QRAX

Quantum-Resistance Anonymous Transaction

QRAX is a confidential payment network and repository of crypto assets. It is decentralized, peer-to-peer, quantum resistant, anonymous, open source, and focused on the development of the crypto community.

[White paper version 1.0 (non-technical)] **Alex McKeys(@QROSLABS)** **Nebula(@Nebula0id)**

ANNOTATION

QRAX is based on Bitcoin Core, which was built by an organization named after Satoshi Nakamoto, but introduces a number of improvements to Bitcoin's architecture. Namely, a two-tier network of nodes and masternodes, DAO for development, self-government and self-financing, and also a unique monetary system. The kernel has been modified and includes improvements for application of the principles of anonymity and transaction security, and transaction confirmation without centralized management. A digital decentralized system is implemented, and it is managed and developed by the holders of nodes and coins - the crypto community.

QRAX is a form of digital money using Blockchain technology, which can be easily distributed around the world, instantly and with reliable confirmation of transactions by the network within one block (about 60 seconds). The QRAX network includes security and privacy solutions.

General introduction

An engaged, motivated, reliable, competent and active community of people with the tools for adequate governance, development and decision-making processes is essential to the success of any decentralized system.The protection of information, especially personal and especially financial, is extremely important for the protection of the rights of any person. Fiduciary monetary systems have proven impractical and historically unwise to trust centralized regulators to fully protect personal data.

In addition, without a logical and uninterested management system, it is equally unwise to trust a cryptocurrency project or a specific blockchain with claims of decentralization, since one person can usurp the network, unilaterally make a decision, or, even worse, lose access, having lost the coded basis, private keys, etc.

For the flourishing of the developing cryptocurrency community around the world, where:

1. Energy should not be perceived as a commitment to the execution of the process,

2. There is a solid economic model for network growth and scalability,

3. It is possible to access the global network and make money on it from any device with minimal costs and energy consumption, it is necessary to understand the chosen algorithm (proof-of-work or proof-of-stake) underlying economies and means of participation in the network.

Understanding such a community model reveals the qualities and tools of the Quantum Resistant Anonymous Transactions (QRAX) system. Preservation of rights and freedoms, secure financial data and blockchain that protects privacy all add value and enable widespread adoption in an efficient, cost-effective and environmentally friendly protocol-level manner. QRAX simultaneously enhances security and provides resistance to censorship or exploitation of rights and freedoms on the worldwide web.

To address the above challenges in the current highly rugged terrain cryptocurrency landscape of the human community, QRAX encourages each node in the network to participate in the block generation process through the implementation of the Proof-of-Stake consensus algorithm to decide which block will be tied next. Another layer of the network contains masternodes that provide second-layer networking functions such as self-government, self-development and self-financing mechanisms.

Additional characteristics:

1. Balancing monetary flows at the protocol level by balancing inflation/deflation mechanisms stimulates decentralization and minimizes the involvement of external monetary systems.

2. Correlation of the activity of a network node in the form of a reward for the activity and popularization of the system, as well as a rate with a static emission of rewards for a block and final inflation, allows more efficient allocation of resources.

3. Rewards for site activity on the network create a motivated environment for communities and businesses.

4. Low hardware/device costs to participate and/or manage Masternodes, which lowers the participation cost barrier, allows anyone to participate in the network at any scale, and outperforms other network systems that require wasteful energy and hardware costs.

5. Global decentralized community-driven governance allows for oversight of network parameters without the participation of centralized mechanisms of states and communities, and also ensures direct participation of the involved community and continuous dialectical growth and governance of the monetary system.

6. Advanced Proof-of-Stake features such as DPoS further improve access, safety and freedom for people without burdensome hardware requirements.

   The QRAX ecosystem, for a better understanding of its principles of organization, can be compared to the so-called “onion” routing (TOP), but at the same time it is completely decentralized, self-organizing, self-financed and rewarding for participation.

Quantum Resistant Anonymous Transactions | Official document, version 1.0, 2021

1. INTRODUCTION

The advent of the blockchain era came in 2009 due to the creation of Bitcoin and its underlying Blockchain technology - created by an organization known as Satoshi Nakamoto. Following the success of Bitcoin, many competing cryptocurrencies called altcoins were created. The launch of Bitcoin and an original white paper based on the concept of the well-known math problem of the “Chinese generals” solved a problem comparable to the invention of the wheel and created a digital accounting system called the blockchain or linked blockchain. Each block contains a part of the previous block and it is impossible to change this without full control over all network nodes. This process is called decentralization because it does not have a control center and the information reliability of each transaction has the highest level of verification. The potential of blockchain and decentralization technologies has generated an explosive interest in communities for its application in all branches of human activity.

