ONYX COIN WHITE PAPER

A peer-to-peer electronic money for Africa

nulamugarichard@gmail.com

Preface

As the world becomes increasingly digital, cryptocurrency is a natural step in the evolution of money. Onyx coin is a digital currency for everyday people, representing a major step forward in the adoption of cryptocurrency worldwide and especially in Africa.

Our Mission:

In the advent of cryptocurrency, it is crucial to build an infrastructure for Africa. Our mission is to build an inclusive and economically sound cryptocurrency and smart contracts platform that is secured and operated by everyday people.

Our Vision:

To build the world's most inclusive peer-to-peer ecosystem and online experience, fueled by onyx coin, the world's most economically inclusive cryptocurrency.

Introduction

In recent years, cryptocurrencies have emerged as a revolutionary force in the financial landscape, redefining the way we think about and engage with money. These digital or virtual currencies use cryptographic techniques to secure transactions, control the creation of new units, and verify the transfer of assets, all while operating independently of central banks or traditional financial institutions. The role of cryptocurrencies extends far beyond their function as a medium of exchange; they are reshaping economic systems, fostering financial inclusion, and driving innovation in technology and investment.

One of the most significant benefits of cryptocurrencies is their potential to democratize financial access. By enabling peer-to-peer transactions without intermediaries, they offer a more inclusive financial ecosystem, particularly for those in underbanked or underserved regions like in Africa. Cryptocurrencies also provide a level of transparency and security that traditional financial systems struggle to match, thanks to blockchain technology, which records all transactions in an immutable and publicly accessible ledger. Additionally, their decentralized nature reduces transaction costs and increase transaction speed, making financial operations more efficient and accessible. As the world continues to embrace digital transformation, cryptocurrencies stand poised to play a pivotal role in shaping the future of finance.

Onyx coin is coming in as revolutionary digital currency designed purposely for the African market with global impact. As a cryptocurrency, onyx coin offers a new paradigm for economic interaction that holds considerable promise for economic emancipation, particularly in regions where traditional financial system are limited or non-existent.

ONYX – A PRE-MINED COIN

Pre-mined cryptocurrencies, often referred to as "pre-mined coins," are digital assets that are fully generated and allocated before they are released to the public. Unlike cryptocurrencies that are mined over time through a consensus process, pre-mined cryptocurrencies are created in their entirety during their development phase, an example of this is XRP coins. This approach for Onyx coins comes with several distinct advantages:

1. Predictable Supply and Controlled Inflation

Onyx coins have a fixed supply right from the start, which can help manage inflationary pressures. By establishing a maximum supply of Onyx coins before any are distributed, we avoid the risk of excessive inflation that may occur with traditional mining models. This predetermined supply can contribute to the asset's stability and provide clearer insights into its long-term value trajectory.

2. Enhanced Security and Stability

As a pre-mined coin, we ensure that the initial distribution is secure and managed. Since all coins are created upfront, there’s no risk of vulnerabilities associated with mining processes, such as potential attacks on the mining network or the impact of mining centralization. This will enhance the overall security and stability of Onyx coins, particularly during its early stages.

3. Incentivizing Development and Adoption

Onyx coins come with allocated reserves for development, partnerships, and marketing. By setting aside a portion of the total supply for these purposes, we incentivize early adopters, fund project growth, and establish strategic partnerships. This can accelerate the cryptocurrency’s adoption and enhance our ecosystem, leading to increased utility and value over time.

4. Avoiding Mining Centralization Issues

In some cryptocurrency networks, mining can become centralized if only a few entities control the majority of the mining power. This centralization can undermine the decentralization ethos of blockchain technology and create security risks. Onyx cryptocurrencies bypass these issues by eliminating the need for mining altogether, ensuring that no single entity can dominate the network through mining control.

5. Transparency in Distribution

Onyx coins have a clear and transparent distribution plan. The allocation of onyx coins is outlined in this project whitepaper, providing clarity on how the total supply is divided among founders, investors, advisors, and the community (more in tokenomics paper). This transparency helps us build trust among stakeholders and reduces concerns about hidden or unfair coin distributions.

6. Immediate Liquidity and Usability

Since Onyx coins are fully issued from the outset, they are immediately available for use and trading at launched. This immediate availability will facilitate liquidity and usability, allowing

users to transact, invest, or use the coin's services without waiting for the gradual issuance process of mined coins.

ONYX COIN CONSENSUS

THE BYZANTINE FAULT TOLERANCE (BFT) CONSENSUS AND THE RIPPLE PROTOCOL CONSENSUS ALGORITHM

This consensus is a critical concept in blockchain technology and distributed computing that addresses the challenge of achieving agreement in a network where some nodes may act arbitrarily, fail, or exhibit malicious behavior. The term originates from the Byzantine Generals Problem, a theoretical problem in computer science and cryptography that illustrates the difficulty of reaching consensus in the presence of unreliable or dishonest participants.

