540,000,000	0%	12	48 Months Linear
Team	7%	504,000,000	0%	12	48 Months Linear
Public	0.5%	36,000,000	100%	0	0
Market Liquidity	10.0%	720,000,000	100% (Strategic Unlock)	0	0
Validators	10.0%	720,000,000	100% (Locked in Stake)	0	0
Total	**100.0%**	**7,200,000,000**	**1,836,000,000 VENOM**	-	-

7.4. Features

Account Abstraction

Other blockchains typically represent wallet accounts as simple addresses controlled by a private key, and this approach is called external ownership.

The Venom blockchain offers a significant competitive advantage. With every account in the Venom blockchain being a smart contract, the contract's code can include any authentication logic necessary to verify a user's identity.

This design pattern is known as account abstraction, which offers authentication beyond external ownership and enables accounts to interact with each other in a more flexible nature.

Account abstraction provides users with greater control and flexibility over external ownership compared. With smart contracts as accounts, users can define custom permission levels, batch transactions, implement account recovery mechanisms, and set transaction limits through smart contract code.

This enables a higher level of security, customization, and usability that is not possible with key pair ownership.

By removing the reliance on external ownership, account abstraction can pave the way for more widespread adoption of blockchain technology by simplifying the user experience and enhancing security.

Cross-chain communications

Native cross-chain communication protocol enables workchains to interact with each other in a trustless manner without relying on third-party bridges or intermediaries. This allows for seamless workchains interoperability, enabling the transfer of data, assets, and value.

By using a cross-chain communication protocol for heterogeneous chains, the Venom blockchain can maintain interoperability between public and private networks, which opens up the possibility of creating powerful user cases:

Public-to-Public workchains are open for communication with each other and can maintain shared liquidity in, which means they can easily share value between networks. It is useful for DeFi applications, such as decentralized exchanges, cross-chain lending, and more.

Private-to-Private workchains are suitable for CBDC and crypto payments where privacy and compliance are essential. These workchains are generally closed to public exploration and can be operated by a single organization or consortium. Private-to-Private can securely and privately serve sensitive data and transactions, such as financial and personal information.

Public-to-Private workchains enable the creation of a system where two types of assets are strongly connected. The first, protected by regulation and compliant, is within private networks, while the second, transparent and participating in open DeFi markets, exist on public networks.

Blockchain interoperability provides numerous benefits, including the ability to create customizable Web3 services by mixing and matching different protocols and applications. This allows for the creation of entirely new instruments and platforms that were previously impossible with legacy industries and business models of the Web2 era.

Invisible gas fees

A stablecoin (or CBDC) on the Venom blockchain can charge transaction fees in any on-chain currency, creating a simple user experience and seamless accounting with the existing traditional system.

Other public blockchains have friction levels because they require a third instrument to charge fees exclusively using their native token to pay gas and other fees, making the process highly complex. The Venom blockchain simplifies the process of paying transaction fees by allowing users to pay in any on-chain currency accepted by the dApp they are interacting with.

Protocol standards

Distributed Fungible Tokens

A Distributed Fungible Token is the principal token standard on the Venom network. DFT was designed to match the distributed system design of the Venom network and is cost-effective due to its fee-paying model and scalable due to its distributed nature.

A Distributed FT provides the following functionalities:

- Transfer tokens from one account to another;
    - Get the current token balance of an account;
- Get the total supply of the token available on the network;
    - Mint and burn tokens.

Distributed Non-Fungible Tokens

The Distributed Non-Fungible Token standard is tailored to the architecture of the Venom network, and it defines the second most popular type of token, which is the Non-Fungible Token (NFT). This standard provides an efficient way to create, exchange, and trade NFTs within the Venom network.

8. The Target market

The failures of the crypto market in 2022 showed that the stability and security of the underlying technology of the public blockchain platforms were not the primary concern. Instead, the issues were caused by poor auditing practices, mismanagement of funds, and fraudulent activities by individuals and organizations. And these issues are not unique to the crypto market. The traditional financial sector faced similar problems in the 2008 financial crisis and the recent scandals involving large financial institutions.

