Kii Whitepaper

Summary.

Kii is a cryptocurrency based off Dash with various improvements that allow an increase in the total amount of coins emitted and the speed of blocks released. It maintains a two leveled encouraged network known as Masternode network and instantaneous payments with KiiSend, which facilitate instant confirmation of the transaction without a centralized authority.

1. Introduction

Bitcoin is a cryptocurrency that has become a popular mean for exchange, as the first digital currency to capture a fair amount of users. Since its start in 2009, Bitcoin has experienced rapid adoption among many and is often used in retail sales. An essential problem when accepting the use of Bitcoin arises in situations where the network requires long wait time to confirm that the transaction is valid. Various payment companies have created alternative methodsto allow sellers to perform unconfirmed transactions, but these solutions use a trust counterpart to mediate the transaction in addition to the protocol.

Bitcoin offers pseudo-anonymous transactions in a public accounting ledger, with a one on one relationship between the issuer and the receiver. This structure facilitates a permanent record of all the transactions that have ever taken place in the network. Bitcoin is greatly known in academic environments for offering reduced privacy, yet, even when this limitation exists, many peopletrust its financial blockchain history.

Dash is the first cryptographic currency that focuses on privacy based off of Bitcoin and it offers additional features through its PrivateSend option and instantaneous payments through InstantSend.

In this paper we propose a series of improvements that result in the creation of the KII Blockchain that permits instantaneous transactions, constructs a secondary encouraged network that improves security, lowers the network fees and offers staking rewards.

2. Masternode Network

The complete nodes are servers that function on a p2p network, which allow their peers to access the information on that network. These nodes require high traffic volume along with other resources that require a substantial cost. Therefore, in the Bitcoin network there has been a constant reduction in the number of nodes through time, resulting in an increasing spread of the block reaching up to 40 seconds. Many solutions have been proposed for this, such as the new rewards plan by Microsoft Research and Bitnodes´ incentive program.

These nodes are very important for the health of the network. They provide the clients the capacity to synchronize and spread the messages quickly through the network. Similar to Dash, Kii maintains a secondary network called the "Masternodes network". These nodes will have a higher bandwidth and provide greater availability to the network of the Masternode Rewards Program.

2.1 *Masternode Rewards Program - Costs and Payments*

The main cause in the reduction of the amount of complete nodes of the Bitcoin network is the lack of incentives to operate one of them. The cost of maintenance of a complete node increases with time because the use of the network is growing, therefore increasing the cost for its operators. Due to the increase in cost, the operators provide the service in a way that is less expensive for them to operate or employ a light node, which hinders the network.

The master nodes are complete nodes, analogous to their counterparties on the Bitcoin network, with the difference that they provide a level of service to the network and require collateral to be able to participate. The collateral is fixed and is secure as long as the Masternode is functioning. This allows investors to service to the network, produce yield from their investment and reduce the volatility of the currency.

To operate a Masternode, the node must store 150,000 KII. When they are active, the nodes provide services to the clients of the network and in exchange they get paid in the form of a dividend. This allows the users to pay for the services and obtain a return on investment. The Masternodes receive the payment from the same financial reserve. 45% of the total block reward is dedicated to this program.

Since the Masternodes reward program is a fixed percentage and the total number of nodes in the network fluctuates, the expected rewards vary according to the total number of active Maternodes. The payments for operating a Masternode on a standard day can be calculated with the following formula:

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

n is the number of Masternodes controlled by an operator

t is the total number of nodes Masternodes

r is the reward for the current block (currently 300 Kii)

b is the average blocks in a day. It is generally 1440 for the Kii network.

a is the average Masternode payment (45% of the average payment amount per block).

The return of investment for operating a Masternode is calculated with

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

Where the variables are the same as above.

The cost associated with operating a Masternode implies some hard and soft limits of the active nodes on the network. Currently with 1,350 million of KII in circulation, a maximum of 9,000 nodes could work on the network. The soft limit is imposed by the price of acquiring a node and the limited liquidity in the exchange is due to the use of Kii as a currency and not simply as an investment.