The market is currently filled with tokens and coins with different intentions, motivations, and affiliations. While there are many projects, some of which are innovative and ambitious, they are essentially clones with catchy names and serve as a deterrent to the wider adoption of cryptocurrency as a legal and borderless alternative to fiat currency. Bitcoin, despite its revolutionary solutions, in our opinion, cannot be widely used and accepted as the worldwide and only currency and is considered today as a store of value, and not a means of conducting transactions and everyday business. Many Bitcoin enthusiasts eventually turn into speculators and marketers, which negatively affects the first decentralized network of transactions. Bitcoin also cannot solve energy problems due to the excessive use of electricity required to maintain the network and mine coins.

More than eleven years have passed since the inception of the Bitcoin network, but the ultimate identity and architecture of cryptocurrencies is constantly evolving and changing. The general heterogeneity has led the public to view cryptocurrency as a kind of stock market, and not as a means of payments and transactions. Bitcoin’s inherent volatility and saturation is not suitable for potentially all users who see it not as an alternative to fiat currencies, but as an opportunity for risky investment.

QRAX seeks to bring together communities and provide tools for technically educated, thinking people who understand the reality of the world around them. QRAX provides secure means by which investors and the general public can conduct business without the need for centralized financial institutions and intermediaries. QRAX provides people in an increasingly interconnected world with a practical and secure means of doing business on their behalf.

"The essence of cryptocurrencies and blockchains is to solve the problems of traditional currencies by transferring power and responsibility to the holders of the currency." ~ Mike Chu [1].

2. NETWORK DESIGN

2.1 Introduction to QRAX Network Genesis

QRAX network was announced on bitcointalk.org on April 12, 2021. [2].

The first QRAX block was created on Mon, 12 Apr 2021 06:07:08 UTC. [3]

Today QRAX is, as it was when it first launched, decentralized, motivated and open source. [4]

The first phase (the first superblock or 44,000 blocks) was launched using the Proof-of-Work technology, which provided a fair start to the network for the initial mining of coins to create 21 core masternodes. [5]

On block 44,000, 20M coins were generated in the network for the distribution of coins among the supporting masternodes and the formation of the QRAX crypto community. [5]

PoW is essential for the fair launch of the network. QRAX implemented the first phase on the Quark hashing algorithm as it was considered the fairest one due to its low technical requirements and sufficient reliability. The network began with premining 1M-QRAX (coins of the same name QRAX) on the genesis block. The goal was to create 21 initial master masternodes. Then, on block 44,000, the transition to the PoS algorithm was made and the start of an approximately 6-week (six times of 10,080 blocks) pre-sale period to satisfy the interest in the coin from the crypto community. All remnants of this premine will be burned at block 104480. There are no artificial generations and no QRAX coins will be locked to manipulate the QRAX economy. After a period of 44,000 blocks, PoW was replaced by a Proof of Stake (PoS) consensus model to provide the most reliable, lower economic barriers, energy efficient and long term sustainable network protections. In doing so, rewarding those members who help ensure the safety, development and management of the network. Thus, the expensive hardware that limits mining has been replaced with energy efficient, easier-to-use stakenodes and masternodes. Also, the second level was transferred to the blockchain, which is often called the second layer network protocol. It currently provides mechanisms for decentralized governance and full-fledged self-financing development.

PoW Phase Period: April 12, 2021 - May 14, 2021 (COMPLETED)

Block height	Masternodes	Budget
1 block - network start 2-43999 blocks - PoW phase blocks Block 44,000 - present PoS phase	21 backbone masternodes	Accumulated on each block, allocated based on the results of active voting by masternodes on each superblock.

Table 1. Staking reward phases (PoS nodes / masternodes)

Phase	Block interval		Total Reward	Masternode / Staker		Budget		
#	Start	End	QRAX	QRAX	QRAX	QRAX	%	Max
1	44000	87999	70	50	10	10	16.67	440000
2	88000	131999	63	45	9	9	16.67	396000
3	132000	175999	56	40	8	8	16.67	352000
4	176000	219999	49	35	7	7	16.67	308000
5	220000	263999	42	30	6	6	16.67	264000
6	264000	307999	35	25	5	5	16.67	220000
7	308000	351999	28	20	4	4	16.67	176000
8	352000	395999	21	15	3	3	16.67	132000
9	396000	439999	14	10	2	2	16.67	88000
10	440000	~	7	5	1	1	16.67	44000

Table 2. Phases of reward for assets (halving reward for popularizing the network)

Phase	Block interval		Year %
1	44000	307999	255.5
2	308000	571999	127.8
3	572000	835999	63.9
4	836000	1099999	31.9
5	1100000	1363999	16.0
6	1364000	1627999	8.0
7	1628000	1891999	4.0
8	1892000	2155999	2.0
9	2156000	~	1.0

2.2 Proof-of-stake

The QRAX network is currently running on the PoS consensus algorithm.
The original concept was largely based on the concept of "coin age" or duration of the UTXO model.

