Riecoin

The Riecoin Developers

September 14, 2023

Abstract

The present Whitepaper summarizes the ideas and knowledge that anyone getting interested or involved in the Riecoin Project should know. It clarifies the Project's aspirations and provides an overview of technical details of the Riecoin currency, as well as possible upcoming improvements and some guidelines. The first version of this document was written almost ten years after the Riecoin release as no whitepaper was originally produced. As the Project advances, the document is expected to be updated once a while, and the reader should ensure to have its latest version.

1 History

1.1 Worldwide Currency Attempts

In 1907, Swiss Esperantist and Mathematician René de Saussure proposed the **Speso**[1], or more commonly known as its multiple **Spesmilo** (1000 Spesoj), a gold backed international currency in line with the Esperanto creator Ludwik Lejzer Zamenhof's aspiration of a peaceful world without barriers. The currency found use in several banks, notably the *Ĉekbanko Esperantista* that proposed practical and inexpensive transactions to clients over 43 countries. The promising project was unfortunately cut short by the First World War.

Decades later, as Humanity lives yet again in dark times as the Second World War rages, a group of persecuted Esperantists gathered in 1942 and founded the *Universala Ligo*, whose goal was to concretize the Zamenhof's aspirations. For them, this would not only be achieved with a common language, but also a world currency, and they thus created in 1946 the **Stelo**[6][4], a spiritual successor to the Spesmilo. The initiative gained traction over the years, with even coins being minted by the Royal Dutch Mint in 1960 and 1965.

A 1 Stelo coin. *CC-BY-SA*

Unfortunately, the project did not gain further traction and stalled for decades before effectively dying when the Universala Ligo was dissoluted in 1993.

Like de Saussure and the Universala Ligo, the Riecoin Project supports the idea that Humanity will benefit from a widely used common currency, and proposes a currency that has desirable properties for this purpose.

1.2 The First Cryptocurrency

In the aftermath of the historic Global Financial Crisis, pseudonymous developer Satoshi Nakamoto released **Bitcoin** in 2009[5], a groundbreaking digital currency introducing solutions allowing "online payments to be sent from one party to another without going though a financial institution", which not only provided a way to emancipate from actors responsible for the economic collapse, but also a spiritual successor to the Spesmilo and Stelo as a practical world currency candidate. In 2021, the country of El Salvador adopted Bitcoin as a legal tender currency.

1.3 Riecoin

Riecoin is a currency based on Bitcoin, and its development started by a developer using the nickname *Gatra* in 2013, an era when not more than 200 cryptocurrencies existed. It was formally announced on BitcoinTalk on February 3, 2014, and effectively launched on February 11.

The key change from Bitcoin is the improved proof of work (PoW). While Bitcoin becoming the world currency would be in accordance with the Project's aspirations, it is a shame that its PoW only consists of finding useless hashes, and Riecoin instead supports the idea that the gigantic mining power can also serve scientific research, thus be of greater value for the society and power a better world currency.

Unfortunately, for unexplained reasons, the original developer ceased further Riecoin development and communication, and effectively disappeared in 2018, causing the downfall of Riecoin, that so far performed well with notably support on major exchanges and pools at the time. The Project has been taken over by a few developers, but still struggles to recover from the downfall due to this history and unfavorable context.

Gatra did not publish any Whitepaper, and a first version of this document was instead written by the Riecoin Developer Pttn almost ten years after the first release.

2 Riecoin Technical Details

This section details notable technical specifications of the Riecoin protocol, provide rationales for key choices, and also a glimpse to probable upcoming updates. Browse the Riecoin website to find more information.

2.1 General Paramaters

- Ticker: RIC;
- Blocks every 2.5 minutes (150 seconds);
- Base block reward of 50 RIC, halving every 840000 blocks (about 4 years);

- Maximum supply: about 84 million RIC;
- Smallest amount: 0.00000001 RIC, or 1 riemann;
- Bech32 Address Prefixes: ric (Mainnet), tric (Testnet), rric (Regtest);
- RPC port: 28332 (38332 for Testnet, 38443 for Regtest);
- P2P port: 28333 (38333 for Testnet, 38444 for Regtest);
- Block limits:
  - 2 MB (weight 8M);
  - Block rewards can be spent only after 100 confirmations;
  - Starting from the second fork, a block's timestamp must be at most 15 s earlier than the previous one, and 15 s later than the current time.
- Magic number (Little Endian) `0xFCBCB2DB` (`0x0D091105` for Testnet, `0xFABFB5DA` for Regtest);
- Signed messages prefix: `Riecoin Signed Message:\n`.