This consensus mechanisms ensure that a decentralized network of nodes can agree on the state of the blockchain (e.g., which transactions are valid or which blocks should be added) even when some nodes fail or behave in a Byzantine manner. This is crucial for maintaining the integrity and reliability of Onyx coin network, as it allows the system to function correctly despite failures or malicious actions as obtained in similar blockchains like the XRP (see ripple.com).

Key advantages of BFT Consensus

1. Resilience to Malicious Behavior

2. Ensuring Network Integrity

3. Mitigating the Risk of Sybil Attacks

4. Reducing the Need for Resource-Intensive Mining

5. Supporting Faster Transaction Processing

6. Enhancing Fault Tolerance

7. Promoting Decentralization and Trust

The Byzantine Fault Tolerance consensus mechanisms play a vital role in ensuring the robustness, security, and efficiency of cryptocurrency systems. By addressing the challenges of malicious behavior, achieving consensus in decentralized networks, and supporting faster and more reliable transaction processing, BFT mechanisms help create resilient and trustworthy blockchain systems. Their ability to tolerate faults and attacks while maintaining network integrity makes it a valuable choice for Onyx coin.

The Ripple Protocol Consensus Algorithm (RPCA)

How it works

- Each server/node s maintains a **unique node list (UNL)**, which are the only nodes that s queries when determining consensus. The UNL forms a trusted subset of the network, even if some individual members of the UNL are not trusted.
- The RPCA is applied by all nodes every few seconds, reaching consensus assuming there are no forks or system errors. The RPCA proceeds in rounds:

1. Each node publishes all valid transactions it has seen that are not yet part of the ledger, forming a **candidate set**
2. Each node amalgamates the candidate sets of all the nodes in its UNL, then votes on the veracity of each transaction.
3. Transactions with more than a certain percentage of 'no' votes are either discarded or included in the next candidate set.
4. If at least 80% of a node's UNL agrees on a transaction, it is applied to the ledger.
5. The ledger is closed, becoming the new **last-closed ledger**.

- **Strong correctness** is guaranteed for $f \leq (n-1)/5$ Byzantine failures. However, although consensus cannot be reached for $20\% < f < 80\%$, in this case fraudulent transactions will not be confirmed. Thus, **weak correctness** is maintained for any $f \leq (4n+1)/5$.
- If the probability of a node colluding maliciously with other nodes is pc, then the probability of correctness $p*$ is given using the Binomial Distribution:

  $$p* = \sum_{i=0}^{\lceil (n-1)/5 \rceil} \binom{n}{i} pc^i (1-pc)^{n-i}$$

- Thus, the UNL must be chosen to minimise pc. This is possible because nodes are cryptographically identifiable, so specific nodes can be grouped with other nodes such that they are less likely to form Byzantine collusions. High pc values can be somewhat compensated for with more nodes in the UNL, e.g. $pc = 0.15, n = 200 \Longrightarrow p* = 90\%$.
- To meet the agreement criterion, some level of interconnectivity is required in the network: the formation of UNL 'cliques may result in forks, as different parts of the network have different ledgers.
- To satisfy the utility criterion, it must be shown that consensus is reached in finite time. Because the RPCA is deterministic and has a preset number of rounds, the limiting factor is latency between nodes. This is bounded by removing nodes where latency increases beyond a certain value. Note that the final UNL must satisfy the correctness/agreement bounds in terms of network size and connectivity.

- A number of other heuristics are used:
    - mandatory 2 second window for nodes to propose candidate sets, to allow for slow connections within latency bounds.
    - during voting, nodes can be flagged and removed for repeated malicious behaviour, such as consistent ‘no’ votes
    - default UNLs are provided to minimise *pc*, though nodes are encouraged to choose their own UNL.
    - each node monitors the size of its UNL: a sudden drop may signify a fork.
    - the rounds in the RPCA allow for latency detection to improve overall network speed.
- The overall low latency, speed, and provable security (given the bounds) of the Ripple network make it ideal for financial transactions and for use by Onyx coin.

ONYX COIN VIRTUAL MACHINE (OVM)

The concept of a virtual machine (VM) in blockchain refers to a simulated computing environment that executes smart contracts and processes transactions without the need for a physical machine. This abstraction layer provides significant benefits in terms of security, decentralization, and interoperability. Here’s a detailed look at the role of virtual machines on the onyx blockchain:

1. Definition and Purpose

Virtual Machine: A virtual machine in blockchain serves as a runtime environment that interprets and executes code written in smart contract languages. It abstracts the complexities of the underlying hardware and operating systems.

Purpose: The primary purpose of a VM is to facilitate the execution of decentralized applications (dApps) in a secure and deterministic manner, ensuring that all nodes in the network can independently verify the results of computations.

2. Key Features

Isolation: VMs operate in an isolated environment, meaning that the execution of smart contracts does not affect the overall state of the blockchain or other contracts directly. This enhances security by preventing malicious contracts from compromising the entire onyx coin network.