Thus, the PoS model differs from PoW in that it does not focus on miners and hardware and does not reward miners, but rather rewards everyone who wishes to participate in the network (by keeping their coins on the node). The protocol was further refined in the second version of PoS with several security fixes potentially noted in the original protocol. Vasin's fixes included not allowing a malicious node to abuse coin age to double-spend, allowing honest nodes to abuse the system by only betting periodically, and consensus denial of coin age. The reliability and innovation of the PoS QRAX model is clear.

QRAX has gone beyond the original PoS concepts, constantly evolving to provide superior security and newness to the appropriate level of masternodes and financial data protection features.

Due to the PoS implementation, the network has available computing resources that automatically select the node to generate the upcoming block in the chain based on delimited competition. In the case of QRAX, these limits are delimited based on the balance (UTXO) set by the wallet - each staking node competes to create a valid block, which is very similar to PoW. However, nodes are technically limited in the number of times they can try at a given time (eliminating the need for higher processing power), and the difficulty of obtaining a valid block is inversely proportional to the rate. A higher balance means a higher chance and challenge to meet difficulty criteria, check a block, and receive a reward. Staking requires significantly less resources than PoW mining, since there is no need to strive for the constantly increasing complexity of solving the algorithms required to generate coins, and the associated increase in computing power to solve the mentioned algorithms. PoS is inherently an environmentally friendly alternative to PoW.

While the environmental factor already helps to differentiate PoS from PoW, there is another factor to consider: maintaining a fair distribution of power across the network, which should be a high priority goal for any cryptocurrency. With the increasing complexity of PoW mining, which requires more powerful devices and mining farms that are more expensive to operate and market, the ability for people to actually control such devices becomes more exclusive. The real barriers for the average person involved in PoW operations include the cost of equipment, electricity consumption spent on computing, and further consumption for cooling. This inevitably leads to the fact that most of the power can belong to smaller groups of miners, of which even fewer will be able to remain competitive, which will lead not only to a monopoly of rewards, but also to control over the networks. The QRAX network's use of PoS instead of PoW represents a much lower economic and resource independent choice for network participation and global use. In addition, setting up a PoW mining device requires more technical/advanced knowledge than creating a staking node, which opens up space for wider adoption and involvement of non-technical users.

2.3 Masternodes

The QRAX network has two layers. The staking tier is the first tier in which all QRAX holders can participate by placing their QRAX coins; the second is the masternode level. Masternodes are a collection of motivated nodes in the QRAX network that are responsible for performing certain specific tasks. The QRAX Masternode network originates from the Dash and PIVX cryptocurrencies, with a significant restructuring to the Proof of Stake consensus algorithm. As such, these nodes are an integral part of the QRAX digital ecosystem and are essential for network performance.

The masternode network performs a number of functions independently of the staking nodes. These various functions are limited to masternodes and cannot be performed by standard staking nodes. These responsibilities are spread across the masternode network, and no masternode has power or authority that exceeds other masternodes on the network.

2.3.1 Determined masternodes

Deterministic masternode lists are masternode lists built in each block based only on the data in the chain (previous list and transactions included in the current block). Deterministic lists are constantly recalculated on each block, forming a survey of all masternodes in the network to reach a consensus.

All nodes obtain (and validate) their masternode lists independently, from the same transactions in the chain, so they immediately reach a consensus on the state of the second level (number of masternodes, properties and status of each of them).

The previous system was supported by consensus mechanisms that existed before Satoshi Nakamoto solved the problem of Chinese generals. This meant that each node needed to maintain its own individual list of masternodes with P2P messages, not a blockchain-based solution. Due to the nature of the P2P system, there was no guarantee that nodes would come to the same conclusion about how the list of masternodes should look like. Discrepancies may, for example, arise due to a different order in which messages were received, or because messages were not received at all. This created certain risks for reaching consensus and limited the possible use of quorums by the system.

As a specific example, the previous system required the implementation of workarounds such as “voting for masternode bounty”, which was done several blocks in advance for each block to ensure that consensus was found and agreed. However, adhering to this consensus still carries a risk that could fork the network, so an attempt to disable Masternode in payment enforcement was added to prevent this issue from occurring. Spork has been used intermittently after major application and core updates.

This is a major overhaul that also brings many improvements to the user environment and experience while addressing the shortcomings of the previous system.

2.3.2 Masternode roles

Three different "roles" are defined for each masternode. Each role is represented by a pair of private / public keys.

