KII Whitepaper

Table of Contents

1. Summary

KII is an encrypted and decentralized cryptocurrency, with serval improvements that allow for an increase in the total amount of coins emitted and the speed of blocks released. It maintains a two leveled incentivized network with Miners and Masternodes that allow for instantaneous payments and confirmations of a transaction without a centralized authority.

2. Introduction

Bitcoin is a cryptocurrency that has become a popular mean for exchange, as the first digital currency to capture a fair number of users. Since its start in 2009, its adoption has grown exponentially, however, a problem in the acceptance of Bitcoin in commercial establishments arises from the long confirmation times in the transaction.

Over time, other types of cryptocurrencies were created, such as Dash, the first cryptographic currency focused on reducing transaction times with "InstantSend" and increasing privacy features based on Bitcoin with "PrivateSend".

In this Whitepaper we propose several modifications to the Dash source code, resulting in KII, a decentralized cryptocurrency, which removes CoinJoin and the reward earmarked for projects within the source code governance system, guaranteeing the decentralization of the currency and prioritizing the incentives to the participants in the network.

With these improvements, the mining time in each block is reduced, generating instant, secure and low-cost transactions. At the same time, a secondary peer-to-peer network is set up that is incentivized to offer services to the network called KII Master Nodes.

3. Characteristics of the KII Network

3.1. Regular Node

Regular nodes can store an exact, complete, up-to-date copy of the chain. The Nodes create an interconnected network that shares information in a safe, fast and decentralized way. This operation performed by the Nodes is vital for the health and activity of the Blockchain network.

3.2. Mining Supply

The maximum total amount of coins is 1,800,000,000 KII of which 1,326,960,000 KII were obtained with the release of the genesis block and the other 473,040,000 KII will be obtained by mining in the release of each subsequent block, equivalent to 26.28% of the total supply.

This proportion is the result of giving priority to the Miners and incentivizing to lend their work capacity in the KII Blockchain since many available coins were allocated as rewards for the Miners.

KII is a cryptocurrency designed for real world use, therefore, the initial mining reward is 300 KII for each mined block, with an average target spacing of 1 minute and the halving will be every 788,400 blocks.

The production of KII is programmed to last during this century, since each halving programmed in 1.5 years or 788,400 blocks, will reduce the released coins by 50% every minute. This means that the rewards for mining will last until the end of the year 2074.

Block release time: 1 minute
Reward: 300 KII
Miners 50%: 150 KII
Master nodes 50%: 150 KII
Mining Coins: 473,040,000 KII
Duration of mining: Approximately 52 years.

When a Miner services the KII network, 150 KII are released every minute. These released coins are distributed according to the number of active miners in the network, along with the hash rate capacity offered during mining.

3.3. Network of Master Nodes

There are two types of Nodes. Regular Nodes are virtual connection points which allow to create, send and receive all forms of data and information maintaining an interconnection in the Blockchain network. However, regular nodes do not receive rewards every time a block is released.

Master Nodes, which are servers that work in a p2p network, receive the rewards allocated each time a block is released on the Blockchain, that is, they allow their use by peers to receive updates about events in the

network.

These nodes require a significant volume of traffic and other associated resources that carry a substantial cost. Therefore, the Bitcoin network has seen a steady decline in the number of these nodes over time. Many solutions have been proposed for this, such as a new rewards plan by Microsoft Research and the Bitnodes incentive program.

Masternodes are very important for the health of the network, for this reason in the configuration of the KII Blockchain, they have high reward incentives to maintain their permanence over time.

Masternodes offer users the ability to quickly synchronize and propagate messages across the network. For this reason, we add a secondary network, the KII Masternode network, in the same way as Dash proposes. These Master Nodes will have high availability and provide a certain level of service to the network to be part of the Master Node Reward Program, pre-verifying the information that is being recorded in the block. As a result, validation times are reduced and network security is increased.

3.4. Instant transactions using InstantSend

Transactions made through InstantSend technology are characterized by being instantaneous, completing the transaction in seconds. This technology makes its application and implementation useful in POS "Point of Service" points of commerce, allowing sellers to use mobile devices in their traditional locations with point-of-sale systems for commerce in everyday life. In turn, users will be able to use this technology to make fast payments, non-commercial transfers without requiring a central authority.