Determinism: VMs ensure that the same input will always produce the same output across all nodes, which is essential for maintaining consensus within a decentralized network.

3. Examples of Virtual Machines

Ethereum Virtual Machine (EVM): The most well-known VM, it allows developers to write smart contracts in languages like Solidity. The EVM uses a stack-based architecture and manages state transitions via gas fees.

Hyperledger Fabric: Uses a modular architecture with its own smart contract execution environment, which can support various programming languages. Hyperledger's VM is designed for enterprise use cases.

Binance Smart Chain (BSC) Virtual Machine: Compatible with the EVM, it allows Ethereum developers to deploy their dApps on the BSC network with minimal changes.

4. Benefits of Using a VM on the Onyx coin Blockchain

Security: By running code in a sandboxed environment, VMs reduce the risk of vulnerabilities impacting the broader network. Bugs and exploits are contained within the VM.

Portability: Smart contracts can be executed on any node running the same VM, facilitating easier deployment and scaling across different environments.

Resource Management: VMs use mechanisms like gas fees to manage computational resources effectively, preventing network congestion and spam attacks.

5. Future Developments on the Onyx coin chain

Layer 2 Solutions: Innovations like rollups and state channels are developed to improve scalability and efficiency while leveraging existing VMs.

Interoperability: As blockchain ecosystems grow, the need for VMs that can communicate and execute contracts across different chains is becoming more important, leading to research and development in cross-chain compatibility.

The concept of virtual machines in blockchain is integral to the functionality and security of decentralized applications. By providing a controlled and isolated environment for executing smart contracts, VMs enable the creation of robust and secure dApps on the Onyx coin chain while maintaining the core principles of decentralization and consensus. As the technology evolves, the role of VMs continues to adapt, enhancing the capabilities and performance of blockchain networks.

Key Features of ONYX COIN Virtual Machine:

1. **High Performance**: The Onyx Virtual Machine is optimized for fast execution, allowing for quick transaction processing, which is crucial for decentralized applications that require real-time interactions.
2. **Smart Contract Support**: It enables developers to write and deploy smart contracts using a high-level programming language. This opens up a wide range of use cases, from simple token contracts to complex decentralized finance (DeFi) applications.
3. **Scalability**: The Onyx coin architecture is designed for scalability. It uses sharding to distribute the workload across multiple nodes, enhancing throughput and performance as more users and applications join the network.
4. **Interoperability**: Onyx coin aims to facilitate interactions between different blockchain networks, allowing for seamless transfers of assets and data across platforms.
5. **Security**: The virtual machine incorporates robust security features to protect against common vulnerabilities in smart contracts, making it a safer environment for developers.
6. **User-Friendly Development**: The ecosystem will provide tools and libraries that simplify the development process, making it more accessible for developers to create and deploy dApps.

Onyx coin Economic Model

Onyx coin supply strikes a balance between creating a sense of scarcity and availability of a digital coin for economic use, while still ensuring that a large amount does not end up in the control of very few numbers of hands. We want to make sure our users have access to onyx coin as they participate in the ecosystem. Onyx coin's goal is to build an economic model that is efficient enough to achieve and balance these priorities while remaining intuitive enough for people to use.

Model design requirements:

- Availability: get onyx coin into the hands of every user.
- Scarcity: control the number of coins available for users. No user should have more than they should have and inactive accounts will be revoked. (see Onyx coin tokenomics paper)
- Fair distribution: Give a critical mass of the world's population access to onyx, with limited sale units to accounts.
- No loses: dormant accounts are recovered after a certain period of time. (see Onyx coin tokenomics paper)

Onyx coin – Token Supply

Token and Distribution Policy

1. Total Max Supply = 360 million onyx coins
2. Distribution ratios, rate and timeline at launch.

DESCRIPTION	DISTRIBUTION RATIO	INJECTION RATE	TIMELINE
LOCKED UP RATE	128,000,000	-	8 MONTHS AFTER LAUNCH
FOUNDERS	70,000,000	5.5M	
INVESTORS	35,000,000	15M	
DEVELOPERS	15,000,000	7M	
LIQUIDITY PROVIDERS	10,000,000	10M	
COMMUNITY	110,000,000	60M	
TOTAL	360,000,000	97.5M	

3. Subsequent release

   After the first 8 months of launch, 20 million onyx coins will be release again into the ecosystem in the space of 6 months for three years (3 yrs.). On the final release, 14.5 million will be released to make up a total of 232 million Onyx coins in circulation.

4. Lock up value.

   128M will be for the Onyx Coin Foundation to support projects on ecosystem, community events and also to give relief support where necessary.

Roadmap

- White paper
- Protocol development:
  1. Testnet
  2. Mainnet
- Utility integrated wallet development
- Launch (ICO and Airdrops)
- Marketing and community onboarding
- KYC and accounts validation

REFERENCEES

1. Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple protocol consensus algorithm. Ripple Labs Inc White Paper, 1–8. Retrieved from ripple.com.

2. Chatgpt prompt