Duino-Coin

Whitepaper v2

Robert Piotrowski
robik123.345@gmail.com
revoxhere.github.io/duino-coin/

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.

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 want to develop our project in many ways, including adding new possibilities and expanding our audience.

Technical informations

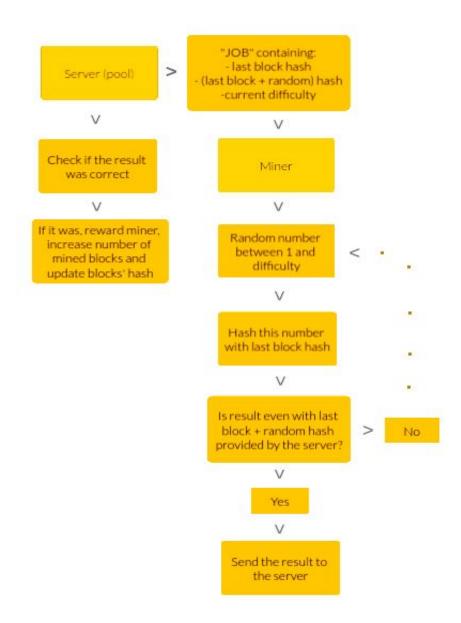|	
Supply	~ 35k
Premine	~ 5k
Block time	Instant ⚡
Decimals	8
Symbol	Ðɘ
Ticker	DUCO
Algorithms	DUCO-S1, DUCO-S1A; PoT

Mining methods

There are several ways of earning Duino-Coins. The main way is to mine with the DUCO-S1 algorithm (based on SHA1), where you are rewarded for each dug block that is also a share. To allow everyone to write the miner on their platform, this diagram was made:

```
┌─────────────────┐         ┌─────────────────────┐
│  Server (pool)  │    >    │  "JOB" containing:  │
│                 │         │  - last block hash  │
└─────────────────┘         │ - (last block +     │
                            │   random) hash      │
                            │ - current difficulty│
        V                   └─────────────────────┘
┌─────────────────┐                  V
│ Check if the    │         ┌─────────────────────┐
│ result was      │         │       Miner         │
│ correct         │         │                     │
└─────────────────┘         └─────────────────────┘
        V                            V
┌─────────────────┐         ┌─────────────────┐
│ If it was,      │         │ Random number   │   <   .
│ reward miner,   │         │ between 1 and   │       .
│ increase number │         │ difficulty      │
│ of mined blocks │         └─────────────────┘
│ and update      │                  V          .
│ blocks' hash    │         ┌─────────────────┐
└─────────────────┘         │ Hash this number│  .
                            │ with last block │
                            │ hash            │  .
                            └─────────────────┘
                                     V          .
                            ┌─────────────────────┐
                            │ Is result even with │
                            │ last block + random │  >   ┌──────┐
                            │ hash provided by    │      │  No  │
                            │ the server?         │      └──────┘
                            └─────────────────────┘
                                     V
                            ┌─────────────────┐
                            │      Yes        │
                            └─────────────────┘
                                     V
                            ┌─────────────────┐
                            │ Send the result │
                            │ to the server   │
                            └─────────────────┘
```

If someone plans to create their own version, it's worth looking at the official PC Miner or Minimal PC Miner code.

Another way to get the coins is to use a Proof-of-Time Miner, which awards you literally for your time.
Proof-of-Time changes its principle from time to time so it is impossible to describe it in more detail here.

Why is Duino-Coin centralized?

Of course, everyone has their own opinion but we think that decentralization doesn't make much sense.
Why bother downloading blockchains or other relatively useless things for if a regular user doesn't care about this stuff and most importantly they can be securely stored inside a server so they 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 someone has, however, then there is nothing stopping him from using another cryptocurrency.

Sources and useful links

Duino-Coin GitHub: *https://github.com/revoxhere/duino-coin*
Duino-Coin Website: *https://revoxhere.github.io/duino-coin/*
Duino-Coin 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 2019-2020