The Ritocoin Manifesto

Trevali Hudson
https://www.ritocoin.org
December 2018

Ritocoin is a blockchain software development project designed to experiment with alternative and additional concepts with ideas based on those begun by the Ravencoin project.

Thank you to the founders, developers and community members of Bitcoin and Ravencoin. The Ritocoin project was launched based on the hard work and continuous effort of countless developers across all the vast realms of the cryptocurrency ecosystem. We are eternally grateful to them for their contributions to the science of free software and the open source blockchain community. The Ritocoin project is built above the foundation they have collectively created.

Abstract. Ritocoin launches with the spirit of community, cypherpunk culture and hacker ethics. Ritocoin is a fork of the Ravencoin codebase, which is an experimental blockchain and platform optimized for transferring assets, such as tokens, from one holder to another. The launch of Ritocoin offers several improvements to Ravencoin. First, a change in the proof-of-work mining algorithm, second, a commitment to keeping mining accessible to casual hobbyists, third, a roadmap for masternode functionality to be added, and finally, an emphasis on the community-driven development of user friendly features and add-on utilities. The culture of Ritocoin will be of rapid software development and frequent releases of experimental features.

Ritocoins (RITO) are fairly issued and mined publicly and transparently using Proof of Work (POW) with the X21S algorithm, which was created for this project. The network produces, with the aid of DGW[1], a block on average every 60 seconds which contains 5,000 RITO. For the first 525,600 blocks, which corresponds to approximately 1 year, each block will generate an additional 50 RITO (approximately 1% of the full reward) sent to a fund that will provide funding for community-driven developments and community events. The intention is to distribute these coins to members of the community for development work and other services they provide during the first year of this coin's life. Unless the community consensus dictates otherwise, this development fund will cease approximately a year after Ritocoin's launch.

Ritocoin is intended to be a bazaar[2] of ideas prioritizing security, user control, privacy, censorship resistance, and fair distribution of hashrate to all members of the cryptocurrency community. It is open to use and develop in any jurisdiction, providing users simple additional features based on need.

0. The Ritocoin Vision

> "*Hacking refers to the spirit of fun in which we were developing software. The hacker ethic refers to ... the ethical ideas ... that knowledge should be shared with other people who can benefit from it...*" -- Richard Stallman, 1996
>
> "*It is hard to write a simple definition of something as varied as hacking, but I think what these activities have in common is playfulness, cleverness, and exploration. Thus, hacking means exploring the limits of what is possible, in a spirit of playful cleverness.*" -- Richard Stallman, 2002
>
> "*I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu)*" -- Linus Torvalds, 1991

People have a desire to contribute to the greater good of a community into which they have been welcomed and accepted. Hackers want to make software that others want to use. Enthusiasts want to promote and market a project. Writers want to help by creating documentation, FAQs and tutorials on wiki-style websites. Artists want to see their artwork used and enjoyed. People with winning personalities want to help moderate online forums centered around the project. The communities that build up around free software projects such as Linux, GNU, Bitcoin and others, are meritocracies where the individuals are celebrated solely on the merit of their achievements. Hackers contribute ideas and collaborate with each other to improve on the work they are all doing, and thereby produce unexpected and sometimes amazing results.

Ritocoin's vision focuses on creating and cultivating an environment into which individuals can pour their energies, and out of which innovative ideas can be realized.

1. The Starting Goals for Ritocoin

Culture

We will cultivate and promote a community that builds a cypherpunk culture centered around free software development with hacker ethics. Ritocoin has no corporate backing, and is 100% driven by a community of individuals. The developer fund will prime the pump for ongoing software development by the community during the first year. The core team will lead development, recruit coders, review work and produce guidance and leadership.

Hobbyist Mining

We give a firm commitment to maintaining the accessibility of mining Ritocoin for hobbyists. Ritocoin is a GPU mineable coin because that's what hobbyists have in their home and workplace. To that end, no ASIC will mine Ritocoin, and FPGAs will be resisted. We created the X21S algorithm to get ahead of FPGAs and we will continue to develop our hashing algorithm and will fork the chain to ever more complex and difficult algorithms as time goes on. NiceHash and any similar hash renting services will be resisted in the same way.