2.2 Bitcoin Basis

The original developer chose Bitcoin as the base for the Riecoin software and protocol. This notably means that Riecoin has its own blockchain rather than being a token depending on another project such as Ethereum or the Binance Smart Chain. Being similar to Bitcoin, a lot of literature or documentation about it also applies to Riecoin.

Riecoin will certainly remain based on Bitcoin in the foreseeable future for practical reasons, such as avoiding a complicated transition or being able to implement useful features such as the Lightning Network in a more straightforward way. Though, the idea of rewriting the software from scratch in a similar fashion as the Pandanite project did may eventually be considered, in order to favor future developments with a much more elegant code that may also be more suited to the Project's aspirations.

Hard forks can be designed by the Riecoin Developers in order to introduce useful or necessary updates that require to break blockchain compatibility, and this has been done twice so far.

2.3 Proof of Work (PoW)

One of the fundamental Bitcoin features is the *Proof of Work* mechanism, which consists of having transactions validated by a network of machines continuously solving a specific problem in a process called *mining*. In the Bitcoin and other PoW altcoins cases, the problem is to find an hash that meets an arbitrary criteria, so miners are continuously generating random hashes until they find one meeting the criteria. This does work to make a cryptocurrency functional, but the whole process consumes a lot of energy and is regularly criticized in times of climate crisis.

Meanwhile, scientists all over the world make use of powerful machines in order to simulate various phenomenons in domains ranging from biology to mathematics, via physics, weather forecasting, and many others, which naturally also consumes a lot of energy, but is necessary in order to advance research and serve the society.

Riecoin proposes to make mining to not only power a secure and practical world currency, but also to be at disposal of useful scientific computations. Over the years, the Project proved that it is achievable, as miners broke and hold several number theory world records[2]. By putting

in common the energy use, it effectively solves the Bitcoin's power consumption issue without resorting to ideas like PoS that makes value out of thin air.

Since miners will want to optimize their earnings, developers will be incentivized to improve the algorithms used by miner software, possibly finding groundbreaking ideas to solve the PoW problem in the process, which further increases the utility of an useful PoW.

2.3.1 Prime Constellations

The current Riecoin PoW problem is based on prime constellations, or prime k-tuplets. In simple words, these consist of tuples of k prime numbers, that are as close as possible. Since the second hard fork, $k = 7$, so Riecoin miners are currently looking for septuplets of large prime numbers. In the same fashion as one says that Bitcoin's PoW is *SHA256*, the Riecoin's PoW is called *Stella*.

It is a common misconception that specifically looking for interesting prime numbers is the Riecoin's finality, while it just happened to be a choice of the original developer, and Riecoin aims to support broad ranges of research domains. And even if Riecoin were to stick to the narrow scope of prime constellations, there will always be hobbyists competing with each other to find large interesting prime numbers and beat world records, and Riecoin makes possible for anyone to join this competition and earn money in return.

2.3.2 Difficulty Adjustment Algorithm

Initially, Riecoin used a difficulty adjustment algorithm that was similar as Bitcoin's, adapted to the Riecoin's PoW and with a shorter retarget period of 288 blocks. Some tweaks were added when the first hard fork introduced "superblocks". The second hard fork removed them and replaced the algorithm with another based on ASERT[3] and updating the difficulty at every block.

2.3.3 Support of Additional PoW problems

As the mining power increases and reaches a point that can be considered as safe to consider the scenario, more problems could be supported by the Riecoin's PoW, extending its scientific utility.

Basically, any useful problem consisting of computing results that can be encoded to an appropriate form for the blockchain, which difficulty to calculate can practically and arbitrarily be scaled, and which validation is much easier to do than computation, can be considered. Several solutions exist in order to support them.