1. Owner: Must be unique on the network. Can update the other two roles and the Masternode payout address.

2. Operator: must be unique on the network. The operator's key is stored in the QRAX.conf of the remote node and is used to sign P2P messages related to masternodes (for example, budget completion or masternode winners in compatibility code). It can also be used to update the IP address of the Masternode or the payout address of the operator (if the Masternode is configured to allow the payment of a percentage of the operator's reward).

3. Voting: Does not have to be unique (multiple masternodes can use the same voting key). It is used for voting on the budget.

The same key pair can be used for all three roles (at least for now, will the operator key be changed to BLS key soon?), but they must be different from the sub-address key.

2.3.3 New type of transaction

In QRAX, four new transaction types are introduced, each of which identifies a specific transaction payload with its own validation rules:

- COLLATERAL (Registry Provider): This is a basic special deal. Used to register a new Masternode, setting all its properties (for example, keys for each role). He creates the provision of the Masternode as one of its outputs, or refers to the unspent output of 50,000 QRAX in the blockchain (in which case it must include a signature with its keys as proof of ownership of 50,000 QRAX). PROUPSERV (provider-update-service):
- sent by the masternode operator to update the properties associated with the service (IP address, operator payout address).
- PROUPREG (provider-update-registrator): sent by the owner of masternode to update the operator key, voting key or payout address.
- RESTORATION (provider-update-revoke): sent by operator masternode to revoke a service and put masternode in a PoS disabled state (for example, in case of key cracking). The masternode can be revived later by sending ProUpReg tx, which sets the new operator key, and then ProUpServ tx (signed with the new key), which sets the new IP address for the masternode.

2.3.4 Code architecture

Deterministic masternodes are represented as objects of the CDeterministicMN class.
This class includes a member variable that stores a generic pointer to a persistent CDeterministicMNState object that encapsulates the DMN state (updated properties and status).

The list of masternodes is represented by the CDeterministicMNList class, which uses immutable functional maps to store up-to-date information about each record. A new list is created in each block and is maintained by CDeterministicMNManager. The use of immutable functional maps is an elegant solution developed by Codablock[7] to reduce the memory overhead required to update the list of masternodes in each block by adopting a copy-on-write approach.

Immutable data structures are provided by default in functional programming oriented languages like Clojure or Scala, but for C ++ we currently need to rely on third party libraries. In the future, it will be possible to study an implementation based on std :: maps, but this will seriously affect performance and will require hundreds of MB in RAM just to serve the MN list.

2.3.5 Masternode vote on budget allocation

As a Decentralized Autonomous Organization (DAO), QRAX operates and is subject to its own self-governing community. Neither entity nor a small group of coherent entities have the ability to determine the direction in which QRAX grows. This organic approach to governance is designed to maximize the benefits of members of the QRAX community who act in their own best interests. One way to achieve this form of governance is by voting by masternodes on monthly budget spending. Currently, masternode operators are given the opportunity to vote on suggestions made by community members to improve QRAX or circumstances for it for whatever reason. With over 100+ masternodes that require a significant investment in QRAX to operate, currently in use, this approach shares power significantly.

2.4 Steak nodes or simple nodes

Basically, PoS serves the same function as PoW in achieving blockchain consensus. However, as noted earlier, it is much less resource intensive, which is why it has become the consensus method of choice for QRAX and many other projects. Using the Proof-of-Stake model requires users to invest in a node by wagering (placing) their coins / QRAX on the node (the main QRAX wallet). In exchange for bets, users receive a certain amount of coins in return. Stakenodes are responsible for what miners do in Proof-of-Work: ordering transactions and creating new blocks so that all nodes can agree on the state of the network.

Proof-of-Stake and Stakenodes contain a number of significant improvements over the Proof-of-Work system [8]

- Better energy efficiency - no need to use multiple energy sources, lowering barriers to entry.

- Reduced hardware requirements - no expensive or specialized hardware is needed to have a chance to create new blocks.

- Stronger immunity to centralization - Proof-of-stake leads to more nodes on the network.

  To run Stakenode, users simply need to run the latest version of the main QRAX wallet app (on the device that will support it - laptop, desktop, raspberry pi, etc.) and have at least 1 QRAX in their wallet and have a wallet unlocked for staking.

2.5 Assets Network

2.5.1 Description

Assets development was created to attract participants to the network, maintain the state, develop and popularize. Each participant creates his own structure of child nodes. Upon receipt of the first transaction, the participant's wallet is activated in the network and is embedded in the general data structure. Assets represent the percentage of accruals per day/month/year, the size of the reward from the main balance, the sum of the balances of child nodes up to level 100 in depth.

2.5.2 Terms

Structure - is a set of nodes and connections between them, having a tree-like form, with an unlimited number of nodes in width and 100 nodes in depth.