The ideal solution would be to find a balance between the strengths of both systems, incorporating the transparency and innovation of public blockchains and the DeFi ecosystem while also providing the necessary protections and stability of regulated markets. This balance can be achieved through appropriate regulations and technical solutions that give a clear and transparent link between assets and activities.

Thanks to the aforementioned features [7.4], we see that the Venom blockchain can provide this balance to the market. This approach allows the network to bridge the gap between the traditional financial system and the decentralized world of cryptocurrency, providing a balance of decentralization and control ideal for a wide range of use cases.

8.1. Proof of Reserves mechanisms

Proof of Reserves (PoR) is a mechanism used to verify that a trading platform or crypto company holds the assets it claims to have. This is important because it helps to ensure that the platform or firm is financially stable and can meet its obligations to its customers.

The Venom Foundation suggests a heterogeneous multi-blockchain model combining private and public chains can be a solution to creating robust Proof of Reserves (PoR) mechanisms. Using a private blockchain to manage and control such assets as CBDCs makes it possible to maintain regulatory compliance while ensuring the privacy of sensitive information. At the same time, using a public blockchain can provide the necessary transparency and immutability required for proof of reserves, allowing anyone to verify the assets backing the stablecoin or crypto exchange funds.

8.2. CBDC

Central Bank Digital Currency is a digital form of fiat currency issued and backed by a country's central bank. It is stored and transacted electronically instead of in physical form. CBDCs are distinct from cryptocurrencies, which are decentralized and not backed by any central authority. Private blockchains can be permissioned, meaning that only approved entities can participate in the network, which can help to prevent fraud, illicit activities, and other security risks. Additionally, private blockchains may offer greater privacy for transactions and user data.

The Venom blockchain's private permissioned workchains can be utilized to issue and transact CBDCs while maintaining compliance with regulatory requirements. This approach offers several advantages over traditional fiat currency, including faster settlement times, increased security, and reduced costs.

The CBDC issuer can charge transaction fees in any on-chain currency, creating a simple user experience and seamless accounting with the existing traditional system.

By utilizing the account abstraction feature, the Venom blockchain can provide greater flexibility and control, enabling to implementation of account recovery mechanisms. Users no longer need to record their seed phrase and can have access to the ability to regain access to their funds even if they lose their initial account authentication credentials. Also, that helps users unfamiliar with cryptocurrencies use other authentication methods to use their assets in a non-custodial manner.

8.3. CBDC-backed stablecoin

The appearance CBDCs on workchains makes it possible to use them as collateral for stablecoins on public workchains. This is possible thanks to Venom workchains interoperability.

Organizations issuing such stablecoins can demonstrate reserve holdings from the private workchain to the public one, only disclosing balance information. The central bank's obligations ensure the security of the stablecoin, which can circulate freely in the public workchain and be utilized in DeFi. The private sector remains the issuer of the stablecoin, with the possibility of having proof of ownership of CBDCs funds. Reverse proof of ownership can also be provided to the private network, allowing for the receipt of CBDCs in the private network.

Our vision at the Venom Foundation is that this approach can create sustainable stablecoins and mass adoption.

8.4. Trade finance

Trade finance is an industry that encompasses a multitude of processes related to financing international trade. It plays a crucial role in developing the global economy but also faces several challenges, such as high costs, slow transaction processing, and security risks.

Venom's technologies can address these issues and significantly improve trade finance processes.

One approach to applying blockchain in trade finance is to use blockchains that combine the benefits of both public and private chains. Private workchains can be used for processing and storing confidential information such as client data, financial instruments, and transactions. This can provide a higher level of confidentiality and protection of commercial secrets, which is particularly important for large and complex deals in trade finance. On the other hand, public workchains and proof of reserve mechanisms can be used to provide transparency and openness regarding counterparty balances, transaction data, trade documents, and additional information. This can provide a higher level of trust and reduce the likelihood of fraud, which is especially important for small and medium-sized enterprises that may not have access to traditional forms of financing.

