Pyrk: A Multi PoW PrivacyCentric CryptoCurrency

Michael Osullivan mike@pyrk.org

NOTE: SOME OF THE CONTENT OF THIS WHITEPAPER WAS TAKEN FROM DASH AND DGB SOURCES (WHITEPAPER/WIKI). I AM NOT THE ORIGINAL AUTHOR OF SOME OF THIS CONTENT.

Abstract: A cryptocurrency based on Bitcoin, with additional features imported from both Dash and Digibyte. Improvements include triple algorithm Proof of Work with Multishield difficulty adjustment, Masternodes, Private Send, a Community Fund, and a Simple Tokenized asset layer.

1 Introduction

Pyrk is a privacy centric cryptographic currency based on the work of Bitcoin, Dash, and Digibyte. In this paper we propose a series of improvements to these three well known cryptocurrencies resulting in a single currency with all of the best features of its predecessors. Pyrk is officially a fork of Dash v0.12.3.4 with Multi-Algorithm mining and Multishield difficulty adjustment taken from Digibyte. Much of the contents of this white paper are taken directly from the original Dash white paper (https://whitepaperdatabase.com/dash-whitepaper/) with additional information added as necessary.

2 Triple Algorithm Proof-of-Work

Many of todays cryptocurrencies use a single algorithm Proof-of-Work mechanism. This can lead to 51% attack avenues on currencies which haven't yet achieved a significant mass mining adoption. Since PoW is still the preferred mining consensus mechanism, we propose to take a multiple algorithm approach. Instead of trying to use algorithms which are ASIC resistant, we propose to use algorithms which have had ASIC miners for quite some time. These are: SHA256, Scrypt, and X11. Since these miners are already in wide use, the distribution of mining should be fair and even. Furthermore, the use of three different algorithms results in a far less chance of any single person gaining a majority hash rate share. Lastly, we use the Multishield difficulty adjustment algorithm to prevent difficulty spike issues resulting from burst mining.

2.1 Triple algorithm proof-of-work

The idea of multi-algorithm originated in Digibyte. Splitting the mining into three different algorithms effectively splits the amount of work performed by each algorithm to 33% of the total network hashrate. This means that any pool or miner mining can only achieve 33% of the total hashrate even if they are mining 100% of the hash rate of a single algorithm. It is an exceedingly unlikely case that a single miner attains 100% of the hash rate of a single algorithm, especially as the number of miners and pool grows with the network. The triple algorithm approach helps to further protect the network from bad actors while also providing the preferred Proof-of-Work mechanism.

2.2 Multishield

Multishield was originally developed by Digibyte. In order to maintain an "average" block timing, blockchains such as Bitcoin, Litecoin and Pyrk all use different methods of "difficulty retargeting". The idea being that as there is more hash-power provided by the miners it needs to become harder and harder to find the blocks.

Pyrk has a 90-second block timing target, meaning mathematically based on the previous blocks the "difficulty" in finding the cryptographic answer for each block will become harder or easier in order to maintain an approximate 90-second block timing.

Miners sometimes change between the blockchains that they mine, especially on smaller chaiins, in order to maximize profits. The original Bitcoin adjusts difficulty every 2016 blocks. However, for chains that have sporadic mining bursts this can cause long periods of extremely high difficulty, which results in exceedingly long block times.

MultiShield adjusts after each block, rather than once every 2016 blocks. MultiShield is designed to let the difficulty "fall" very fast, in order that the chain doesn't freeze.

MultiShield was originally created to account for such wild fluctuations, so that the blockchain doesn't "freeze" when a large exodus of hash power occurs. It also means miners cannot flood a few consecutive blocks with a high amount of hash power and benefit from low difficulty, giving blocks near instantly one after another before traditional difficulty retargeting occurs.

3 Masternode Network

Full nodes are very important to the health of the network. They provide clients with the ability to synchronize and quick propagation of messages throughout the network. The Masternode network has high availability and provide a required level of service to the network in order to take part in the Masternode Reward Program.

3.1 Masternode Reward Program - Cost and Payments

Much of the reason for the decrease of full nodes on the Bitcoin network, is the lack of incentive to run one. Over time the cost of running a full node increases as the network gets used more, creating more bandwidth and costing the operator more money. If there is no benefit to an operator to run a full node all the time, it is likely they will not.