- Make the problem's results part of accepted Riecoin PoW and link the different difficulty scales (for the problem A at difficulty D_A, which difficulty D_B would require about the same computational power for the problem B?). "Multi PoW" cryptocurrencies such as MyriadCoin do exist, demonstrating the feasibility of this solution. It adds some complexity to a fundamental feature, but the mining power for the various problems fully contributes to the robustness of the network;

- Develop separate Riecoin-like blockchains which fully diluted supplies are capped and backed with RIC. This point is important as it would otherwise mean creating value out of thin air or effectively increasing the RIC supply, and contradict with the limited supply principle. This solution offers more flexibility, though it also implies a spread of the mining power over multiple blockchains, potentially reducing the security of each one (this can also be irrelevant if at the time the global Riecoin mining power is high and distributed

enough). The strategy could be combined with the first point, for example there could be blockchains specializing on "CPU only" problems and others on GPU or ASIC friendly ones;

- Port/adapt the Bitcoin's DriveChain (BIPs 300-301) technology, meant to integrate arbitrary altcoins in the Bitcoin's network.

For problems not satisfying the conditions above, it still remains the possibility of setting up a regular distributed computing project and automate reward distribution to participants using funds in RIC, increasing the currency's utility and supporting the Riecoin Project, which can in return also provide some publicity.

2.4 Block Time

The choice of the block time target of 2.5 minutes was justified by the original developer using the fact that Litecoin, a successful cryptocurrency that was already established for years at the time Riecoin was being developed, also used such block time without issues. A faster block time is more convenient than Bitcoin's relatively long 10 minutes, but too frequent blocks would significantly increase disk space and bandwidth requirements for node operators. For instant transactions, Layer 2 solutions such as a port of the Lightning Network could be implemented and used, or centralized services considered with appropriate precautions.

2.5 Block Size and Weight

The block limit of 2 MB (or weight of 8M) were presumably also taken from Litecoin by the original developer. The current Riecoin developers consider that it was a mistake that shall be fixed as this can aggravate transaction spam attacks while not providing practical benefits for Riecoin users. Bitcoin enforcing a size limit twice smaller and having blocks appearing four times less frequently shows that more block space is not needed, though its history of getting congested also indicates that a higher capacity would still be beneficial. We thus propose to decrease via a soft fork the limit to 500 kB (weight 2M) or half of Bitcoin's, so that the block capacity is effectively twice as Bitcoin's rather than eightfold. Such update shall be proposed as a small but mandatory update, as trivial to apply as replacing the binaries and restarting the node, and at a time most of the major Riecoin actors (mining pools, exchanges) are up to date.

2.6 Monetary Policy

RIC are distributed to Riecoin miners to reward them. The base block reward is 50 RIC, and is halved every 840000 blocks or about 4 years. Historically, the following particularities also affected the currency emission, though the effects are negligible in the long run:

- Riecoin had a "Fair Launch" policy in order to not favor very early miners:
  - The first 576 blocks do not yield any reward;
  - The next 576 blocks yield a linearily increased reward, from 0 to 50 RIC.
- The first hard fork introduced "superblocks", consisting of weekly blocks much harder to solve than usual in order to find larger prime numbers, but also yielding many more coins. A mechanism was also implemented to compensate the longer time to find the superblock by making a certain number of blocks around it slightly easier to solve. Due to the added complexity of the concept, the superblocks weekly halting the whole network for hours, and

the fact that 7-tuplets introduced in the second fork can also be part of longer constellations, the superblock feature was removed.

2.6.1 Limited Supply

The total supply of RIC is by construction capped at about 84 millions coins. Two millions of coins were definitively destroyed after an unsuccessful campaign proposing a bounty of 1,000,000 RIC to whoever makes a fruitful partnership with the project and significantly contributes to the Riecoin adoption, making the effective maximum supply 82 millions.

A capped amount of coins is a key for a more responsible society that favors stability and frugalism over consumerism and waste of resources, and thus a fundamental principle that shall always hold in future Riecoin updates. In the far future, as the block rewards are becoming negligible, it is expected that transaction fees will be appreciable and incentivizing rewards for miners. In the contrary case, some measures including redistributing part of burnt coins could be considered, but a cap of at most 82 millions RIC shall always be enforced.

2.6.2 Transaction Fees and Burn Policy

The transaction fee system is pretty much the same as Bitcoin's, and no burn policy was initially implemented in Riecoin.