The identifier - is a unique hash string of the wallet created when the transaction is first received.

A node - is a separate wallet activated by a transaction and tied to an upstream node ID.

A pool - is a network member organizing a dpos reception to provide a larger percentage of the reward to members.

dpos - the procedure for delegating your balance to the pool in order to receive a reward based on the percentage of the pool.

2.5.3 How Assets work

Each wallet can be included in the structure only in one place, it has a single upstream node and many downstream nodes. Upon receipt of the first transaction, the node is activated and installed into the structure. The data is written to the blockchain. You can view your structure in the Assets tab. When the balance of the wallet (incoming or outgoing transaction) changes, the accumulated accruals of Assets are calculated by interest and balance at the time of receipt of the transaction. The reward is paid in the next block after the block containing the transaction. The accrual of rewards does not depend on the availability of the wallet (disabled/enabled).

2.5.4 Delegated POS

Each participant can delegate their coins to a remote address, which acts as a pool. A participant delegating a certain amount of coins will receive an Assets reward based on the percentage of the pool, while the delegated amount will not be taken into account in calculating Assets in his own wallet. The pool operator receives 10% of the reward calculated for the pool member.

2.5.5 Technical implementation

When a transaction is sent, the sender's identifier is written into its structure; on the receiver's side, the data is read and written into memory. The wallet and upstream ID is written to the wallet.dat file. Any node in the network has an identical structure of all nodes. The identifiers are written to the block. The reward transaction is of the "assetsmint" type, all nodes that need to receive the reward are written to the recipients in one transaction.

2.6 Coins burning

Coins are burned when sending any amount to the genesis wallet address: QU1yzBpsPpbg6BN5pgsVbssW6WWAcxHFHd

3. CONTROL

Community-developed decentralized governance is the governing function of the QRAX DAO. Within the framework of this system, there is the possibility of monthly financing of proposals from the QRAX budget. Proposals are submitted by any level 2 masternode voting node. Masternode owners located around the world determine whether it is appropriate to fund an offer.

3.1.1 Community Budget:

Approximately every month, the QRAX treasury has a fixed number of coins freely available. These funds are directed to the implementation of proposals that received a sufficient percentage of votes "for" in relation to votes "against" (~ 10%). For example, if there are 100 masternodes, the proposal must have 10 (10% of 100) or more clear Yes votes. (Yes votes minus No votes).

The QRAX budget is funded through one QRAX for each block added to the network. This creates a single available budget for each block cycle. These QRAX are not "created" by themselves, but are only distributed as available for creation / use. Proposals are submitted to the community system, voted on, and those proposals that are accepted are allocated the funds requested by them.

The payment of these budgetary funds occurs in the form of a "superblock" that occurs every 44,000 blocks (approximately 1 month). Superblocks were created to seamlessly administer the payment side of decentralized voting proposals. If the proposal is voted and confirmed, Superblock will appear at a certain number of blocks and will automatically take care of all payments, as confirmed by the code. This provides a decentralized system for the voting/payment process.

Superblocks work hand in hand with a budget system. At the first stage of the budget system, the proposal is prepared and transmitted to the network. After 24 hours, it is considered competent and can be voted on. Once this happens, at least 10% of the network needs to vote "yes" to get into the "budget forecast". The budget projection is simply all eligible bids sorted in {YesCount - NoCount} order (the number of masternodes that voted for a given proposal minus the number of nodes voted against). Since bids are paid, this continues until the budget system runs out of QRAX for that billing period and it stops adding bids to the forecast. Subsequently, the QRAX network will accept the budget forecast and refine it. At this point, the rest of the Masternode network will compare their forecast with the final budget, and if they match, they will vote "Yes". If more than 10% of the network votes for the final budget, then when the next superblock is reached, the network will create these blocks. Superblocks simply pay one proposal per block until the monthly budget is paid.

The available funds for each superblock are equal to the number of blocks since the last superblock multiplied by the number of QRAX allocated to the superblock from each block. The math here is pretty straightforward, especially because this is where the "dedicated" QRAX comes into play. One QRAX per block and one block every minute for 24 hours every 31 days This forms the "budget" available for proposals.

Offers are sorted by their net yes votes (yes votes minus no votes) and then they are paid in order from highest pure yes to lowest.

The total amount of QRAX required to fund all pending proposals is rarely equal to the available QRAX, see table 1. If the total funds required for all pending proposals are within budget, not all QRAX will be created. For example, if all passing offers are 20,000 QRAX, then only 20,000 QRAX are created and paid for by those offers.

