Pyrk: Privacy where everyone can participate.

Whitepaper revision 2.0

David Owen Morris and Michael Osullivan

david@pyrk.org mike@pyrk.org

Abstract: A cryptocurrency based on Bitcoin, with additional features uniquely combined from Dash, Digibyte, Trezarcoin and the coloured coins protocol. Features include quintuple algorithmic Proof of Work with Multishield difficulty adjustment, Masternodes, Chainlocks, a Community Dao, and a flexible multifunctional asset layer.

1 Introduction:

Pryk is a privacy centric yet unique cryptographic currency based mainly on the works of the Bitcoin, Dash and Digibyte developers. In this paper we will explore how combining features from these and other projects blend to combine and form a privacy driven yet highly versatile and resilient blockchain ecosystem capable of a lot more than most blockchains. Pyrk's privacy features do not revolve around its transactions but rather the implementation of some of its additional features.

These features come into play in the form of a decentralized uncensorable messenger facilitating free and unhindered client to client communication in an exceptionally secure manner. This is becoming more and more relevant by the day if you follow the censorship debates currently raging on social media.

Additionally, Pyrk's tokens being interactive open up whole new dimensions of usage such as, participating in voting, signing contracts as well as multiple other potentially censored activities that the Pyrk team feel great pride and joy in facilitating. We are now in as a potential tech provider for a rather hotly contested referendum so the clock is ticking on uncensorable yet immutable token transations!

2 Quintuple Proof of work:

Many cryptocurrencies use a single algorithm Proof-of-Work mechanism/algorithm. This can lead to 51% of consensus attacks being viable in currencies which have not achieved sufficient mass mining adoption. Pyrk has a two-pronged approach to addressing this issue. One based on its over all proof of work mechanism the other based on its network supporting masternodes.

Since PoW is still the least contentious consensus mechanism, we propose to take a multiple algorithm approach strengthening all its aspects.

Instead of trying to use algorithms which are ASIC resistant, we are using algorithms which have had ASIC miners for quite some time. These are: SHA256, Scrypt, and X11. To supplement these, we have YesPower and Lyra2z330 for CPU/GPU mining opening the field for wider participation.

There are miners in wide use for all of these, so the distribution of mining should be reasonably fair and even. Furthermore, the use of five different algorithms results in a far less chance of any single person gaining a majority hash rate share.

Lastly, we are using Digibyte's Multishield difficulty adjustment algorithm to prevent difficulty spike issues resulting from burst mining. This has proven to be less effective than desired with multipool mining and we have added the 5th algorithm lyra2z330 for enhanced stability and have plans for a hardened difficulty framework locking the output of each algorithm to 20% of the blocks over a certain average.

2.1 The Future of Pyrk's Proof of Work

Being a community driven project and wanting that ethos to come through in all aspects of the project we do have one additional proof of work had fork planned for later in the year where we remove the scrypt and x11 and replace them with ProgPow and RandomX. We are doing this for the simple reason that we are currently testing a new method for adjusting difficulty which will facilitate a smoother flow of blocks multipool mining regardless.

We are planning this to A) provide a significantly improved UX for the end user with a smooth stream of blocks to work with and B) for mining to be as inclusive as possible. We feel that as much inclusiveness as possible is about as inline as it is possible to get with Satoshi's original vision on "One Cpu one Vote!"

Once complete we will have:

1) Sha for ASIC miners.

2) Progpow variant for modern GPU & FPGA miners.

3) RandomX for modern CPUminers

4) Yespower for older CPU miners.

5) Lyra2z3330 for older GPUs/CPUs

3 Masternode Network

Full nodes are important to the health of any blockchain network. They provide clients the ability to synchronize blocks and ensure the quick propagation of messages throughout the network.

The Masternode network has high availability and provide required services to the network earning them a share in block rewards (the coins issued with each produced block).

Masternodes on the Pyrk network are written to a deterministic on chain list so none of the payment variance possible on the separate list system can occur on the Pyrk network.

3.1 Masternode Reward Program - Cost and Payments

One of the reason for fewer full nodes on the Bitcoin network is that there is no incentive for running such despite the obvious benefits they provide to the network. However, incentivising a node for merely running to some extent goes against the ethos of proof of work blockchains. Dash innovatively added the Proof of Service requirements for masternodes which Pyrk with its current update has expanded somewhat on.