The use of this technology is available in our applications, including the Web Wallet, enabled for use on the official page of www.kii.global. It will also be available on the App Store and Google Play. However, if the user wishes to have the application from a desktop device, it is already available for download on Windows, Mac OS and Linux OS.

This technology can be executed through quorums with Master Nodes, where users are able to send and receive instant and irreversible transactions. Once a Quorum is formed, transaction inputs are locked to a single specific transaction, a transaction lock requires about two seconds to be established on the network.

If a lock consensus is reached in the Masternode network, all conflicting

transactions or blocks thereafter will be rejected, unless they coincide with the exact ID of the transaction assigned to the lock that takes place. This configuration makes the Master Nodes exercise a second layer of security in the KII network, making the reliability of protecting or sending money through KII highly secure, providing confidence to users.

3.5. Chainlocks

Chainlocks is a dedicated Maternodos Quorum that offers an additional layer of security. The Quorum opens with 400 masternodes in the KII network that provides security when accepting payments and prevents attacks on the Blockchain.

This technology is implemented in parallel with InstantSend and creates an environment where payments can be accepted immediately without the risk of a "Blockchain shake-up event".

4. Architecture

4.1. Deterministic Ordering

A special deterministic algorithm is used to create a random ordering of the Masternodes. Using the proof-of-work hash of each block, the security of this functionality is guaranteed by the mining network.

Pseudocode to select a Master Node:

```
For (mastenode in
masternodes){ n =
masternode.CalculateScore();
 if(n > best_score){
 best_score = n;
 winning_node = masternode; } }
CMasterNode::CalculateScore(){
n1 = GetProofOfWorkHash(nBlockHeight); // get the hash of this
blockn2 = Hash(n1); //hash the POW hash to increase the entropy
n3 = abs(n2 •
masternode_vin); return n3;}
```

The sample code can be extended to provide a ranking of the Masternodes,

by selecting a “second”, “third”, “fourth” Masternode from the list.

4.2. Roles and Proof of Service

The Masternodes can provide a multitude of additional services to the network. As a proof of concept, our first implementation included *InstantSend*. Through what we call proof of service, we can request that these nodes be online, responding to the standard of the correct block height.

Malicious actors could also operate Masternodes, but not offer the quality of service required by the rest of the network. To reduce the possibility of people using the system for their exclusive benefit, the nodes must ping the rest of the network to ensure that they remain active.

This task is done in the Maternodes network by selecting two quorums per block. Quorum A verifies the work of Quorum B on every block. Quorum A are the closest nodes to the current block hash, while Quorum B are the furthest from said hash.

Masternode A (1) verifies Masternode B (range 2300) Masternode A (2) verifies Masternode (range 2299) Masternode A (3) verifies Masternode B (range 2298).

All the necessary work to check if the network nodes are active is done by the Master Node network itself. Approximately 1% of the network will be checked in each block. This results in the entire network being checked more than fourteen times a day. In order to keep the system trustless, we randomly select nodes with the Quorum system. Then we also require a minimum of six violations to disable a node.

To cheat the system an attacker will need to be selected six times in a row. Otherwise, the violations will be neutralized by the system as other nodes are selected by the Quorum system.

The selection of Masternodes is pseudo-random based on the Quorum system.

4.3. Masternode Protocol

Masternodes propagate themselves on the network through a series of protocol extensions including an advertisement message and the Masternode ping message. These two messages are all that is needed to make a node active on the network. Part of these messages are those intended to perform a service test request, *InstantSend*.

Masternodes are originally formed by sending 150,000 KII to a specific wallet address, which will “activate” the node thus making it capable of being propagated through the network. A private secondary key is created to sign all subsequent messages. The above key allows to completely block the wallet when it works in a self-sufficient mode.

A cold mode is possible thanks to the secondary private key stored on two separate machines. The primary "hot" client signs the 150,000 KII input by including the secondary signing private key in the message. Shortly after, the “cold” client sees a message that includes its secondary key and is activated as a new Master Node. This allows the “hot” client to deactivate (client disconnected) and leaves no chance for an attacker to get the 150,000 KII by gaining access to the Masternode after activation.

As soon as it is started, a Master Node sends a message to the network "Master Node Announcement", containing the following:

Message: (Input 150,000 KII, Accessible IP Address, Signature, Signature Time, 150,000 KII Public Key, Secondary Public Key, Donation Public Key, Donation Percentage).

