LKSCOIN Chain

Protocol Information

Masternodes

In parallel to other blockchain protocols that use Full Nodes P2P networks that are very important to the health of the network, our LKSCOIN blockchain protocol uses a secondary network, better known as a Masternode network. These nodes have high availability and provide the required level of service to the network in order to be able to receive predetermined block rewards.

Masternode Reward Program

With time we could observe that full nodes on world known blockchains as Bitcoin were starting to decrease in number, as there was not enough incentive to run one (the more users using the network and the higher bandwidth, the higher the operational costs to run one). As the costs of operating full nodes raised, operators consolidated their services to be cheaper to run, or to run light clients which did not help the network at all.

Masternodes are full nodes, just like in the Bitcoin network, except they must provide a level of service to the network and have a bond of collateral to participate. The collateral is never forfeit and is safe while the masternode is operating. This allows masternode operators to provide a service to the network, earn payments for their services and reduce the volatility of the currency.

To run a masternode, the operator must demonstrate to control over **100.000 LKSCOIN**. When active, masternodes provide services to clients on the network, and in return receive regular payment from the block reward. Since LKS Foundation wants to incentivize masternodes, the rewards paid from blocks are **80%** (until block 614820, after this block the percentage will be 72%) dedicated to this program.

Due to the fact that the masternode rewards program is a fixed percentage and the masternode network nodes are fluctuating, expected masternode rewards will vary according to the current total count of active masternodes. Payments for a standard day for running a masternode can be calculated by using the following formula:

(n/t)* rba

n is the number of masternodes an operator controls
t is the total number of masternodes
r is the current block reward (500 LKSCOIN excluding PowerBlocks)
b is blocks in an average day. For the LKSCOIN network this usually is around 550 blocks.
a is the average masternode payment (72% of the average block reward)

Deterministic Ordering

A special deterministic algorithm is used to create a pseudo-random ordering of the Masternodes. By using the hash from the proof-of-work for each block, security of this functionality will be provided by the mining network.

Pseudocode, for selecting a masternode:

```
For(mastenode in masternodes){
   current_score = masternode.CalculateScore();

   if(current_score > best_score){
```

```
      best_score = current_score;
      winning_node = masternode;
   }
}

CMasterNode::CalculateScore(){
  pow_hash = GetProofOfWorkHash(nBlockHeight); // get the hash of this block
  pow_hash_hash = Hash(pow_hash); //hash the POW hash to increase the entropy
  difference = abs(pow_hash_hash - masternode_vin);
  return difference;
}
```

Trustless Quorums

Currently the LKSCOIN network has around **700 active** masternodes. By requiring 100.000 LKSCOIN collateral to become an active masternode, we created a system in which no one can control the entire network of masternodes. For example, if someone wanted to control 50% of the masternode network, they would have to buy 20,000,000 LKSCOIN from the open market. This would raise the price substantially and it would become impossible to acquire the needed LKSCOIN.

With the addition of the masternode network and the collateral requirements, we can use this secondary network to do highly sensitive tasks in a trustless way, where no single entity can control the outcome. By selecting N pseudo random masternodes from the total pool to perform the same task, these nodes can act as an oracle, without having the whole network do the task.

Roles and Proof-Of-Service

Masternodes can provide any number of extra services to the network. By utilizing what we call proof-of-service, we can require that these nodes are online, responding and even at the correct block height.

Bad actors could also run masternodes, but not provide any of the quality service that is required of the rest of the network. To reduce the possibility of people using the system to their advantage, nodes must ping the rest of the network to ensure they remain active. This work is done by the masternode network by selecting 2 quorums per block. Quorum A checks the service of Quorum B each block. Quorum A are the closest nodes to the current block hash, while Quorum B are the furthest nodes from said hash.

Masternode A (1) checks Masternode B (rank 2300)
Masternode A (2) checks Masternode B (rank 2299)
Masternode A (3) checks Masternode B (rank 2298)

All work done to check the network to prove that nodes are active is done by the masternode network itself. Approximately 1% of the network will be checked each block. This results in the entire network being checked about six times per day. In order to keep this system trustless, we select nodes randomly via the Quorum system, then we also require a minimum of six violations in order to deactivate a node.