Masternodes on the Pyrk network receive 30% of block rewards (see appended table) for providing 51% attack protection aka chainlocks as well being available for mobile SPV wallets to synch with and on top of that providing routing for the Pyrk messenger.

To ensure honest masternodes on the network running one requires a collateral of 2500 soon to be 5000 Pyrk locked in an on chain address and registered on the deterministic list. This collateral is never at risk but is rather an insurance policy to help ensure that the masternode has the best interests of the chain at heart.

In addition to the collateral requirement, the masternodes all participate in distributed key generation sessions that are used for determining if a masternode is ready and available on the network. Should they not be, a ban score will be imposed on them and they will require reactivation once they get past a certain threshold.

3.2 LLMNQs - Long Lived MasterNode Quorums

An LLMNQ defines a Long Living Masternode Quorums (LLMQ). A LLMQ is a deterministic subset of the global deterministic masternode list. Or to put it in layman’s terms a subset of an ordered list.

A quorum is formed with the help of a distributed key generation (DKG) protocol and is supposed to be active for a long time (e.g. days). Multiple quorums are kept alive at the same time, allowing load balancing between these quorums, as well as having multiple functions implemented via the quorums.

The main task of a LLMQ is to perform threshold signing of consensus related messages meaning signing individual blocks onto the chain as well as performing functions such as chainlocking transactions facilitating both Dashstyle privatesend and instasend.

Quorums are set up in the following order:

1. Initialization
2. Contribution
3. Complaining
4. Justification
5. Commitment
6. Finalization
7. Mining/Working

1) What happens during the first stages is nodes are selected for quorum participation. This selection depends on their participation in other quorums and placement on the overall deterministic list vs other potential participants.

2) This next step is where the quorum sets up its own capabilities through a distributed key generation session. During such a session, each node creates and shares a contribution towards a whole key with the remainder of the quorum. For smaller lower security quorums, this is a very quick and easy task. Whereas for larger more complex quorums, it is a complicated task that may take up to an hour or more.
   Particularly since a multitude of factors are verified during the process quorumHash, proTxHash, quorumThreshold, and duplicates.

3) During the preceding contribution phase, the quorum tracks any malformed signatures and messages quorumHash, proTxHash, quorumThreshold, bitvectors, and duplicates may all be complained about to the rest of the quorum. The logic cycle for it is complex to say the least but there is a strong emphasis on fairness throughout given that there may be problems with networking hardware in multiple places even across a well developed net.

4) In this phase, each member that was previously complained about must justify for a valid contribution. Justification is only allowed for members who sent a contribution and is not allowed for members previously marked as bad. Justification means that a member has to reveal the secret key contribution that it had initially encrypted and sent to the complainer.
   This way all other members can verify if the secret key contribution is valid. If the secret key contribution is invalid, the justifier is immediately marked as

bad. If the secret key contribution is valid, the complained state for the specific complainer is removed from the justifier.

5) During the commitment-phase, all members collect all contributions (keys) from all members not marked as bad. The members then build the final quorum verification vector (joint key) from the individual verification vectors of the members.
   The members also create their own threshold secret key (the n of m keys from bls signatures) share from the secret key contributions received by all valid members.

6) As the name implies, during this stage, all the previously mentioned steps are combined into a whole and broadcast to all full nodes on the network.
   This is so pools can verify blocks have been signed, as well as solominers (yes, there are a few) being able to do the same as well.

7) This phase is initiated by the successful broadcast of a special transaction which is called a “quorum commitment” once this has been completed, the quorum will activate and take on its assigned function depending on the type of quorum.
   There are special rules to ensure that this special transaction has to be incorporated into the next mined block and the network will orphan blocks mined without adding such a broadcast transaction.

As you can see, this is a long and complicated process which involves a multitude of steps including many, which have been somewhat glossed over in the description above.

This complex yes cryptographically secure process provides Pyrk’s blockchain with exceptional capabilities well beyond those of conventional blockchains.

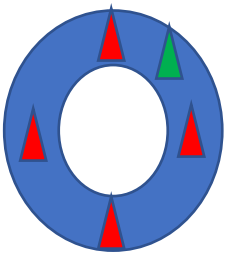
3.3 Possible future usage for Pyrk's Masternode network and LLMNQs.