Every 15 minutes and thereafter, a ping message is sent to prove that the node is still up:

Message: (150,000 KII Entry, Signature (using secondary key), Signature Time, Stop).

After a time to live has expired the network itself will remove the inactive node from it, causing the node to not be used by clients or receive payments. Nodes can also constantly ping the network, but if they don't have their ports open, they will eventually be marked down and not charged.

4.4. Masternode list propagation

New clients joining the KII network must be notified of the currently active Master Nodes in order to use their services. As soon as they join the mesh network, a command is sent to their peers requesting the known list of Masternodes.

Clients perform a process similar to cache clearing, to register Masternodes

by updating their current state, so when clients reset the list, they simply load this file instead of asking for the full list of Masternodes, improving the ease of administration and updating of data in the master nodes.

4.5. Payments through Mining and Imposition

To ensure that each Masternode collects its fair share of the block reward, the network must enforce payment of blocks to the correct Masternode. If a miner does not comply with the rules, their blocks must be rejected by the network, otherwise cheating would be incentivized.

We propose a strategy where the Masternodes form quorums, selecting a winning Masternode and propagating their message. After N messages have been propagated to select the same beneficiary, a consensus will be formed and said block in question will be required to pay the Master Node.

When mining on the network, the pool software (websites that combine the efforts of individual miners, *the Mining Pool*) uses the RPC API to get the information about how a block should be generated. To pay the Masternodes, this interface must be extended by adding a secondary beneficiary (GetBlockTemplate). Afterwards, the groups propagate their successfully mined blocks, including a payment that is shared between them and a Master Node.

This payment has a proportion of 50% of the coins released each minute, which corresponds to 150 KII for mining, during the first halving or in the first 788,400 blocks, these released coins will be distributed according to the actors that are active in the network, along with the mining capacity that is made available on the KII network.

The number of mined coins will decrease by 50% between each halving which is scheduled every 18 months, that is, 300 KII corresponding to Halving 1, 150 KII to Halving 2, 75 KII to Halving 3, and so on until at least 52 years of mining.

4.6. X11 Hashing Algorithm

The X11 algorithm is a "Proof of Work" POW protocol, which is characterized by being minable, it also has one of the safest Blockchain configurations that exist in the crypto world, since by combining the sequence of 11 different Hash functions known as chaining of focused algorithms with a single purpose,

results in the best possible security in a network.

This algorithm is widely used since the ROI "Return on Investment" is higher than other protocols, making it an attractive algorithm for miners.

In this way, miners and users will have peace of mind in operating and using our network. In turn, the configuration of the miner is a simple task to synchronize, where a large mining capacity is not needed to be active in the network, that is, a miner with a low Hash rate capacity will also have a low consumption at comparison of larger machines.

5. Network Incentives

Quorums Without the Need for Trust

The voting process bestowed in the Quorum is essential, which oversees verifying if the transaction is valid or not, and whether is should be released or blocked. Currently the KII network has ~50 active Masternodes. To become an active Masternode, a guarantee of 150,000 KII in collateral is required.

We created a system in which no one can control the entire network. For example, if someone wants to control 50% of the Masternode network, they must buy 3,750,000 KII on the open market.

All transactions are verified by temporary Quorums, guided by a deterministic voting formula that makes it almost impossible to have the majority of the participation within the Quorum.

With the addition of the Masternode network and the collateral requirements, we can use this secondary network to perform delicate tasks without the need for trust, where no entity is capable of 100% control of the outcome. By selecting N pseudo-random Master Nodes from the total in the pool to carry out the same task, these nodes can act as an oracle, without the entire network performing the task. You can see an example of a quorum implementation without the need for InstantSend trust, which uses Quorums to ratify transactions and block entries or the proof of service implementation.

This deterministic process makes it possible to eliminate monopolies in decision-making, reducing the fact that only one party has total control of the network, while increasing security standards and reducing malicious attacks

on the KII Blockchain ecosystem.

6. Tokenomics and rewards

6.1. Masternode Reward Program – Costs and Payments.

One of the causes of the decrease in the number of full nodes of the Bitcoin network is the absence of incentives in their operation. Therefore, the maintenance costs of a full node increase over time since the use of the network is larger, creating more bandwidth and increasing operator costs.

