Yerbas

YERB - The "Good Shit" coin!

WARNING! Yerbas is a work in progress...Use at your own risk!

Yerbas is a community driven, developmental, grassroots, digital currency that enables instant payments to anyone, anywhere in the world. The Yerbas Coin uses peer-to-peer technology to operate with no central authority: managing transactions and issuing money are carried out collectively by the network. Yerbas is a code fork of Bitcoin/Dash/Raptoreum and inherits current and optionally future features such as chain locks, oracles etc. The inspiration for the name Yerbas is derived from the Latin(herba) and Español(hierba) words for herb, grass, or weeds.

We are further expanding capabilities by adding the following features:

A) The deployment of a unique asset layer. ---pushing you luck here, but maybe ;)

B) Collaboration with real world vendors offering rewards and incentives to utilize Yerbas for everyday goods and services.

Problems Yerbas Is Attempting To Solve:

Driving Mass Adoption:
One of the largest issues that Crypto as a whole faces is mass adoption. Yerbas helps to solve this by providing value to users. How we plan to address this: A majority portion of the development fund will be used for rewards and and offers while providing an easy to use reward and payment system benefiting traders, consumers, artists, merchants and industry providers.

FPGA And ASIC Resistance: Yerbas is dedicated to keeping ASICs and FPGAs off the network to increase decentralization and keep it mine-able by everyone without the use of high cost specialized hardware.

As part of our effort to make this happen we have adopted the POW algorithm code named "GhostRider" [3]. GhostRider uses the x16r randomizer combined with CNv1-8, this results in an algorithm that discourages ASIC and FPGA by making it much too expensive for a minimal gain. Additionally, we are developing the ability to adjust the algorithm on the fly. This allows Yerbas to change some algorithmic parameters on a real-time basis that would dump ASICS and FPGA should they be found to be on the network, without requiring the slow, costly and insecure process of forking fully.

Hyperinflation: Masternodes, while a powerful tool, can cause hyperinflation that can cause a coin to crash on the markets and cause irrevocable damage to a project. Yerbas introduces a custom tiered collateral and reward system to prevent this (see Smartnodes).

Smartnodes

Smartnodes play a critical role on the Yerbas network by running Dash-style chainlocks. Yerbas

uses a custom emissions curve with a tiered smartnode collateral and reward system, thus avoiding the hyperinflation that damages many other coins that use Master/Smartnodes.
Hardware:

Yerbas Smartnode collateral increase schedule

Block #	Collateral Amount
4200 - 69420	10,000
69421 - 100420	16,000
100421 - 200420	22,000
200421 - 300420	28,000
300421 - 400420	34,000
> 400421	42,000

Overall smartnode rewards and ROI:
With a fully developed network of 4000-6000 smartnodes at a maximum collateral of 42,000 YERB, annual ROI should be sitting at the 8-12% mark depending on the exact number of nodes on the network and the numbers of asset and futures transactions. This is not an unreasonable level of return given that the cost of setting up and maintaining a node is not substantial.

Block reward emission schedule

Block #	Block reward	Miner Reward	Smartnode reward	Dev reward
0 - 420	4.2	4.2	0	0
421 – 1,000,000	100	75	20	5
1,000,000 - 2,000,000	80	60	16	4
2,000,000 - 3,000,000	70	52.5	14	3.5
3,000,000 - 4,000,000	50	37.5	10	2.5
4,000,000 - 5,000,000	40	30	8	2
5,000,000 - 6,000,000	20	15	4	1
6,000,000 - 7,000,000	10	7.5	2	0.5
7,000,000 - 8,000,000	9	6.75	1.8	0.45
8,000,000 - 9,000,000	8	6	1.6	0.4
9,000,000 - 10,000,000	7	5.25	1.4	0.35
10,000,000 - 11,000,000	6	4.5	1.6	0.3
11,000,000 - 12,000,000	5	3.75	1	0.25

12,000,000 - 13,000,000	4.20	3.15	0.84	0.21
13,000,000 - 14,000,000	3	2.25	0.6	0.15
14,000,000 - 15,000,000	2	1.5	0.4	.1
15,000,000 - 16,000,000	1	0.75	0.2	0.05
> 16,000,000	0.420	0.315	0.084	0.021

GhostRider Mining Algorithm

ByTri Nguyen-PhamI.

Objective: Create an alternative mining algorithm that is highly resistant to asics as well as minimize the effect of fpgas and heighten the entry point cost for fpga mining significantly.

- Technology: GhostRider is a combination of known mining technologies and methodologies from x16r (Raven) and CryptoNight (Monero). X16r provides a randomness to an existing hash chaining methodology for mining, it lacks a memory requirement which means asics can potentially gain significant advantages over gpus. CryptoNight, on other hand has features that require cpu/gpu memory which makes it harder for asics to gain a significant advantage over cpu/gpu, but it lacks the randomness that x16r has. Over the recent year, the Monero team committed to combat asics by forking CryptoNight to add more variables to its memory requirements, as well as hashing methodology. However, each fork's hashing method remains static.

- GhostRider methodology:With the realization of the value that the x16r randomness provides in battling the curve of asic efficiency combined with the impact of a high memory requirement. The concept of GhostRider was born by combining both methodologies together by randomly selecting 15 different core base algorithms and mixing them with 3different random variants of Cryptonight hashing. These algorithms are divided into 3 groups of 5 random order core algorithms followed by 1 random order CN variant. All 15 order core algorithms are random but not no single algorithm being repeated in the same chain. The same goes for the order of CN derivatives.

Random ordering algorithm: To archive pre-deterministic ordering,the algorithm uses previous block hash nibbles in order from right to left to determine what algorithm to hash next for the 15core algos. Each nibble is a single hex digit(0-F) and there are64 nibbles in a block hash. If a nibble hex is F(15 in decimal)then it wraps around as 0. See hex number to algo map below. If a hex digit has seen before in the previous nibbles, it moves to next nibble in the hash. The process is repeated until all 15unique hexes are selected. Similarly, CN variant ordering is determined by hex digit and _modified_.

Hex to algo maping:
0 or F-Blake
1-Bmw
2-Groestl

Contact

Discord: https://discord.gg/XGEp2cKSKF
Telegram: https://t.me/yerbas
Twitter: https://twitter.com/Yerbas_Endeavor

Sources

[1] 2018 51% and double spend attacks:
https://thenextweb.com/hardfork/2018/10/23/cryptocurrency-51-percent-attacks/ [2]
[2]Cost to perform 51% attacks
https://www.crypto51.app/
[3] GhostRider Explained: https://medium.com/@kawwwoin/raptoreums-ghostrider#algorithm-explained-93f1f8070158