Exploring a potential additional applications of this tech, namely control of a Dex wallet for trustless peer to peer trading, the process would work something like this:

A Dex wallet accepts coins for trading against another coin where some type of oracle service has been established.

1) From the main list of MN a quorum of 500 is selected. This quorum controls the main Dex wallet which functions a as "holding" addresses.

2) These 500 form a main quorum with 4 smaller listening quorums of 50 nodes each.



3) So, when BTC or ETH is sent to the payment addresses included when depositing into a holding address, a signal is sent to the 4 listening quorums. (This can be from a ChainLink oracle or distributed api endpoints)

4) The 4 listening quorums vote on the validity of the signalled data, if they all agree, data is forwarded to the main quorum for additional verification.

5) Should the request for a pay out pass the full quorum validation, a "sending" quorum of 10 nodes is assigned to construct a transaction (possibly coinbase) sending the held amount of Pyrk to the requested address.

6) The joint quorum sings the transaction to chain issuing the desired address X coins and at the same time adjusting the tally of held coins.

The exact methodologies and implementations for such a process still need some additional investigation and exploration by the Pyrk developers. However, the main substance is possible thanks to this implementation of quorum technology. Facilitating decentralized and trustless transactions for Pyrk holders.

The entire crypto space owes a debt to thanks to the DASH developers who pioneered and facilitated this two-layer approach,

4 Additional Improvements:

A different approach to restricting the inflation of mining is taken in Pyrk, using a reduction in supply every 100,000 blocks. Only the first halving is a 50% reduction (at block 100), future reductions are half of the previous reduction until block 500,000 where the block reductions reach 3.75%. The maximum supply is approximately 100,000,000

Block Start	Block End	Block Reward	Total Period Reward	Total Circulation	Days Since Genesis	End Date	Blocks	Reduction
1	100000	100.00000000	10000000.00000000	10000000.00000000	104	Aug 12, 2020	100000	1.00000000
100001	200000	50.00000000	5000000.00000000	15000000.00000000	208	Nov 12, 2020	100000	0.50000000
200001	300000	37.50000000	3750000.00000000	18750000.00000000	313	Mar 12, 2021	100000	0.25000000
300001	400000	32.81250000	3281250.00000000	22031250.00000000	417	Jun 12, 2021	100000	0.12500000
400001	500000	30.76171875	3076171.87500000	25107421.87500000	521	Oct 12, 2021	100000	0.06250000
500001	600000	29.60815430	2960815.42968750	28068237.30468750	625	Jan 12, 2022	100000	0.03750000
600001	700000	28.49784851	2849784.85107422	30918022.15576170	729	Apr 12, 2022	100000	0.03750000
700001	800000	27.42917919	2742917.91915894	33660940.07492060	833	Aug 12, 2022	100000	0.03750000
800001	900000	26.40058497	2640058.49719048	36300998.57211110	938	Nov 12, 2022	100000	0.03750000
900001	1000000	25.41056304	2541056.30354584	38842054.87565690	1042	Mar 12, 2023	100000	0.03750000
1000001	1100000	24.45766692	2445766.69216287	41287821.56781980	1146	Jun 12, 2023	100000	0.03750000
1100001	1200000	23.54050441	2354050.44120676	43641872.00902660	1250	Oct 12, 2023	100000	0.03750000
1200001	1300000	22.65773550	2265773.54966151	45907645.55868810	1354	Jan 12, 2024	100000	0.03750000
1300001	1400000	21.80807042	2180807.04154920	48088452.60023730	1458	Apr 12, 2024	100000	0.03750000
1400001	1500000	20.99026777	2099026.77749111	50187479.37772840	1563	Aug 12, 2024	100000	0.03750000
1500001	1600000	20.20313273	2020313.27333519	52207792.65106360	1667	Nov 12, 2024	100000	0.03750000
1600001	1700000	19.44551526	1944551.52558512	54152344.17664870	1771	Mar 12, 2025	100000	0.03750000
1700001	1800000	18.71630843	1871630.84337568	56023975.02002440	1875	Jun 12, 2025	100000	0.03750000
1800001	1900000	18.01444687	1801444.68674909	57825419.70677350	1979	Oct 12, 2025	100000	0.03750000
1900001	2000000	17.33890511	1733890.51099600	59559310.21776950	2083	Jan 12, 2026	100000	0.03750000
2000001	2100000	16.68869617	1668869.61683365	61228179.83460320	2188	Apr 12, 2026	100000	0.03750000
2100001	2200000	16.06287006	1606287.00620239	62834466.84080560	2292	Aug 12, 2026	100000	0.03750000
2200001	2300000	15.46051243	1546051.24346980	64380518.08427540	2396	Nov 12, 2026	100000	0.03750000
2300001	2400000	14.88074322	1488074.32183968	65868592.40611510	2500	Mar 12, 2027	100000	0.03750000
2400001	2500000	14.32271535	1432271.53477069	67300863.94088580	2604	Jun 12, 2027	100000	0.03750000
2500001	2600000	13.78561352	1378561.35221679	68679425.29310260	2708	Oct 12, 2027	100000	0.03750000
2600001	2700000	13.26865302	1326865.30150866	70006290.59461130	2813	Jan 12, 2028	100000	0.03750000
2700001	2800000	12.77107853	1277107.85270209	71283398.44731340	2917	Apr 12, 2028	100000	0.03750000
2800001	2900000	12.29216308	1229216.30822576	72512614.75553920	3021	Aug 12, 2028	100000	0.03750000
2900001	3000000	11.83120697	1183120.69666729	73695735.45220650	3125	Nov 12, 2028	100000	0.03750000
3000001	3100000	11.38753671	1138753.67054227	74834489.12274880	3229	Mar 12, 2029	100000	0.03750000
3100001	3200000	10.96050408	1096050.40789693	75930539.53064570	3333	Jun 12, 2029	100000	0.03750000
3200001	3300000	10.54948518	1054948.51760080	76985488.04824650	3438	Oct 12, 2029	100000	0.03750000
3300001	3400000	10.15387948	1015387.94819077	78000875.99643730	3542	Jan 12, 2030	100000	0.03750000
3400001	3500000	9.77310900	977310.90013362	78978186.89657090	3646	Apr 12, 2030	100000	0.03750000
3500001	3600000	9.40661741	940661.74137861	79918848.63794950	3750	Aug 12, 2030	100000	0.03750000
3600001	3700000	9.05386926	905386.92607691	80824235.56402640	3854	Nov 12, 2030	100000	0.03750000