Masternodes

Masternodes give miners fun and interesting goals to mine toward, as they work to build a holding sufficient to stake their own masternode. Many miners enjoy working together to pool their mined coins to create cooperatively managed masternodes. Sub-communities gather around these shared masternodes enhancing the experience for everyone involved. Ritocoin recognizes and appreciates the interesting features that other coins have added to their blockchain. We intend to explore the feasibility of incorporating these features into our blockchain. Instant transactions, in particular, is an innovation that masternodes can bring to a network. Privacy features are a second key feature we will investigate. Masternodes also give new and interesting ways for hobbyists to become more intimately involved with a coin project. Finally, permitting voting on important community matters is an attractive governance model that masternodes can help solve.

Through early 2019, we will be conducting open conversations about this topic with the Ritocoin community of miners and holders, and we will collaboratively design and implement a masternode system for Ritocoin. Masternodes will be available to anyone who owns enough RITO. The only way to obtain a masternode will be to mine RITO or obtain the coins from other RITO holders.

Track Ravencoin developments and incorporate their future additions

The asset layer has already been launched by Ravencoin, and has been added to Ritocoin. It will activate on the Ritocoin blockchain at block height 50,000. Future additions, such as asset reward distribution, unique assets, messaging and voting, will all be added to Ritocoin as they become available in the Ravencoin codebase. We want to explore innovative and different ways to enhance our blockchain to put these features to new uses, experimenting with new utilities that take these features to new and surprising places.

Collaborate with the larger cryptocurrency ecosystem

We do not see other cryptocurrency projects as competitors. Our default position is one of cooperation and collaboration with all free software projects. We want to track developments across the entire sector incorporating the best ideas, and contributing back the best ideas of our own. There have already been initial discussions with the developers of other coin projects centered around developments that can provide additional security to both chains. We enthusiastically embrace all such conversations.

2. The Rito want to have fun

Some members of the Ravencoin and blockchain communities are thirsty for new horizons to cross and new worlds to explore. As Ravencoin continues maturing through its inexorable march toward blockchain supremacy, the cypherpunks among us wish to remain in hacker space and have fun with a coin that we can easily mine without worrying about FPGA, ASIC and NiceHash coming in and taking away our fun. We want to mine our coin, write new wallets, create new explorers, and make interesting utilities that do unusual and surprising things with the blockchain. We want to mine coins and then spend those coins freely amongst ourselves and to the burn addresses where we will make assets for pleasure and for business. Ritocoin is a playground for programmers and the coins are not intended to be hoarded as money, but held and used as tools.

3. We want to mine our coin

We are on the brink of entering a post-GPU era of cryptocurrency mining, and those of us who own farms of rigs wish to continue to see our hardware continue to be put to use. This desire is, in fact, the primary reason many of us joined the Ravencoin ranks in the first place. The X16R algorithm on which Ravencoin was founded was designed specifically for ASIC resistance.[3] While we applaud Ravencoin's commitment to resist ASIC domination of their chain, we are sorry that they have adopted the decision to allow FPGAs to mine their coin. Until the day comes that FPGAs are commonplace in homes across the world, Ritocoin is committed to ensuring that GPUs will always have a fair and even chance to mine the blocks in this chain.

Additionally, centralized hash renting services such as NiceHash have a similarly chilling effect on miners. At the time of this writing, about 33% of the network hash for X16R is coming through NiceHash. For the sake of the security of the network and for the other reasons we mentioned above, we desire for our coin's network to remain inaccessible to services like NiceHash. We do recognize that these kinds of services can easily add new algorithms to their offerings, but we remain committed to staying ahead of that cat and mouse game. We are willing to make periodic hard forks to new algorithms in order to keep our chain safe and minable by our GPUs.

4. The X21S Algorithm

The cornerstone feature of our coin at launch is the new X21S algorithm. To make X21S we started with the X22i algorithm, developed by SUQA.[4] X22i has 22 chained algorithms that are processed sequentially. In X21S, however, the first 16 algorithms are shuffled and hashed in the order prescribed by X16S[5], followed by 5 additional hashing algorithms: haval256, tiger, lyra2, gost512, and sha256. The inclusion of lyra2[6] brings numerous advantages, making parallelization of the algorithm practically impossible, with each step relying on the previous step having already been computed. It is a "friendly" algorithm that makes GPUs produce much less heat and uses less electricity during mining.