Masternodes are full nodes except they must provide a level of service to the network and have a bond of collateral to participate. Collateral is never forfeit and is safe while the Masternode is operating. Collateral becomes available to the user again when the node is turned off. This allows users to provide a service to the network, while also earning a reward on their collateral investment while also reducing the volatility of the currency.

To run a Masternode, the node must store 1000 PYRK as collateral. When active, nodes provide services to clients on the network and in return are paid in the form of a dividend. This allows the users to pay for the services and earn a return on investment. Masternodes are all paid from generated block rewards. The Masternode rewards start at block 10,000 and the master node network receives 20% of the block reward. At block 100,000, the reward goes up to 30%, however the collateral also goes up at block 100,000 to 2500 PYRK.

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:

NOTE: These forumulas where taken directly from the Dash whitepaper, as we use the same formulas.

$(\boldsymbol{n}/\boldsymbol{t}) * \boldsymbol{r} * \boldsymbol{b} * \boldsymbol{a}$

Where:

n is the number of Masternodes an operator controls
t is the total number of Masternodes
r is the current block reward (100 PYRK at launch)
b is blocks in an average day. For the Pyrk network this usually is 960.
a is the average Masternode payment (30% of the average block amount)

Return on investment for running a Masternode can be calculated as

$((\boldsymbol{n}/\boldsymbol{t}) * \boldsymbol{r} * \boldsymbol{b} * \boldsymbol{a} * 365) / 1000$

Where variables are the same as above.

The cost associated with running a Masternode creates a hard and soft limit of active nodes on the network. The number of possible Masternodes running on the network are in direct relation to the total number of PYRK in circulation. The soft limit is imposed by the price it costs to acquire a node and the limited liquidity on exchanges due to usage of Pyrk as a currency and not merely an investment into a Masternode.

3.2 Deterministic Ordering

A special deterministic algorithm is used to create a pseudorandom 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.

Pseudo Code, for selecting 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 block
    n2 = Hash(n1); //hash the POW hash to increase the entropy
    n3 = abs(n2  masternode_vin);

