Duino-Coin

White Paper (version 4)

Robert “revox” Piotrowski
robik123.345@gmail.com
duinocoin.com

Preface

Duino-Coin has no intention of becoming the best, biggest or most modern crypto.
Duino-Coin has no intention of rediscovering privacy either.
Duino-Coin does not use complicated systems, algorithms or solutions.
And it won't. Because if someone is looking for a cryptocurrency with such requirements, with thousands of different crypto coins in the world they will find it in a few minutes.

However, Duino-Coin is distinguished by its instant transactions, the ability to acquire coins in various ways on a large number of platforms, global availability, cost-effectiveness, openness, simplicity, ease of exchange and a friendly, growing community of avid miners who also want to contribute to our project.

Duino-Coin is meant to be a platform that allows people to learn something and at the same time earn some money (thanks to already existing exchange services).

Why did we create Duino-Coin?

Simply saying, there are many cryptocurrencies available but most of them can be mined only using powerful CPUs, GPUs or ASICs to make some real money.
We wanted to change that, so that's how Duino-Coin started. It is also a great example for teaching how crypto-coins work thanks to its heavily commented, open-source code.

What do we want to achieve?

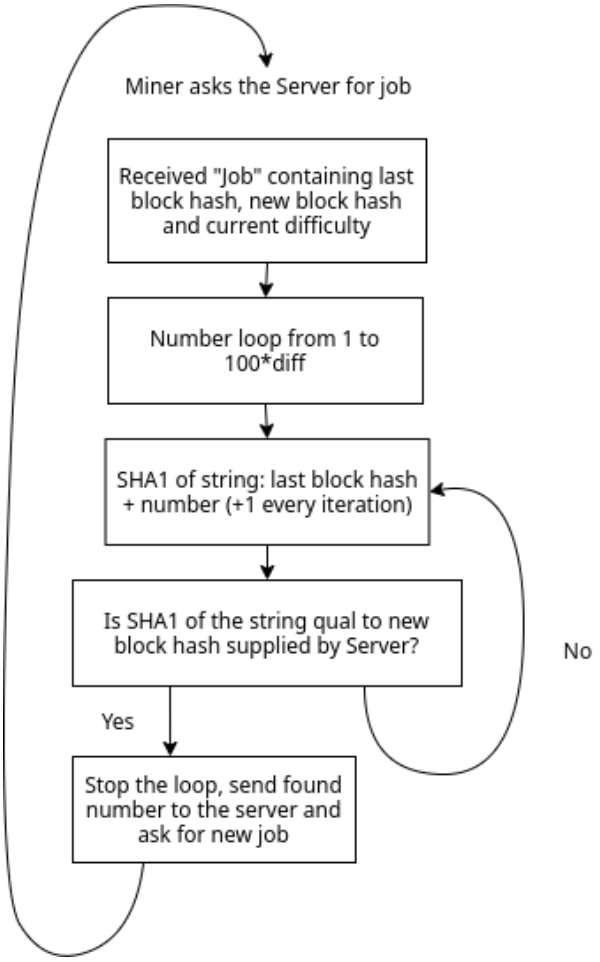
The main goal was to create a cryptocurrency capable of mining on Arduino boards, regular computers and other devices with low computing power.
We've already achieved it so now we are expanding our project in many ways, including adding new ways of mining, expanding our audience and making mining as fair as possible for every device.

Technical informations

Supply	Infinite (before December 2020: 350k coins)
Premine	< 5k blocks - < 500coins
Block time	Instant ⚡
Decimals	20
Symbol	Ɗ
Ticker	DUCO
Algorithms	DUCO-S1, DUCO-S1A, XXHASH (+more planned)

Mining methods

Main Duino-Coin algorithm (DUCO-S1 and DUCO-S1A) is based on SHA1. Miner is being rewarded for each mined block that is also called a share. To allow everyone to write the miner on their platform, this simple diagram was made:



If someone plans to create their own version, it's worth looking at code which is available on GitHub. It’s also worth noting, that **Server calculates the rewards for Miners by checking how long submitting the share took**, significantly “faster” miners can get the same or even less reward as the “slower” ones for their shares (Kolka system - read below).

What is the “Kolka system” and how does it work?

Other than adding rules, which miners have to follow (see Terms of service), we’ve come up with our original “Kolka system”. It helps to keep the rewards fair and essentially eliminate “big” miners from the network. Here are some of the main methods we use to achieve that:

- Kolka V1 (introduced around March 2020):
  - have separate difficulties for AVR, ESP and PC mining
  - make the rewards dependent on (but not only):
    - hashrate used to find a share
    - time it took to find a share
    - number of shares submitted in a period of time
    - amount of workers mining on an account
    - used difficulty
    - randomness

- Kolka V2 (introduced around June 2020) :
  - everything from the previous point, with addition of:
  - throttling fast miners (those, who exceed max shares per some period of time)
  - checking for hashrate on difficulties (for example, AVR board won’t make more than 150 H/s) and rejecting shares who come from suspicious miners

- Kolka V3 (introduced in March 2021):
    - everything from the previous points, with addition of:
    - variable difficulty dependent on sharetime
        - if the sharetime was faster than the expected sharetime, raise the difficulty with the help of this formula:
          p = 2 - sharetime / expected_sharetime
          *new_diff = diff * p*
          This system essentially ensures the miner is using the correct difficulty for his system.

- Kolka V4 (planned):
    - everything from the previous points, with addition of:
    - reporting unique IDs of AVR chips to the server for verification
    - more rules to be discussed

With these steps, we're slowly making the whole mining process more and more fair for low energy devices.

Why is Duino-Coin centralized?

Making Arduino and other low powered devices not only profitable, but just possible would be impossible to maintain if the coin was decentralized. Some people don't like this idea, but this is the sacrifice we had to make to be able to put our idea into a working system that has fair rewards for practically every device.
We're not the first centralized cryptocurrency, for example, at Ripple (XRP) - it's centralized and it's going very strong.
I, as a founder of Duino-Coin think that decentralization doesn't make much sense: why bother downloading blockchains or other useless things if 99% people don't care about it and just want to easily use the coin without waiting ages for stuff to load. Storing stuff inside a secure server also ensures the funds won't be lost.
Quoting developer of leading crypto mining software, xmr-stak: *"This is cryptocurrency world. Everyone is looking out for themselves. What your friend is trying to do is advance his social position by giving you bad financial advice. [...] Because just like privacy [decentralization] is just an empty marketing slogan [...]".*

I haven't met anyone that had problems with centralized crypto. If you don't like that idea then there is nothing stopping you from using another cryptocurrency.

Sources and useful links

GitHub: https://github.com/revoxhere/duino-coin
Website: https://duinocoin.com
Explorer & Network stats: https://explorer.duinocoin.com
Discord: https://discord.gg/kvBkccy

Xmr-stak developer quote:
https://github.com/fireice-uk/xmr-stak/releases/tag/1.0.4-rx
Monero "privacy": https://www.wired.com/story/monero-privacy

Thank you for reading this document.
We hope we convinced you to take a look at our project.

Duino-Coin 2019-2021