The cross-chain communication protocol allows for interoperability between public and private networks, enabling the exchange of data, assets, and value between workchains without needing third-party bridges. This can provide greater efficiency and lower costs for trade finance transactions, such as trade finance loans and international payments.

Trade finance also can benefit from the advantages of incorporating CBDCs. CBDCs can provide a fast and cost-effective means of payment for international trade.

Using the Venom blockchain can significantly impact the trade market by incorporating private and public workchains, incorporating CBDCs and proof of reserve mechanisms. This approach can unlock its full potential and provide a more secure and stable environment for international trade by providing a balance of transparency, privacy, and regulatory compliance.

8.5. Finance for the unbanked and micro transactions

Using heterogeneous chains could benefit our approach to finance for the unbanked and micro transactions. Private workchains could be used to store and process confidential information, such as client data, while public workchains could provide transparency and openness regarding the reserves of the financial service provider. This would enable us to create a more secure and transparent environment for financial transactions, particularly in developing markets where traditional financial services may not be available.

Partnering with payment systems, exchanges, and financial institutions could also benefit, as it would allow these partnerships to reach a wider range of users, promoting greater financial inclusion and economic opportunities for all.

Incorporating private and public blockchains into the Venom blockchain's approach to finance for the unbanked and micro transactions could provide a more secure and efficient way to provide essential financial services to those who have been excluded from the traditional financial system.

8.6. Community driven blockchain

We recognize that our target markets are not limited to those specific goals. The beauty of blockchain technology is that it is an open environment for anyone to create products and solutions for any market they see fit. This allows for innovation and creativity to thrive and for communities to come together to build a better future.

At the Venom Foundation, we believe in fostering an open, inclusive, and supportive community of each other's ideas and projects. We encourage our community members to share their insights and experiences, collaborate, and build products that can benefit everyone.

In summary, we recognize that the potential of blockchain technology extends far beyond the discussed markets. We encourage everyone to explore and create products that can serve any market, and we are committed to supporting our community in their endeavors.

9. Governance

An effective network's governance must be agile and reflective of the many environments— economic, social, regulatory, etc.—in which it finds itself. The governance mechanism of the Venom blockchain is designed to strive towards ethically ensuring the sustainable success of the network in a rapidly changing economy.

The Venom Foundation plays a role in the governance of the network by overseeing the decision-making process and providing resources to facilitate it. The foundation is responsible for managing the development of the ecosystem, shaping the technology development strategy, and promoting the adoption of the network. Additionally, the foundation acts as a bridge between the network's participants and external stakeholders, helping to facilitate communication and collaboration between different groups.

The Venom Foundation contributes significantly to the governance of the network, but it is important to note that the governance of the Venom blockchain is designed to be decentralized. The network's governance model allows for a broad range of participants, including users, validators, and developers, to have a say in the decision-making process.

The governance structure of the Venom blockchain is designed to strive towards dynamic and adaptable, allowing it to respond to changing economic, social, and regulatory conditions. Through the use of on-chain governance mechanisms, such as voting and proposal systems, the network's participants can make decisions about upgrades, new features, and overall improvements to the network.

Aims of the governance mechanism are to ensure that the blockchain is adequately maintained and regularly updated. This will translate to the long-term sustainability of the ecosystem and the community. The Venom blockchain's governance has been designed to make the blockchain's development, operation, and updating processes transparent, effective, and secure.

The Venom Foundation's role in the governance of the network is to support a decentralized decision-making process that enables all participants to have a voice in the network's evolution.

9.1. Infrastructure Governance

The governance procedure consists of two phases: (a) raising an update proposal for a vote and (b) voting for the proposal by community members.

A voting proposal related to infrastructure governance can be raised by any member of the community. We allow every community member to raise voting proposals to maximize the probability of critical issues being found and properly addressed, therefore facilitating the process of constant improvement of the network. Permitting the minor Venom contributors to appraise technical issues, we demonstrate the true power of decentralization. We are willing to make the governance more transparent, fair, and equitable than other networks.