In order to trick this system, an attacker would need to be selected six times in a row. Otherwise, violations would be cancelled out by the system as other nodes are selected by the quorum system.

Attacker Controlled Masternodes / Total Masternodes	Required Picked Times In A Row	Probability of success $(n/t)^r$	LKSCOIN Required
1/200	6	16e-15	100.000 LKSCOIN
10/200	6	16e-9	1,000,000 LKSCOIN
100/200	6	1,6%	10,000,000 LKSCOIN

The probability of tricking the system representing one individual masternode as failing proof-of-service

Where:
n is the total number of nodes controlled by the attacker
t is the total number of masternodes in the network
r is the depth of the chain

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

Masternode Protocol

The masternodes are propagated around the network using a series of protocol extensions including a masternode announce message and masternode ping message. These two messages are all that is needed to make a node active on the network, beyond these there are other messages for executing a proof-of-service request such as InstantSend.

Masternodes are originally formed by sending 100,000 LKSCOIN to a specific address in a wallet that will “activate” the node making it capable of being propagated across the network. A secondary private key is created that is used for signing all further messages. The latter key allows the wallet to be completely locked when running in standalone mode.*

*To raise the security of transactions, LKS Foundation raised collateral to 100.000 LKSCOIN tokens (from 1000 tokens on the Dash Network), while maintaining the 1000 LKSCOIN limit (same 1000 tokens on the Dash Network) for transactions.

A cold mode is made possible by utilizing the secondary private key on two separate machines. The primary “hot” client signs the 100,000 LKSCOIN input including the secondary signing private key in the message. Soon after the “cold” client sees a message including its secondary key and activates as a masternode. This allows the “hot” client to be deactivated (client turned off) and leaves no possibility of an attacker gaining access to the 100,000 LKSCOIN by gaining access to the masternode after activation.

Upon starting, a masternode sends a “Masternode Announce” message to the network, containing:

Message: (100K LKSCOIN Input, Reachable IP Address, Signature, Signature Time, 100K LKSCOIN Public Key, Secondary Public Key, Donation Public Key, Donation Percentage)

Every 15 minutes thereafter, a ping message is sent proving the node is still alive.

Message: (100K LKSCOIN Input, Signature (using secondary key), Signature Time, Stop)

After a time-to-live has expired, the network will remove an inactive node from the network, causing the node to not be used by clients or paid. Nodes can also ping the network constantly, but if they do not have their ports open, they will eventually be flagged as inactive and not be paid.

Propagation of the Masternode List

New clients entering the LKSCOIN network must be made aware of the currently active masternodes on the network to be able to utilize their services. As soon as they join the mesh network, a command is sent to their peers asking for the known list of masternodes. A cache object is used for clients to record masternodes and their current status, so when clients restart they will simply load this file rather than asking for the full list of masternodes.

Payments via Mining and Enforcement

To ensure that each masternode is paid its fair share of the block reward, the network must enforce that blocks pay the correct masternode. If a miner is non-compliant their blocks must be rejected by the network, otherwise cheating will be incentivized.

Our LKSCOIN network uses a strategy where masternodes form quorums, select a winning masternode and broadcast their message. After N messages have been broadcast to select the same target payee, a consensus will be formed and that block in question will be required to pay that masternode.

When mining on the network, pool software (websites that merge the efforts of individual miners) use the RPC API interface to get information about how to make a block. To pay the masternodes, this interface must be extended by adding a secondary payee to GetBlockTemplate. Pools then propagate their successfully mined blocks, with a split payment between themselves and a masternode.

LKSCOIN Network Block Rewards

When LKS foundation was deciding on the rewards for the mined blocks, our utmost concern was to try to limit the deflation of value of LKSCOIN token in the first few years of token existence. More on that below.