    return n3;
}
```

3.3 Trustless Quorums

By requiring 1000 PYRK collateral to become an active Masternode, we create a system in which no one can control the entire network of Masternodes. For example, if someone wants to control 50% of the Masternode network, they would either have to buy enough PYRK from the open market or mine it. This would end up raising the price thus would become more difficult to acquire.

With 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.

For an example implementation of a trustless quorum see InstantSend, which uses quorums to approve transactions and lock the inputs or the proof-of-service implementation. (Instant send was originally developed by Dash)

3.4 Roles and Proof-Of-Service

Masternodes can provide any number of extra services to the network. We use them for the PrivateSend and InstantSend services. By utilizing what is called proof-of-service, we can require that these nodes are online, responding and even at the correct block height.

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.

To learn more about how Masternodes work, check out the Dash Whitepaper: https://whitepaperdatabase.com/dash-whitepaper/

4 Privatesend

Originally developed by Dash, Privatesend is an improved and extended version of the CoinJoin protocol, which employs a series of improvements such as decentralization, strong anonymity by using a chaining approach , denominations and passive ahead-of-time mixing.

To read more about how Privatesend works, check out the original Dash white paper: https://whitepaperdatabase.com/dash-whitepaper/

In order to send private transactions, you must first enter a mixing period which can take some time depending on the amount required.   If you intend on using this feature, it is recommended to mix well ahead of time so that they are ready when you need them.

By default, sending transactions on the Pyrk network do not use privatesend.

5 Instant Transactions via InstantSend

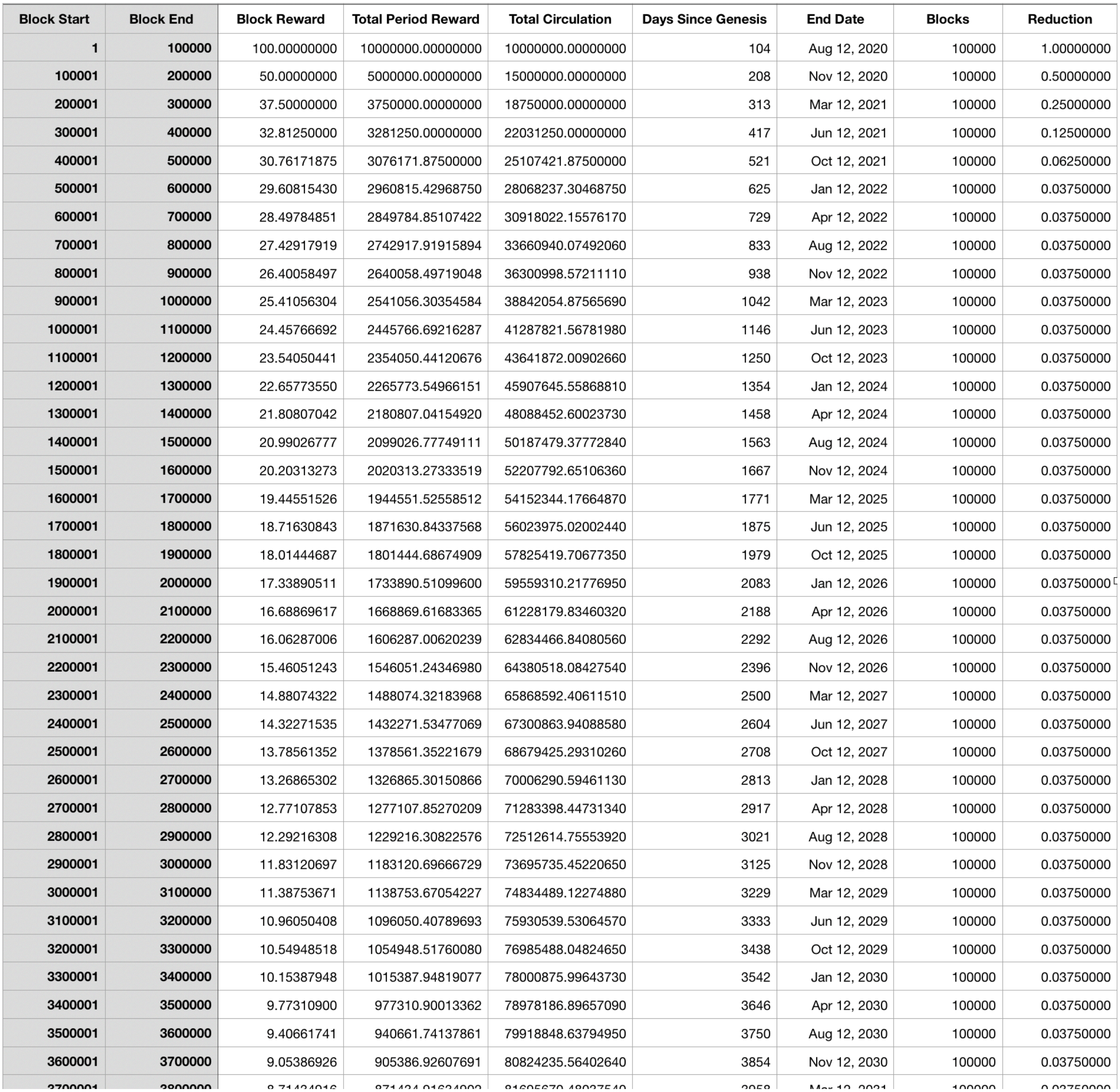
Originally developed by Dash. Instant Transactions utilize Masternode quorums, users are able to send and receive instant irreversible transactions. Once a quorum has been formed, the inputs of the transaction are locked to only be spendable in a specific transaction, a transaction lock takes about 4 seconds to be set currently on the network. If consensus is reached on a lock by the Masternode network, all conflicting transactions or conflicting blocks are rejected thereafter, unless they matched the exact transaction ID of the lock in place. This allows vendors to use mobile devices in place of traditional POS systems for real world commerce and allow users to quickly settle face-to-face non commercial transactions as with traditional cash. This is done without a central authority.

To read more about how Instant Transactions work. check out the Dash whitepaper.

6 Additional Improvements

6.1 Mining Supply and Halvings

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
3700001	3800000	8.71434916	871434.91634902	81695670.48037540	3958	Mar 12, 2031	100000	0.03750000

Figure 6: Mining Reward Schedule

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.

7 Other Improvements

7.1 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 loosely on 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 VS Ethereum ERC-20

Pyrk Tokens are far easier to create and maintain than ERC-20 tokens. 99% of ERC-20 tokens in existence use the same basic features:

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