However, it has been observed that some bad miners with lots of mining power are bloating the blockchain with spam transactions that they confirm themselves, getting back the transaction fee that should have deterred them. So, in order to both support RIC holders and deter transaction spam, it will be mandatory for miners to burn at least half of the miner's fee. The measure will firstly be implemented as default but not mandatory feature, and then the burn will be enforced by another update, in principle the same as the one reducing the block size limit. The measure can be accompanied with the enforcing of a minimum fee that is negligible for most users but high enough to make spam transactions costly, and a measure that will consider dust transactions as burnt.

Coins associated with outdated technologies (such as obsolete address types) that are no longer used by any current and practical implementation may eventually be discarded and effectively burnt in order to not carry legacy burdens, and forks that require an active transfer of coins may also cause the loss of untransferred coins. RIC holders are expected to follow at least once a while the Riecoin news and take action if needed, though the Developers will always allow a reasonably long deadline for such events.

2.7 On other Platforms

In order to enable new opportunities for Riecoin users, especially traders, Riecoin was made available in the form of a convenience token on the Binance Smart Chain: *Riecoin BEP20* (RICB).

The token contract is `0xc2097531d6cd4a712ae08f398283a92631dc39f9`.

84,000,000 RICB were minted for an address controlled by the Riecoin Developers, and there is no way to mint more tokens. They are once a while put in circulation depending on new services using RIC(B) or the demand. Unused RICB will eventually be burnt once there appears to be no more reason to put more RICB in circulation.

Tokens put in circulation are 1:1 pegged with actual RIC, and this is guaranteed with a reserve controlled by the Riecoin Developers and disclosed on the Riecoin website. The Developers can be contacted anytime to exchange appreciable amounts of RICB for RIC at the 1:1 rate minus

transaction fees, or vice versa as long as the unused RICB was not burnt. Though, this should only be done as a last resort, and exchanges supporting swaps should be used instead.

Tokens following the same principle will likely be introduced on similar platforms in the future.

3 Getting Involved

3.1 Aspiring for a Better World

The history section mentioned the Project's inspiration by initiatives made by Esperantists. Riecoin is not just a currency but also a movement aspiring for a better world.

The Project deplores the fact that despite the amazing technological progress that could since long provide more than enough resources for everyone's well being, suffering and pressure is still the standard for a great part of the population, in a world driven and enslaved by a system favoring greed, competition and division, over altruism, cooperation, and unity.

By getting involved in the Riecoin Project, you commit to follow its principles, bring a new feeling into the world and call it to come it its senses. The Project is open to fruitful partnerships with like minded entities and projects, though it is important to note the Project's resources are currently very limited, donations are also welcomed.

3.2 Riecoin Developers (Team)

Taking inspiration from "The Bitcoin Developers" copyright found in reference Bitcoin software, notable contributors to the Riecoin Project are collectively designed with the expression "The Riecoin Developers". We do not provide a formal list composing a hypothetical Riecoin Team, and invite the reader to find out by themselves who is actively supporting the Project on official discussion channels.

3.3 Investing and Contributing

Due to its unfortunate history and the state of the cryptosphere, the odds are strongly against the Riecoin project. Unless one possesses significant resources (say valuated one or more order of magnitudes over the RIC market cap), no "easy" profits should currently be expected, and those looking for these are not at the right place.

In the other cases, you are welcomed to join and help the Project with the best of your abilities and resources to fulfill its aspirations, and possibly meet like minded people that support each other and collaborate in a fruitful way either for the Project or outside.

The Project does not provide a particular roadmap and expects contributors to be autonomous and find out by themselves what can be done to improve Riecoin, and make meaningful contributions that are in line with its aspirations. Contributions do not need to be directly for the Riecoin software, and it is important to also work on the Riecoin adoption. Examples range from code improvements to buying and holding large amounts of RIC, via accepting RIC for external services you might propose or promoting Riecoin in artistic works.

3.4 Responsibility

The Project expects all its participants be it users or contributors to be responsible in order to help making Riecoin thrive and avoid harming it unnecessarily.