- Total number of LKSCOIN tokens: **4.081.632.600 LKS**
- Total number of mined LKSCOIN tokens today: **∽ 2.000.000.000 LKS**

- From block 1 to block 40 (40 blocks in total), the payment reward is **50.000.000 LKSCOIN/block**; total mineable tokens in this phase: **2.000.000.000 LKSCOIN**
- From block 41 to block 8.040 (8000 blocks in total), the payment reward is **10.000 LKSCOIN/block**; total mineable tokens in this phase: **80.000.000 LKSCOIN**
- From block 8.041 to block 44.319 (36.280 blocks in total), the payment reward is **45 LKSCOIN/block**; total mineable tokens in this phase: **1.632.000 LKSCOIN** - *because we want to prevent deflation of value in the first 6-10 months of LKSCOIN token existence, and because of the low mining difficulty, we have decided on the reward of 45 LKSCOIN tokens*
- From block 44.320 and on (3.500.740 blocks in total), the payment reward is **500 LKSCOIN/block** (excluding 740 PowerBlocks*); total mineable tokens in this phase: **1.750.000.000 LKSCOIN** from standard blocks and **250.000.000 LKSCOIN** from PowerBlocks.

**As mentioned in chapter 3.1. PowerBlock will pay out every 4.670 blocks (roughly every 8 days) and will reward from 100.000 to 1.000.000 LKSCOIN*

PowerBlock Size of the Rewards and Rewarding Block Numbers (in the table below you can find the block number before the PowerBlock)

Reward	Block n.	Block n.	Block n.	Block n.	Block n.	Block n.	Block n.	Block n.	Block n.	Block n.
100000	48989	399062	749135	1099208	1449281	1799354	2149427	2499500	2849573	3199646
100000	53659	403732	753805	1103878	1453951	1804024	2154097	2504170	2854243	3204316
200000	58329	408402	758475	1108548	1458621	1808694	2158767	2508840	2858913	3208986
100000	62999	413072	763145	1113218	1463291	1813364	2163437	2513510	2863583	3213656
100000	67669	417742	767815	1117888	1467961	1818034	2168107	2518180	2868253	3218326
200000	72339	422412	772485	1122558	1472631	1822704	2172777	2522850	2872923	3222996
100000	77009	427082	777155	1127228	1477301	1827374	2177447	2527520	2877593	3227666
100000	81679	431752	781825	1131898	1481971	1832044	2182117	2532190	2882263	3232336
200000	86349	436422	786495	1136568	1486641	1836714	2186787	2536860	2886933	3237006
100000	91019	441092	791165	1141238	1491311	1841384	2191457	2541530	2891603	3241676
1000000	95689	445762	795835	1145908	1495981	1846054	2196127	2546200	2896273	3246346
200000	100359	450432	800505	1150578	1500651	1850724	2200797	2550870	2900943	3251016
100000	105029	455102	805175	1155248	1505321	1855394	2205467	2555540	2905613	3255686
100000	109699	459772	809845	1159918	1509991	1860064	2210137	2560210	2910283	3260356
200000	114369	464442	814515	1164588	1514661	1864734	2214807	2564880	2914953	3265026
100000	119039	469112	819185	1169258	1519331	1869404	2219477	2569550	2919623	3269696
400000	123709	473782	823855	1173928	1524001	1874074	2224147	2574220	2924293	3274366
100000	128379	478452	828525	1178598	1528671	1878744	2228817	2578890	2928963	3279036
600000	133049	483122	833195	1183268	1533341	1883414	2233487	2583560	2933633	3283706