Due to the halving nature, total supply becomes logarithmic, having a maximum total supply of approximately 100 Million Pyrk. Approximately 50% of the maximum supply will be mined in the first 4 years.

5 Pyrk Tokens

Pyrk Tokens are a simple token system for creating tokenized assets on the blockchain.

This is similar to the SLP (Simple Ledger Protocol) used by Bitcoin Cash and based looselyon the Colored Coins protocol.

You can read more about Pyrk Tokens in the specification draft at: https://www.pyrk.org/Pyrk_Tokens.pdf

Pyrk Tokens are far easier and cheaper to create and maintain than ERC-20 tokens.

Token Methods:

GENESIS

Easily create a token by specifying the Ticker, Name, and Quantity to generate

SEND

Send an amount of tokens to another Pyrk address

BURN

The contract owner can burn tokens (as long as he holds the amount needed for the burn)

ADDMETA

Add additional metadata to the Token. It can be anything, and we provide 4 billion

available MetaID codes for your use

AUTHMETA

Authorize another Pyrk address to add metadata to your token

REVOKEMETA

De-authorize another Pyrk address from adding metadata to your token

PAUSE

Pause the token and prevent any new transactions from occurring on the network

RESUME

Resume activity on a token after it’s been paused

NEWOWNER

Assign ownership of the token to another Pyrk address

5.1 The road ahead for Pyrk Tokens

With just minor additional adaptations of Pyrk's techstack, this opens up using Pyrk's token layer for different forms of voting, membership registration etc all done securely and privately with your private keys guaranteeing your privacy and the immutability of the data on the Pyrk token layer.

A very real application we are working towards is the development of a secure voting or referendum app running on Pyrk's token layer facilitating the bypassing of censorship for political or economic reasons.

Everyone deserves a real voice that can be heard!