Conversely, if the accepted proposals exceed the 44,000 QRAX allotment, the proposals are funded in the order of their positive votes until the QRAX budget is exhausted. For example, if there are five pending proposals for 10,000 QRAX (50,000 total), only the first four will be funded and the remaining will not receive funding. The protocol will finance only those projects that can be fully funded. Any remaining unspent funds are not carried over and never created. It is possible that exactly 44,000 QRAX can fund the ongoing proposals and there will be nothing left.

3.1.2 Submission of proposals:

Anyone can submit their proposal for a vote. Each submission of an offer costs 100 QRAX, which is burned. It does not matter what contribution a person makes to the development of a project - a designer, coder, singer, financier, etc., a useful contribution to the ecosystem is important.

3.1.3 Decentralized voting:

Masternode owners vote on the proposals put forward. This vote is decentralized and anonymous. Each masternode owner has one proposal vote for each masternode they own. That is, one masternode is one vote.

3.2 Community governance and organization

As mentioned above, the proposal system is submitted to the network (by anyone) for voting by level 2 masternodes. These worldwide site owners determine whether or not to fund the proposal.

There is another aspect of QRAX (not directly related to blockchain or budget payments) that relates to how the community (the people who choose to participate, develop and work to help the larger QRAX economy and ecosystem grow) manage themselves and themselves i.e. organize the ecosystem. These aspects relate to ancillary areas of social communication such as Telegram, Twitter, Discord, etc. In some cases, people submit proposals for funding to take on a role (eg social media coordinator, etc.) in managing aspects of the ecosystem. However, in most cases, people voluntarily donate their time, talent and energy to support the broader vision of QRAX.

The first guiding principle around which these people gather is the QRAX manifesto, which states:
PRIVACY is non-negotiable. This is a fundamental human right.
FREEDOM is the most important thing.
TECHNOLOGIES evolve, GOVERNANCE must also evolve.
Confidentiality LETS to have the freedom to share what you want with EVERYONE, as well as the freedom to RESTRICT for those who see your information.
We believe that this is everyone's CHOICE.
MANAGEMENT is used to achieve goals and develop the FUND.
DAO IS UNTOUCHABLE.
Join us WHEN you want, BECAUSE you like and FOR AS MUCH LONG as you like.
Let's explore ALL the options TOGETHER.
You are IMPORTANT to US, IMPORTANT in interaction with the proposed tools.
It's time to use your FULL potential.

Here are some of the key "wise" leadership skills based on the book "Swarmwise" of Rick Falving [10], leader of the Swedish Pirate party [11]:

1 Freedom from control
Breaking free from control is the first rule of the leadership swarm. The leader of the swarm leads primarily through inspiration. Delegating authority can be daunting, but for a swarm to function, all parts of it must be self-sufficient and autonomous. This is the only way to take advantage of swarm efficiency and execution speed. To lead by releasing control, a leader must lead through inspiration and example and empower any member of the swarm to step out and take on the role. It happens organically; when a task or function is required, no one assigns it; someone will volunteer to lead it and inspire others to volunteer to follow it. The swarm architecture allows you to create leaders as needed; as soon as the role, task or function is fulfilled, the leader of this function ceases to lead. No one in the organization has an advantage over anyone else, and no one is assigned a role by anyone else; leadership occurs naturally when a need is met by talent.

2 Build a culture of leadership and trust

For decentralized governance to be successful, it must be supported by a culture of trust. The founder creates this culture for the organization by setting tone and example and leading more as an archetype than as a manager or mentor. Therefore, the founder and all leaders in the organization must maintain an excellent personal reputation, avoid negativity, and always demonstrate values such as patience, collegiality, passion, and understanding.

3 Follow the Rule of Three Pirates when making your decisions.

The Rule of Three Pirates is a method of delegating decision making to the local area of the swarm where a decision is needed, speeding up action, and avoiding bureaucratic inertia. Usually, if three activists agree that something is good, they do not need to ask permission to act on behalf of the organization.

4 Define the message, leave the branding to the swarm.

The swarm leader defines the content of the message and leaves it to others to decide how best to convey the message in terms of context and audience. There are no consistent messages, slogans, catchphrases, or style guides in the swarm. The same message can be delivered in many different ways to meet the needs, values and characteristics of a local audience.

5 Be the face of the media

The rest of the world needs an avatar to associate with the swarm, so it is important for the swarm leader to personally interact with the media, including all press appearances, major public events, and rallies.

6 Build a timeline

Swarm members need to understand where they are, where they are going, and how they are going to get there. To build trust, a leader needs to establish a transparent timeline and identify key milestones that swarm members can understand, participate in, and feel accomplished as they are achieved.