2.2 *Deterministic Ordination*

A special deterministic algorithm is used to create an aleatory ordination of Maternodes. Using the hash of each block´s work test, the security of this functionality is guaranteed by the mining network.

Pseudocode to select a Masternode:

```
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 code used as an example can be extended to provide a classification of Masternodes by selecting a ¨second¨, ¨third¨, ¨fourth¨ Masternode from the list.

2.3 *Quorums without Needing Trust*

Currently the Kii network has ~50 active Masternodes. By demanding a collateral of 150,000 KII to become an active Masternode, we created a system in which no one can control the whole network. For example, if someone wants to control 50% of the Maternodes network they must purchase 3,750,000 KII in the open market. Additionally, all transactions are verified by temporary quorums guided by a deterministic formula of voting which makes it almost impossible to have the majority within the quorum.

By incorporating the Masternodes´ network and the collateral requirements, we can make use of this secondary network for delicate tasks without needing trust, where no entity is able to control the result. Selecting *N* pseudoaleatory Masternodes from the total group that is to take on the same task, these nodes can act as an oracle without having the whole network do the task.

An example can be seen of a quorum implementation without needing trust through *KiiSend*, which uses quorums to rectify transactions and block the inputs or the implementation of proof of service.

2.4 *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 *KiiSend*. Through what we denominated proof of service, we can request that these nodes be aligned, responding in fact to the standard of the correct block.

Malicious actors could also operate Masternodes, but not offer the service quality required by the rest of the network. To diminish the possibility of others using the system for their exclusive benefit, the nodes must ping the rest of the network to ensure they remain active. This task is done in the Maternodes network by selecting 2 quorums per block. Quorum A proves Quorum B´s service in each block. Quorum A are the nodes closest to the hash of the current block, while Quorum B are the farthest away from that hash.

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

All the necessary work to prove if the network nodes are active is done by the Masternodes network itself. Approximately 1% of the network will be tested in each block. This results in the network testing itself completely more than 7 times in a day. With the purpose of maintaining the system without trust, we select aleatory nodes with the Quorum system. After that we also require aminimum of six violations to deactivate a node.

To deceive the system, an attacker will need to be selected six consecutive times. On the contrary, the violations will be neutralized by the system by the selection of other nodes by the Quorum system.

The selection of Masternodes is pseudoaleatory based in the Quorum System.

2.5 *Masterrnodes Protocol*

The Masternodes are spread through the network through a series of extensions from the protocol including an announcement message and the Masternode´s ping message. These two messages are all that is needed to activate a node on the network. Besides these messages are those destined to perform a proof of service petition, *KiiSend*.

Masternodes originally form sending 150,000 KII to a specific wallet destination, which will “activate” the node enabling it to spread through the network. A private second key is created to sign all the posterior messages. The previous key allows the wallet to be completely blocked when it functions under self-sufficient mode.

A cold mode is made possible by the secondary private key stored in two separate machines. The primary ¨hot¨ client signs the input of 150,000 KII including the private key from the secondary signature in the message. Shortly after, the "cold" client sees a message that includes his secondary key, and is activated as a new Masternode. This allows the ¨hot¨ client to deactivate (disconnected client) and leaves no chance for an attacker to obtain the 150,000 KII gaining access to the Masternode upon activation.

As soon as it starts, a Masternode sends a message to the network "Masternode announcement", containing as follows:

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

Every 15 minutes and after, a ping message is sent to show that the node is still active.

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

After a lifespan has expired the network will eliminate the inactive node from itself, causing the node to not be used by the clients or to receive payments. The nodes can also ping the network constantly, but if they do not have their ports open, with time they will be considered as inactive and will not receive the message.

