# Radiologex: Innovating Health IT through Dual Consensus Blockchain

## 1. Introduction

Radiologex stands at the forefront of health IT innovation with its pioneering methodology. By skillfully harnessing the combined strengths of both Proof of Authority (PoA) and Proof of Stake (PoS) consensus mechanisms, our platform is meticulously designed to foster an environment that places a premium on efficiency, fortified security, and unwavering trustworthiness. This synthesis not only ushers in a new paradigm for health IT solutions but also ensures a seamless and secure experience for all stakeholders involved.

## 2. Radiologex's Foundations: Dual Consensus Mechanism

### 2.1. Proof of Authority (PoA)

Role of Authority Nodes: Integral to PoA's structure, these nodes perform pivotal operations.

- Modified QBFT Protocol: At the heart of our PoA lies the QBFT protocol. This enhancement promises quicker transaction finality, reduced energy consumption, and robustness against forks. It also fosters an environment where malicious nodes can be identified and penalized swiftly.
- Transaction Verification: Prioritizing quick turnarounds, they rapidly authenticate and append transactions to the blockchain.
- Network Security and Integrity: With a reputation system, these nodes bolster system defenses, thwarting unauthorized activities.
- Compliance Audits: Regular assessments ensure network alignment with our stringent benchmarks.
- Software Evolution: Paving the path for cutting-edge implementations, authority nodes manage seamless software transitions.
- Efficiency & Scalability: Their decision-making ability, being centralized, expedites high-volume transaction processes.

### 2.2. Proof of Stake (PoS): Masternodes in Action

Masternodes operate as the ecosystem's primary support structures, anchored by substantial RDGX token stakes.

- Transactional Scrutiny: Being the vanguard, they initially vet transactions, ensuring only genuine activities progress to PoA nodes.
- Authlogex Engine Supervision: Steering the Authlogex operations, they guarantee a secure and private mechanism for digital ID verifications in healthcare.
- Advanced Data Management: Beyond mere storage, these nodes ensure encrypted data protection, optimize retrieval processes, and provide decentralized computational resources.
- Rapid Payment Channels: For swift settlements, masternodes manage specialized channels, ensuring timely service fee resolutions.

Incentive Structure:

- Recurring Token Rewards: Masternodes are compensated with RDGX tokens for their vital services.
- Enhanced Service Offerings: Higher stakes potentially unlock advanced services, incentivizing commitment.
- Fee-Based Earnings: Handling specialized tasks could allow masternodes to accrue additional fees.

## 3. Synchronized Network Functionality: PoA & PoS Working in Tandem

Radiologex's efficacy emerges from the flawless synchronization of PoA's swift decision-making prowess with PoS's decentralization tenets.

- Unified Data Authentication: Starting with a transaction broadcast, preliminary checks by the PoS layer (masternodes) set the stage. The PoA nodes then finalize and inscribe the transaction.
- Security Reinforced: Dual consensus adds a layer of redundancy, ensuring operational continuity even if one mechanism falters.
- Optimal Governance Synthesis: Merging rapid centralized resolutions with decentralized verifications guarantees balanced network management.

## 4. Tokenomics: The RDGX Ecosystem Blueprint

Radiologex’s financial ecosystem, underpinned by the RDGX token, showcases a nuanced design.

- Masternode Commencement: A 10,000 RDGX token stake ushers participants into the network's PoS layer as masternodes.
- Reward Reservoir: A significant fraction of RDGX tokens is reserved, ensuring regular and equitable rewards for masternode contributions.
- Market Footprint: By periodically introducing tokens and penetrating secondary marketplaces, Radiologex aspires to cement its market relevance.
- Sculpting the RDGX Ecosystem: The total supply of 1 billion RDGX tokens serves various strategic purposes.
- Masternode Staking: With 10,000 RDGX tokens, any holder can establish a masternode, becoming an active participant in the network's PoS layer.
- Reward Pool Reservoir: A significant portion of the total token supply is earmarked for masternode rewards, ensuring a consistent and fair incentive system.
- Inflationary and Deflationary Tactics: To safeguard the RDGX token's value, strategic mechanisms, like token burns or reward variations, can be triggered based on market conditions.
- Market Presence: By ensuring token liquidity through periodic releases and by tapping into secondary markets, Radiologex aims to solidify its market position.

**Utility Beyond Simple Transactions:**

- Product Discounts: Masternodes receive privileged pricing on Radiologex's suite offerings.

- Exclusive Features & Early Access: Masternodes benefit from tailor-made features and get a preview of upcoming innovations.
- Augmented HDID Status: A testament to their value, they receive an elevated HDID status, fostering trust within the healthcare community.
- Strategic Partnerships: Opportunities to mesh Radiologex's solutions with individual institutional requirements.

# 5. ITokenomics: RDGX Ecosystem & Cutting-Edge Issuance

Radiologex's RDGX token ecosystem integrates traditional tokenomics with the latest in financial technology.