7 Set visible, active, overarching goals

The swarm is not attracting people for social reasons; they join the swarm because they believe in the mission of the swarm and want to complete it. For people to be involved, goals need to be defined, which must be inclusive and engaging. Measurement and gamification are ways to keep the swarm engaged and focused, and to harness natural competition to get things done and achieve goals. To keep swarm members motivated, rewarding them with recognition and attention is an important step in maintaining morale and faith. Swarm leadership increases the resilience of organizations; the swarm leader creates an ecosystem that is adaptable, redundant, and self-organizing. Ultimately, swarm leadership drastically reduces bureaucracy, offering each member the freedom to take the initiative, participate and lead according to their skills and level of interest.

4. PROTECTION OF HUSH FINANCIAL DATA

In this direction, extensive development is underway. According to the road map[9], it should appear in the near future.

5. ECONOMIC MODEL

QRAX's monetary policy is designed to provide resilient infrastructure and services capable of supporting a scalable, decentralized and resilient node infrastructure. This will allow secure, verified and fast transactions around the world without astronomical QE and the resulting devaluation of its own coin. This policy has had a detrimental effect on other cryptocurrency projects, many of which use the PoS protocol.

5.1 Money-credit policy

QRAX's monetary policy will be shaped by how its underlying economic levers are influenced and adjusted over time. Design approvals ensure the long-term stability, robustness, and availability of the protocol. Monetary policy is specifically governed by the blockchain codebase, indirectly through the use of the network by its users, and controlled through the QRAX DAO through its protocol-level governance model.

The main economic levers governed by monetary policy include, but are not limited to:

- Cost & Burning Transaction Fee
- The rate of emission of coins per block.
- Distribution of rewards for issuing coins for a block between stakenodes and masternodes.
- Minimum staking amount.
- Requirements for Masternodes.

5.2 Economy of coins

- QRAX has a fixed generation rate per block (every 60 seconds).
- 6 QRAX is a block reward (1 QRAX for stakernodes, 5 QRAX for masternodes).
- 1 QRAX is "allocated" (not created) to the budget.
- QRAX relies on the fact that both stakers and masternodes own their own QRAX coin to help decentralize, manage and secure the network.

- Both masternodes and stakernodes are rewarded.
- The balance between staking profitability and masternode yield is achieved naturally. Staking profitability decreases with the increase in the total number of coins placed, and the profitability of masternodes decreases with the growth of active masternodes in the network.
- QRAX users pay a small transaction fee.
- All transaction fees are burned, removing coins from the total amount.
- QRAX has tail emissions. (The tail emission is important because the block reward is an incentive for network participants to continue hosting and ensure the operability of the network without shifting costs to users in the form of high commissions.)

Burning transaction fees acts like an economic thermostat - as transactions increase, so does the corresponding burning of coins.

5.3 Maximum number of coins

Although the ideology of the network does not discriminate against any indicator and characteristic of the protocol, and does not limit the maximum number of coins in circulation, however, it should be understood that the actual amount in circulation is strongly correlated with the dynamic supply of coins and the burning of transaction fees, as well as in the separation of unused QRAX from the maximum possible monthly formation of the budget. As a result of these factors, the actual number is likely to be less than all theoretical design highs.

5.4 Dynamic coin supply

While QRAX does not have a hard limit on the number of coins (a certain absolute limit), it does have a soft limit (a limit on the number of coins produced when a certain condition is met). The QRAX soft-cap condition is met when the fee charged for network activities equals the amount set in the block. The blockchain will then start burning the same amount of coins it generates, limiting growth. Thus, QRAX has a dynamic coin feed calibrated by the blockchain in response to network action. The mechanism of the soft cap in a boiling environment shows what the maximum number of coins will be if each monthly budget is used at 100%, and what the new soft limit will be, and it will look at various significant (non-standard) transaction volumes (which will lead to a significant reduction in commission). When the burnout of the commission exceeds the number of coins generated as a block reward, the chart tends downward rather than upward.

To explain in more detail, QRAX's dynamic coin supply has a philosophy similar to that of an elastic currency, where the money supply adjusts in response to economic pressures - that is, business volume - to achieve stability. This is achieved by calibrating the volume in circulation by the volume of the loan. In a monetary economy, elasticity is achieved by removing currency from circulation. This occurs when making a decision in response to an unfolding market. This action pushes the economy in the desired direction.

However, unlike an elastic currency, QRAX does not shrink at the discretion of management and does not respond to the calibration of the volume of circulation in accordance with the volume of the loan. The only influencing factors are those based on transaction volume and commission burn, as interpreted by the algorithm. At a high transaction rate per second, the number of coins burned will be equal to the amount they generate, creating a neutralizing effect on the supply of coins. However, this soft cap value is not easy to predict as fees vary. These variables make it impossible to provide a fixed transaction rate per block for a neutralizing effect.