Prior to the launch of Ritocoin, various collaborators worked together to add the X21S algorithm to a number of open source projects, including the mining pool software yiimp as well as the GPU miner ccminer. The source code for these can be found on the Ritocoin github repository.[7]

At the present time, Ritocoin is the only coin using X21S and we are not currently aware of any efforts to develop FPGA bitstreams for this algorithm. We recognize that if Ritocoin becomes very popular, and/or if other coins adopt our algorithm, we will become a target for these devices. In preparation for such an event, we are already at work developing experimental changes to X21S that can be released at a future time, forking our blockchain to ever increasingly complex algorithms. In this way, we expect to be successful at maintaining this blockchain as a hobbyist-mined coin indefinitely.

5. The Block Mining Reward

Ritocoin was launched as a fork of Ravencoin, with no changes to the block reward schedule. 5,000 RITO are generated by each block with an average block time of 60 seconds. The block reward is

scheduled to be reduced in half every 4 years. Add to this the 50 RITO per block that are generated for the development fund for the first year, the coin amounts to a final supply of 21,026,280,000 RITO.

These numbers are valid and true as of the time of the writing of this paper, but they are subject to change. The introduction of masternodes will change the distribution of new coins in a way that has not yet been determined. The Ritocoin community also has the option in the future to reduce the time between reward halvenings, thereby reducing the overall supply of RITO.

6. Substantial changes to the Ritocoin Consensus Model

When possible and feasible, the introduction of masternodes, algorithm changes, proposals to extend the development fund timeline, altering block reward scheduling, and other blockchain consensus matters will be decided and activated by the miners of the coin using the traditional Bitcoin-style activation mechanisms.[8]

7. Community

The ability of the Ritocoin users and developers to gather in online venues to discuss ideas and collaboratively work on projects is an important component of the project. At the time of this writing, we are using Discord[9] as our primary gathering place. It is a real time chat system that has numerous valuable features, such as creating specific “channels” for different interests, and allowing members to have different roles that give them access to those different channels of the discussion. We intend for the Discord group to be professional in tone, friendly in nature, and we will actively discourage the practice of “trolling”.

We believe that the best ideas are discovered when many voices are heard. We desire our community to be a vocal group of differing opinions where the best ideas can float to the top and be considered. We must remain open and receptive to differing ideas, and be prepared to change even fundamental concepts in this project in response to those ideas and proposals.

The developer fund is a key component of fostering a development-oriented community. By setting aside coins from the block reward for development, we can offer bounties to give to community members for work they do. This has already borne fruit with the development of the GPL-licensed ccminer for X21S, as well as improved compilation code, algorithm work, explorer code, an android wallet, and website development. We feel that the developer fund will continue to be a valuable tool to motivate the members of the community to invest their time and energy into this project during its early life.

8. What about Ravencoin?

We remain committed fans of Ravencoin, and will continue to support that project and hope for its continued success. It is our hope that Ravencoin continues its trajectory toward success, and we desire and expect that the developments we make for Ritocoin will be welcomed back into the Ravencoin fold.

References

[1] https://medium.com/@tronblack/ravencoin-dark-gravity-wave-1da0a71657f7
[2] https://en.wikipedia.org/wiki/The_Cathedral_and_the_Bazaar
[3] https://ravencoin.org/wp-content/uploads/2018/03/X16R-Whitepaper.pdf
[4] https://suqa.org/file/2018/10/x22i-proof-of-work-algorithm.pdf
[5] https://github.com/Pigeoncoin/brand/blob/master/X16S-whitepaper.pdf
[6] https://github.com/bsdphk/PHC/blob/master/Lyra2/Lyra2ReferenceGuide.pdf
[7] https://github.com/RitoProject/
[8] https://medium.com/@elombrozo/forks-signaling-and-activation-d60b6abda49a
[9] https://discordapp.com/