200000	137719	487792	837865	1187938	1538011	1888084	2238157	2588230	2938303	3288376
800000	142389	492462	842535	1192608	1542681	1892754	2242827	2592900	2942973	3293046
400000	147059	497132	847205	1197278	1547351	1897424	2247497	2597570	2947643	3297716
200000	151729	501802	851875	1201948	1552021	1902094	2252167	2602240	2952313	3302386
100000	156399	506472	856545	1206618	1556691	1906764	2256837	2606910	2956983	3307056
100000	161069	511142	861215	1211288	1561361	1911434	2261507	2611580	2961653	3311726
200000	165739	515812	865885	1215958	1566031	1916104	2266177	2616250	2966323	3316396
400000	170409	520482	870555	1220628	1570701	1920774	2270847	2620920	2970993	3321066
600000	175079	525152	875225	1225298	1575371	1925444	2275517	2625590	2975663	3325736
200000	179749	529822	879895	1229968	1580041	1930114	2280187	2630260	2980333	3330406
100000	184419	534492	884565	1234638	1584711	1934784	2284857	2634930	2985003	3335076
200000	189089	539162	889235	1239308	1589381	1939454	2289527	2639600	2989673	3339746
800000	193759	543832	893905	1243978	1594051	1944124	2294197	2644270	2994343	3344416
1000000	198429	548502	898575	1248648	1598721	1948794	2298867	2648940	2999013	3349086
400000	203099	553172	903245	1253318	1603391	1953464	2303537	2653610	3003683	3353756
200000	207769	557842	907915	1257988	1608061	1958134	2308207	2658280	3008353	3358426
200000	212439	562512	912585	1262658	1612731	1962804	2312877	2662950	3013023	3363096
600000	217109	567182	917255	1267328	1617401	1967474	2317547	2667620	3017693	3367766
200000	221779	571852	921925	1271998	1622071	1972144	2322217	2672290	3022363	3372436
400000	226449	576522	926595	1276668	1626741	1976814	2326887	2676960	3027033	3377106
100000	231119	581192	931265	1281338	1631411	1981484	2331557	2681630	3031703	3381776
200000	235789	585862	935935	1286008	1636081	1986154	2336227	2686300	3036373	3386446
100000	240459	590532	940605	1290678	1640751	1990824	2340897	2690970	3041043	3391116
400000	245129	595202	945275	1295348	1645421	1995494	2345567	2695640	3045713	3395786
800000	249799	599872	949945	1300018	1650091	2000164	2350237	2700310	3050383	3400456

200000	254469	604542	954615	1304688	1654761	2004834	2354907	2704980	3055053	3405126
600000	259139	609212	959285	1309358	1659431	2009504	2359577	2709650	3059723	3409796
200000	263809	613882	963955	1314028	1664101	2014174	2364247	2714320	3064393	3414466
1000000	268479	618552	968625	1318698	1668771	2018844	2368917	2718990	3069063	3419136
400000	273149	623222	973295	1323368	1673441	2023514	2373587	2723660	3073733	3423806
200000	277819	627892	977965	1328038	1678111	2028184	2378257	2728330	3078403	3428476
600000	282489	632562	982635	1332708	1682781	2032854	2382927	2733000	3083073	3433146
100000	287159	637232	987305	1337378	1687451	2037524	2387597	2737670	3087743	3437816
200000	291829	641902	991975	1342048	1692121	2042194	2392267	2742340	3092413	3442486
400000	296499	646572	996645	1346718	1696791	2046864	2396937	2747010	3097083	3447156
600000	301169	651242	1001315	1351388	1701461	2051534	2401607	2751680	3101753	3451826
800000	305839	655912	1005985	1356058	1706131	2056204	2406277	2756350	3106423	3456496
100000	310509	660582	1010655	1360728	1710801	2060874	2410947	2761020	3111093	3461166
100000	315179	665252	1015325	1365398	1715471	2065544	2415617	2765690	3115763	3465836
400000	319849	669922	1019995	1370068	1720141	2070214	2420287	2770360	3120433	3470506
100000	324519	674592	1024665	1374738	1724811	2074884	2424957	2775030	3125103	3475176
100000	329189	679262	1029335	1379408	1729481	2079554	2429627	2779700	3129773	3479846
100000	333859	683932	1034005	1384078	1734151	2084224	2434297	2784370	3134443	3484516
1000000	338529	688602	1038675	1388748	1738821	2088894	2438967	2789040	3139113	3489186
600000	343199	693272	1043345	1393418	1743491	2093564	2443637	2793710	3143783	3493856
400000	347869	697942	1048015	1398088	1748161	2098234	2448307	2798380	3148453	3498526
100000	352539	702612	1052685	1402758	1752831	2102904	2452977	2803050	3153123	3503196
100000	357209	707282	1057355	1407428	1757501	2107574	2457647	2807720	3157793	3507866
800000	361879	711952	1062025	1412098	1762171	2112244	2462317	2812390	3162463	3512536
100000	366549	716622	1066695	1416768	1766841	2116914	2466987	2817060	3167133	3517206