It is important to note that the balancing and burning algorithm controls the supply of coins in response to the most recent state of the blockchain. Neither the developer, nor the owner, nor the miners, nor any other party can create new stocks of coins. The algorithm ensures that the absence of a hard cap on the supply of coins works in favor of a healthy economy for QRAX as a currency. Since the target block time is 60 seconds with QRAX, savings are maintained by the minute, daily.

In the event that the balance of the QRAX burn algorithm becomes unfavorable to the health of the QRAX economy, a decentralized government consisting of masternode owners can raise this issue in order to vote for the best solution.

6. FUTURE CONSIDERATIONS

6.1 Beyond reliability

Although it is still too early to speak about the exact design and philosophy of an ideal transaction network that will be used in the future, leading to post-quantum resistance before it becomes a significant risk. This means that QRAX monitors and seeks to get rid of trust in reliable cryptographic evidence created by random participants in order to achieve a reliable PoS setting in blockchain technology, perhaps in version 2.0 a new concept of decentralization and protocol implementation will be proposed.

6.2 The impact of QRAX on the environment

While this is admittedly not the original goal of the QRAX project, the collective organization has realized that the cryptocurrency and blockchain space has pushed environmental boundaries wider and deeper than what we had in 2009. Where did we start in 2018? With the normalization of carbon offsetting in the business world, QRAX has moved off the ground to not only become the first cryptocurrency project to become carbon neutral (decarbonizing the planet), but also the first to span all the years of its existence.
At the date of publication, QRAX has become what we deem necessary: zero emission of CO.

6.3 Private staking

QRAX will introduce a completely new HUSH betting feature in version 2.0. This will allow the person to wager protected coins and receive staking rewards directly to the HUSH address. This feature will protect users' data, support the protection of their financial data and increase the percentage of shielded coins on the QRAX network, further strengthening all PoS protocols used.

6.4 Decentralized Autonomous Rate Pools (DPoS)

The idea for the 'pool' came from PoW. In PoW, you can either mine directly (similar to how it was during Satoshi's time) or join a "conglomeration" of miners called a pool (this is how the vast majority of PoW coins are mined). At QRAX we are now mostly "solo staking" (similar to solo PoW mining). The staker will receive a block reward only if he finds a valid block (in this case he will receive the full part of the block reward, i.e. 10 QRAX). With pools, you don't have to look for the winning block, you just specify the hashrate (in the case of QRAX: the power of the bets). When a block is discovered by a pool, the pool operator takes his share and allocates the remainder to the "reward pool". Every X blocks (for example, once a day or for each transaction), the pool operator distributes the funds accumulated in the reward pool among the stakers in percentage, based on how many bets were provided by each of them. However, in this case, the stakers need to entrust the operator with new rewards (just like PoWminers do when they point their ASICs to the mining pool). The idea behind a "no trust" pool (or rather a "decentralized standalone" DPoS rate pool) is to remove this centralization element by allowing any full node player to participate (and compete) as the pool operator, and by making the reward distribution verifiable by consensus (forced payment at a certain height, as is the case with superblocks).

6.5 Evolution of management

A significant amount of time and research has been spent exploring what the next evolution of DAO governance in QRAX might look like. A selection of these studies can be found on our official website [6].

7. ACKNOWLEDGMENT

QRAX comes from countless ideas, dreams and visions that existed before its creation. The vision of decentralized, rights-protecting, digital freedom of exchange and value transfer was discussed even by Milton Frieddman [12] back in 1999. There are many people who should be commended and thanked. Without the help of many outstanding people, QRAX would not exist. However, especially the current "team" of people, the first QRAX FOREVER community, supporting and developing the QRAX ecosystem as a whole, be they developers, social managers, industry communities, business developers and many others. These groups of people, many of whom volunteer their time and effort, are what drives QRAX forward.

Special thanks to the following individuals for this whitepaper:
@FelixNoctuae - concept, proofreading and layout
@Daydry - tricky questions and clarifications)))

8. LINKS AND LITERATURE

https://dataoverhaulers.com/about-mike-chu/
https://bitcointalk.org/index.php?topic=5330036.msg56763889#msg56763889
https://explorer.qrax.net/block/0000005379c37c08e8c639938403824c3291377a324580705854812d67615b11
https://github.com/QRAX-LABS
https://explorer.qrax.net/charts/supply
https://qrax.org
https://en.wikipedia.org/wiki/Codablock
https://www.investopedia.com/tech/what-dao/
https://qrax.org/site/road-map.html
https://en.wikipedia.org/wiki/Rick_Falkvinge
https://en.wikipedia.org/wiki/Pirate_Party_(Sweden)
https://en.wikipedia.org/wiki/Milton_Friedman