Masternodes are full nodes, analogous to their counterparts on the Bitcoin network, with the difference that they provide a level of service to the network and have an established link with collateral they posted in order to participate.

The guarantee is fixed, and it's safe as long as the Masternode is operating. This allows investors to serve the network, produce a return on their investment, and reduce currency volatility.

To operate a Master Node on KII, the node must store 150,000 KII. When active, nodes provide services to network customers and are paid in return in the form of a dividend. This allows users to pay for services and get a return on investment. Masternodes receive payments from the same money pool, equal to 50% of the total reward of the mined block every minute. This will be directed to the Wallet address tied at the time of configuring the Master Node.

Due to the fact that the Masternode reward schedule is a fixed percentage, and the total number of nodes present on the network fluctuates, the expected rewards will vary based on the current count of all active Masternodes. Payments for a standard day for operating a Master Node can be calculated using the following formula:

$$(n / t)^* \, r^* b^* a$$

Where: n is the number of Masternodes controlled by an operator, t is the total number of Masternodes, r is the current block reward (currently 300 KII), b is the average number of blocks in a day.

Generally speaking, 1440 is the average payment of the Master Node (50% of the average payment amount per block). The return on investment for operating a Master Node is calculated with the following formula:

$$((n / t)* r * b * a * 365) / 1000$$

The calculation must be done with the variables already mentioned. The cost associated with operating a Master Node is minimal, however this depends on how the master node is hosted, that is, the cost is associated with internet, energy, cloud servers, computer equipment and the installation of the master node which has a one-time charge of the KII fee rate.

Currently, with 1.35 billion KII in circulation, a maximum of 9,000 nodes could function on the network.

7. Conclusion

We have created the KII network with a targeted, real-world use: an efficient cryptocurrency focused on speed, security, decentralization and low cost. Users who participate in our project will have the trust that each modification made is in order to provide the best options available to the community, and as such, several profitable means to engage in the network have been created, either as Miner, Master Node, a commercial user, or as a holder of KII.

The models created in KII try to have less price volatility and faster message propagation through the network. This is achieved through a two-tier model encouraged to provide greater security in the KII network, instead of the traditional model that only includes one level, such as Bitcoin.

The creators of KII focused on developing a cryptocurrency capable of solving a latent problem in emerging economies, specifically Latin America, along with the potential for its price and adoption to grow exponentially in the crypto market.

8. References

1. S. Nakamoto. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
2. S. Barber, X. Boyen, E. Shi, E. Uzun. (2012) Bitter to Better — HowtoMakeBitcoin a Better Currency. http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.pdf
3. CCN. (Marzo 2021) 3 Solutions for Instant Bitcoin Confirmations. https://www.cryptocoinsnews.com/3-solutions-instant-bitcoin-confirmations/
4. M. Babaioff, S. Dobzinski, S. Oren. A. Zohar. (2012) On Bitcoin and Red Balloons. http://research.microsoft.com/pubs/156072/bitcoin.pdf
5. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, GM. Voelker, S. Savage. (2013) AFistful of Bitcoins: Characterizing Payments Among Men with No Names. http://www0.cs.ucl.ac.uk/staff/s.meiklejohn/files/imc13.pdf
6. D. Cawrey. (2015) Why Don't People Run Bitcoin Nodes Anymore?. https://medium.com/zapchain-magazine/why-don-t-people-run-bitcoin-nodes-anymore-d4da0b45aae5
7. DASH Ninja. (2022) Deterministic Masternodes Monitoring. https://www.dashninja.pl/
8. Dash (2022) Dash Ecosystem Overview. https://www.dash.org/
9. Blockchain.com (2022) Bitcoin Explorer. https://blockchain.info/tx/4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa89f922952f3e57ee6d603
10. NLST (2012) SHA-3 Project. https://csrc.nist.gov/projects/hash-functions/sha-3-project
11. C. Decker,* R. Wattenhofer. (2013) Information Propagation in the Bitcoin Network. https://tik-old.ee.ethz.ch/file//49318d3f56c1d525aabf7fda78b23fc0/P2P2013_041.pdf
12. Dash Core Group, Inc. (2021) What is Dash?. https://docs.dash.org/en/stable/introduction/about.html#whitepaper