The voting mechanism has been built to give each community member voting power proportional to his/her contribution to the security and stability of the network.

The voting mechanism is tailored to respect the principle of proportionality, considering that each community member's voting power is proportional to his/her contribution to the security and stability of the network.

9.2. Resources governance

Resources governance implies the distribution of funds/assets/resources among those who will contribute to the development of the network itself or its ecosystem. The Venom Foundation's exclusive power is resource governance. The principles of resource governance are reflected in the Venom Foundation's establishing documents.

Grants

The main goal of the Foundation Grant Program is to support and expand the Venom blockchain ecosystem with new products and services. It's open to all developers, whether individuals, teams, or companies. The program encourages applicants to think creatively and propose unique solutions that add value to the Venom ecosystem. The detailed description of the Foundation Grant Program is vested with a separate document within the competence of the Foundation's Board.

Bug Bounty Program

The Bug Bounty Program is an important part of ensuring the security and integrity of the Venom blockchain. The program encourages security researchers and developers to identify and report potential vulnerabilities in the network, which helps prevent malicious attacks and maintain the ecosystem's overall health. In addition to providing a financial incentive for researchers to find bugs and vulnerabilities, the program also serves as a way to engage with the broader developer community and encourage collaboration on security issues.

The program's rules and procedures are outlined in detail in a separate document. The program covers various aspects of the Venom blockchain, including the core protocol, smart contracts, and decentralized applications. Rewards are based on the severity of the reported vulnerability and the quality of the report, with higher rewards offered for more critical vulnerabilities. The Foundation encourages all security researchers and developers to participate and contribute to the security of the Venom blockchain.

10. Launch Roadmap

Stage 0. PoA Launch

The purpose of running The Venom blockchain in Proof of Authority (PoA) mode is to establish a central authority to control the network while it is being developed and tested. In PoA mode, a designated authority, in this case, the Venom Foundation, owns and operates all of the validator nodes on the network. This allows for a more controlled testing environment for the testing period.

The centralized control of the network allows for quicker decision-making and more efficient troubleshooting if issues arise. Once the network is deemed stable and mature enough, it can then transition to a more decentralized consensus mechanism, such as PoS, where validators are elected by the community.

At that time, the participants have the ability to:
- Create accounts, hold, and transfer tokens.
- Stake and claim tokens to validators.
- Deploy and use smart contracts and dApps.
- Interact with the Venom Ecosystem.

Conditions for Moving on to the next stage
- The network is stable and functioning well.
- The target number of tokens held by developers and users has been achieved.
- A sufficient number of applications from validators have been collected.

Stage 1. PoS and Governance

At this stage, The Venom blockchain aims to transition from Proof of Authority (PoA) mode to Proof of Stake (PoS) mode. This involves a shift towards more decentralized node management, where validators are elected by the community rather than controlled by a central authority. Also, The Venom blockchain aims to establish a decentralized community- driven governance structure to manage the network's decision-making process. This will give the community a voice in the network's development and direction and allow for a more democratic decision-making process.

At that time, the participants have the ability to: Run community validator nodes.
- Delegate tokens to support community validators.
- Participate in the grant program for developers. Propose and vote on network upgrades.

Conditions for Moving on to the next stage
- The target number of community validator nodes and stakes has been achieved. The community governance structure has been launched and functioning well.

Stage 2. Workchains and Interoperability

This stage of the Venom blockchain is focused on workchains and interoperability. At this stage, the Venom blockchain is introducing a workchain framework that allows developers to create custom workchains that can perform specific functions or support specific applications. The framework will provide developers with the tools and infrastructure they need to build, test, and deploy their workchains.

At that time, the participants have the ability to:
- Use the Workchain framework to create custom workchains.
- Participate in the grant program for workchains.
- Take advantage of the cross-workchain communication protocol.