200000	371219	721292	1071365	1421438	1771511	2121584	2471657	2821730	3171803	3521876
100000	375889	725962	1076035	1426108	1776181	2126254	2476327	2826400	3176473	3526546
600000	380559	730632	1080705	1430778	1780851	2130924	2480997	2831070	3181143	3531216
800000	385229	735302	1085375	1435448	1785521	2135594	2485667	2835740	3185813	3535886
1000000	389899	739972	1090045	1440118	1790191	2140264	2490337	2840410	3190483	3540556

We want to disclose it straight away, that our changes didn't alter any security or other critical features, that Dash blockchain has to offer. Based on LKSCOIN needs, we only changed/improved these three things:

A. **we have hidden PrivateSend feature**,
B. **we added a PowerBlock functionality**,
C. **we redistributed a % of rewards PoW miners and Masternode operators get.**

A. We think that Dash PrivateSend functionality is a service that still needs to improve on. From our point of view, in this state, it will always have one of these two problems. The first problem is, that "Coin mixing" used for anonymisation of transactions is not 100% secure (there are algorithms that can pinpoint the source transaction with tremendous accuracy[1]), and the second problem is, that if the transactions were 100% anonymous, they would be lucrative for money laundering, and we do not want LKSCOIN to be associated with it.

B. Dash blockchain has proposed something similar to PowerBlock functionality and called it a SuperBlock. However, Dash SuperBlocks are not used to incentivize masternodes or miners, but to incentivize network upgrade proposals, as the rewards are paid out only to the approved proposals.
At the LKS Foundation we wanted to think a step forward. It was proven through

[1] "Dash's privateSend isn't very private... : Monero - Reddit." 3 May. 2019, https://www.reddit.com/r/Monero/comments/bk6u61/dashs_privatesend_isnt_very_private/.

time, that blockchain networks that got truly decentralised and received massive adoption, with time also received true blockchain fans. These fans are eager for the network to thrive and they propose blockchain improvements with or without rewards.

At LKS Foundation we think that the most critical aspect of a successful network, a significant node number and large user base, are not considered in Dash SuperBlock strategy.

LKS Foundation has decided to implement PowerBlocks, which reward the PoW miners and Masternode operators, and thus incentivise new users to join the network, purchase new masternodes, and make the network stronger.

Below is the outline of the difference between Dash SuperBlock and LKSCOIN PowerBlock.

Dash Superblock & LKSCOIN Superblock:

(Occurs each **16616** blocks, or roughly every **30** days. Payment of proposal owners to predesignated payment addresses.)

LKSCOIN PowerBlock:

(Occurs each **4670** blocks, or roughly every **8** days. Payment: 20% to PoW miners, 80% to Masternode operators until block 614820, after this block the 10% of the reward starts for the LKS Project Treasury (future improvements) so the percent for PoW miners becomes 18% and for masternodes 72%).

C. We want LKSCOIN to be truly decentralized and we want LKSCOIN users to have a voice when it comes to voting for blockchain changes and improvements. We married the idea of masternodes who have voting ability Dash proposed, but we thought the percentages of rewards Dash uses for rewarding miners and masternodes is not incentivising enough for the blockchain to have a tendency to organically gravitate towards a more decentralised network.

Dash reward percentages:

(45% for PoW miners, 45% for masternode operators, 10% for the Dash Project Treasury DAO future improvements)

LKSCOIN reward percentages:

(20% for PoW miners, 80% for masternode operators until block 614820, after this block the 10% of the reward starts for the LKS Project Treasury (future improvements) so the percent for PoW miners becomes 18% and for masternodes 72%)

By lowering rewards for PoW miners to 18%, the miners work in loss, and there is an incentive to purchase and operate more masternodes. Purchasing more masternodes helps the network to be more equally distributed, more decentralised, harder and harder to attack with a 51% attack, and more green (PoW mining consumes a lot of electrical energy).