- Decentralized Finance (DeFi): Masternodes can leverage their staked RDGX tokens in DeFi protocols, earning interest or taking loans against their stakes.
- Token Issuance via Special Purpose Entity (SPE): An SPE licensee will manage the RDGX token's sales and issuance, ensuring regulatory compliance and operational efficiency. This structured approach not only separates token operations from the main entity but also optimizes financial management.
- Initial DEX Offering (IDO): Leveraging decentralized exchanges, the token's introduction to the market can maximize distribution while minimizing potential price manipulations.
- Yield Farming: Encouraging token usage and staking, users can earn additional RDGX tokens by providing liquidity or participating in network activities.

# 6. Security:

## 6.1. Security Enhancements for the RDee GoQuourum Node

The GoQuorum node is a vital part of an RDee Blockchain Network. It lays at the core of both PoA validators and future PoS users' nodes. Therefore, it is crucial to have more advanced security measures implemented in order to keep the users' data safe and chain working without interruptions. Thus, we have researched the main security threats which usually can occur in the network. Note, though we have implemented basic security measures on the node's level such as jwt tokens access, safe storing of private key, safely working consensus and safe management of the network, there are still threats which can occur as a result of malicious actions of attackers. Which is why we want to present the main security threats of blockchain nodes and what security measures we propose to implement in order to reduce the potential risk.

## 6.2. Common vulnerabilities and protection measures

### 6.2.1. DDoS

Description: In terms of blockchain, DDoS can occur due to the flood of transactions and lead to the disabling of peer and interrupt the work of network. As a result, valid users won't be able to use it as intended.

Measures:

- Start several archive nodes to distribute the load among them.

- Implement backup system in order to be able to start the nodes easily in an event of DDoS attack.
- Adjust the firewall so that only valid RDee applications can use the network.
- Implement monitoring system such as Grafana and automatically detect and ban any suspicious actions.

### 6.2.2. Malicious transactions and malware

**Description:**

Though the nodes have built-in mechanisms for reaching consensus and rejecting malicious transactions, it works correctly only when the majority of validators are trustworthy. In case a malicious user or a group of users possess a majority of nodes, they can send malicious transactions in order to receive personal gains. This is called 51% attack. In the event of such an attack, attackers are able to take control over the network and decide on whether to add malicious transactions to the chain. Though the RDee Network is private, the PoS consensus is planned where anyone who has staked enough tokens, will be able to join the network as a validator. A malicious user may use it to gain advantage over the network to use malware or malicious transactions.

**Measures:**

- Start as many own PoA validators as possible to have more control over the network.
- Demarcate the privileges of own PoA and PoS validators: PoS validators can't add new peers or vote for validators, etc.
- Implement a consensus where at least one own PoA validator must be active and approve proposed block.
- Implement a mechanism for updates and regularly update the node according to GoQuorum official latest releases.

### 6.2.3. Private storage layer

**Description:**

Since the blockchain might store confidential information, it is crucial to ensure the safety of this information. When PoS validators are enabled, confidential information shouldn't be stored in the storage of PoS validators since it may increase the leakage of users' data.

**Measures:**

- Separate storage into two layers: "Public" and private. "Public" layer will be stored on all the nodes and include tokenomic, public applications and non-confidential information. While private storage layer will be stored only on own PoA nodes and contain confidential information.

### 6.2.4. Data leakage and man in the middle attack.

**Description:**

All the data should transported to the nodes should be encrypted. Though the node already implements several security mechanisms, for example, signing of transactions, additional measures may implemented.

**Measures:**

- TLS certificates.

### 6.2.5. Unpredicted errors.

**Description:**

The unpredicted errors still can happen, which is why it is vital to implement log system to be able to analyse the error and implement the corresponding measures to eliminate such errors in the future.

**Measures:**

- Implement a log system and monitoring.
- Implement metrics.

**Additional Security measures**

- Implement a patch management program to automatically fetch all latest release of GoQourum and own releases for all nodes within the network.
- Monitoring system for detecting malicious actions and preventing potential exploits.
- Implement standard TLS for internal and external communications.
- Implement a NIDS system for detecting a suspicious activity in the network in real time.
- Implement backup for archive nodes.
- Enable metrics.
    - Logs with following features:
    - Log all activities of GoQuorum hosts to a centralized log system.
    - Ensure the centralized log system can answer queries about:
    - Ethereum accounts on the network.
    - Active ledger and transaction manager nodes in the network.
    - Public and private transaction rates per account in the network.
    - Number of public smart contracts in the network.
    - Network connections to ledger nodes and metadata.
    - Consensus protocol metadata (for example, block creation rate and source).

## 7. Epilogue

Radiologex, with its dual consensus integration, charts a new trajectory in healthcare's digital domain. Its intricate network of authority nodes and masternodes, while fostering a secure environment, ensures adaptability and efficiency. Through its equilibrium between centralization's agility and decentralization's robustness, Radiologex is poised to reshape health IT paradigms.