2.6 *Propagation of the Masternodes List*

New clients that join the Kii network must be advised of the current active Masternodes so that their services can be used. As soon as they join the mesh network, an order is sent to their peers requesting the known Masternodes list. The clients use a cache object to register the Masternodes and its current state, that way, when the clients restart they simply load that file instead of asking for the entire Masternodes´ list.

2.7 *Payments through Mining and Imposition*

To guarantee that each Masternode charges its fair share from the reward per block, the network must make the block payments to the correct Masternode. If a miner does not comply with the rules, the network will reject its blocks.

Kii has developed a strategy where Masternodes form quorums. They select a winner Masternode and spread its message. After N messages have been spread to select the same beneficiary, a consensus will be formed and said block will be required to pay the Masternode.

When there is mining on a network, the group´s software (websites that combine the effort of individual miners, Mining Pool) uses the API RPC to obtain the information of how a block should be generated. To pay the Masternodes, this interface should extend itself by adding a secondary beneficiary (GetBlockTemplate). After that, the groups spread their mined blocks with success, including a payment that gets divided between them and a Masternode.

3. Instantaneous Transactions through KiiSend

Through quorums with Masternodes, the users can send and receive instantaneous irreversible transactions. Once a quorum is formed, the inputs of the transaction block to a unique specific transaction. A transaction requires 2 seconds for the blockage to be established on the network. If blocking consensus is reached in the Masternodes network, all the transactions or conflictive blocks would be denied from that moment, unless the exact ID matched the assigned transaction to the block that takes place.

This would allow vendors to use mobile devices in their traditional locations with point of sale (POS) systems for commerce in everyday life, and the users to pay non-commercial transactions rapidly in person as it occurs with traditional cash. All of this is done without a central authority.

4. Hashing X11 Algorithm

X11 is a hashing algorithm widely used, which takes a different approach, known as linking algorithm. X11 consists of all the 11 contenders of SHA3, calculating each particular hash and then sending it to the next algorithm in the chain.

5. Mining Supply

The maximum total of KII is of 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 through the concept of mining with the release of each subsequent block. The reward of initial mining is of 300 KII for each block mined, with an average Target Spacing of 1 minute. Halving will be every 788,400 blocks.

The production of Kii is scheduled to continue in this century decelerating near the end of the year 2074.

6. Conclusion

This paper presents various concepts to perfect Bitcoin and Dash´s design that result in improved fungibility and real world use for the averageuser, lower volatility in the price and a faster propagation of messages through the network. All of this is achieved through a two-leveled encouraged model, instead of the one level model present in other cryptocurrencies such as Bitcoin. Using this alternative network design, it is possible to add many types of services such as the decentralized mixing of coins, instantaneous transactions and decentralized oracles through quorums with Masternodes.

References

1. A peer-to-peer electronic cash system (2008)
2. http://eprints.qut.edu.au/69169/1/Boyen_accepted_draft.p df
3. https://www.cryptocoinsnews.com/3-solutions-instant-bitcoin-confirmations/
4. http://research.microsoft.com/pubs/156072/bitcoin.pdf
5. http://www0.cs.ucl.ac.uk/staff/s.meiklejohn/files/imc13.pdf
6. https://getaddr.bitnodes.io/nodes/incentive/

1. https://medium.com/zapchain-magazine/why-don-t-people-run-bitcoin- nodes-anymore-d4da0b45aae5
2. https://dashninja.pl/
3. https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf
4. https://github.com/dashpay/dash/blob/master/src/Masternode-pos.cpp
5. https://blockchain.info/tx/4eb3b2f9fe597d0aef6e43b58bbaa7b8fb727e645fa8 9f922952f3e57ee6d603
6. https://blockchain.info/tx/1694122b34c8543d01ad422ce600d59f8d8fde495ac9 ddd894edc7139aed7617
7. http://en.wikipedia.org/wiki/NIST_hash_function #competition_Finalists
8. http://www.tik.ee.ethz.ch/file/49318d3f56c1d525aabf7fda78b23fc0/P2P2013_0 41.pdf
9. https://docs.dash.org/en/stable/introductio#n/about.html whitepaper