Conditions for Moving on to the next stage
- The Workchain framework has been released.
- The first Workchain has been run.
- Message passing between workchains has been achieved.After the launch workchains, the Launch Phase was complete, and the Venom blockchain moved into the phase typically called the Continuous Development Phase.

Disclaimer

This document is a technical white paper that presents the current status and future plans for the Venom Foundation. This document serves solely to provide information and is not to give a precise description of plans. The Venom Foundation does not provide a statement of quality assurance or affidavit for the successful development or execution of any of such technologies, innovations, or activities described in this document. Also, within legally permitted scope, the Venom Foundation rejects any liability for quality assurance that is implied by technology or any other methods. No one possesses the right to trust any contents of this document or subsequent inference, and the same applies to any mutual interactions between the Venom Foundation technological interactions that are outlined in this document. Notwithstanding any mistake, default, or negligence, the Venom Foundation does not have legal liability for losses or damages that occur because of errors, negligence, or other acts of an individual or groups in relation to this document. Although information included in this publication were referred from data sources which were deemed to be trusted and reliable by the Venom Foundation, the Venom Foundation does not write any statement of quality assurance, confirmation, or affidavit regarding the accuracy, completeness, and appropriateness of such information. You may not rely on such information, grant rights, or provide solutions to yourself, your employee, creditor, other shareholder, or any other person. Views presented herein indicate current evaluation by the writer of this document and are not necessarily representative of the view of the Venom Foundation. Views reflected herein may change without notice, and do not necessarily comply with the views of the Venom Foundation.

The Venom Foundation does not have the obligation to amend, modify, and renew this document, and is not obliged to make notice to its subscribers and recipients if any views, predictions, forecasts, or assumptions in this document change, or any errors arise in the future. The Venom Foundation, its officers, employees, contractors, and representative do not have any responsibility or liability to any person or recipient (whether by reason of negligence, negligent misstatement or otherwise) arising from any statement, opinion or information, expressed or implied, arising out of, contained in or derived from or omitted from this document. Neither the Venom Foundation nor its advisors have independently verified any of the information, including the forecasts, prospects and projections contained in this. Each recipient is to rely solely on its own knowledge, investigation, judgment, and assessment of the matters which are the subject of this report and any information which is made available in connection with any further investigations and to satisfy him/herself as to the accuracy and completeness of such matters. While every effort has been made to ensure that statements of facts made in this paper are accurate, and that all estimates, projections, forecasts, prospects, and expression of opinions and other subjective judgments contained in this document are based on the projection that they are reasonable at the time of writing, this document must not be construed as a representation that the matters referred to therein will occur. Any plans, projections or forecasts mentioned in this document may not be achieved due to multiple risk factors including limitation defects in technology developments, initiatives or enforcement of legal regulations, market volatility, sector volatility, corporate actions, or the unavailability of complete and accurate information.

The Venom Foundation may provide hyperlinks to websites of entities mentioned in this paper, but the inclusion of a link does not imply that the Venom Foundation endorses, recommends or approves any material on the linked page or accessible from it. Such linked websites are accessed entirely at your own risk. The Venom Foundation accepts no responsibility whatsoever for any such material, or for the consequences of its use. This document is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation. This document may not be redistributed, reproduced or passed on to any other person or published, in part or in whole, for any purpose, without the prior, written consent of the Venom Foundation. The manner of distributing this document may be restricted by law or regulation in certain countries. Persons into whose possession this document may come are required to inform themselves about, and to observe such restrictions. By accessing this document, a recipient hereof agrees to be bound by the foregoing limitations.

This white paper is an information paper subject to continuous update. This paper is not a prospectus, product disclosure statement or other regulated offer document. It has not been endorsed by, or registered with, ADGM or its FSRA. The distribution and use of this paper, including any related advertisement or marketing material may be restricted by law in certain jurisdictions. If you fail to comply with such restrictions, that failure may constitute a violation of applicable law. By accessing this paper, you agree to be bound by this requirement.