Users are expected to follow the Project's developments at least once a while and ensure to be up to date. Indeed, the Riecoin Developers will rather avoid accumulating a legacy burden and unnecessary complexity in Riecoin software, and make future developments smoother, than support those who do not bother to make minimal efforts to update the software and stop using obsolete features.

Contributors shall always properly consider the effective consequences of their actions on the Riecoin Project, as having good intentions does not imply that the actions will actually help, it may actually not improve anything and waste the community's time, or even harm the Project.

3.5 What should not be expected from Riecoin

Some notable properties that might of strong interest in other projects are not deemed fundamental for the Riecoin Project. Those seeking for such properties might want to look into another project to avoid some disappointment or frustration.

3.5.1 Strong Decentralization

Due to its history, Riecoin is currently still in a state similar as Bitcoin was during its beginning, where Satoshi was by far the most influential entity driving the project. Important decisions might thus be taken and implemented by the Riecoin Developers without a formal and long consensus process, but always with their best judgment of the current context and careful consideration for the Riecoin Community. The Developers shall always be open to meaningful feedback.

As the project advances, more formal consensus processes may be specified and the Project may naturally become more decentralized as it happened for Bitcoin. Still, being a strongly decentralized project would also imply slow decisions and improvements that may unnecessarily slow down the Project's progress. Compromises will be unavoidable and the Community shall remain united and accept this fact.

3.5.2 Convenient Privacy

Riecoin is not meant to provide convenient privacy features. The Project also considers that with appropriate measures like avoiding address reuse or services such as coin mixers, Riecoin or Bitcoin can already be private enough for the vast majority of users.

4 Miscellaneous

4.1 Domain Names

`Riecoin.org` was the original domain name for the Riecoin Project, but Gatra refused to transfer the domain to the developers who took over the project as he abandoned it, though he did accept to point it to `Riecoin.dev`, the current domain name. `Riecoin.org` eventually expired but was squatted by the registrar who asked a high price that the Developers could not afford. It has then been bought by an unknown entity that is presumably using it for SEO.

`Riecoin.xyz` is owned by the Riecoin Developers, though is currently unused. It may become in the foreseeable future the new Riecoin domain name as the `xyz` is more representative of the project's aspirations.

In summary, `Riecoin.dev` and `Riecoin.xyz` are the only official Riecoin domain names. Others that might refer to Riecoin in some way or another are not affiliated with the Project.

4.2 Social Accounts and Discussion Channels

The Riecoin Developers manage several accounts on some major social media, but they plan to abandon their use in favor of places that are more in line with the project's aspirations such as the Fediverse or places hosted by themselves or partners. The Whitepaper will be updated accordingly once this will be effective.

Until then, the only official Riecoin accounts or places are the @RiecoinDev X account, the r/Riecoin Subreddit, the Discord server which invite is linked on the Riecoin website, and the @RiecoinDev Telegram Account. Any other place or account are not affiliated with the Project.

The @Riecoin X account is the former Riecoin account, and in a similar fashion as the `Riecoin.org` domain name, Gatra never handed it over to the Developers, though he still gave them partial access via the TweetDeck interface, allowing limited features that include the ability to post from it. Now that TweetDeck is a paid service, @Riecoin can be considered as abandoned.

References

[1] Streboj al internacia mono. Franca Esperantisto. `https://www.eventoj.hu/arkivo/eve-050.htm`, Jan 1994.

[2] Norman Luhn and Anthony D. Forbes. Prime k-tuplets (lists of records). `https://pzktupel.de/ktuplets.php`, 2023.

[3] Mark B. Lundeberg. Static difficulty adjustments, with absolutely scheduled exponentially rising targets (DA-ASERT) — v.2. `https://toom.im/files/da-asert.pdf`, 2020.

[4] L. Mee. De Stabiele Munteenheid Van De Esperantisten: De Stelo. `https://web.archive.org/web/20150923234258/http://www.egmp.nunaar.be/artikels/esperanto.pdf`, 2000.

[5] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. `https://bitcoin.org/bitcoin.pdf`, 2009.

[6] Chaim D Shiboleth. Esperanto and the Dream of a World Currency: The Coinage of the Universala Ligo (1942-1993). `https://web.archive.org/web/20070926003932/http://www.usns.info/pdf/Aust_Coin_%26_Banknote_USNS_002_092005.pdf`.