# ARIONUM v1.0

WWW.ARIONUM.COM

08.01.2018

Arionum aims to offer a simple and secure solution to the growing need for faster and cheaper online payments. The goal is to be easy, fast, secure and for the mining to be democratically spread across non-professional miners.

Today's cryptocurrency market is dominated by the first cryptocurrency, Bitcoin and the first smart cryptocurrency, Ethereum. Each cryptocurrency aimed to solve a specific problem. Bitcoin's aim was to replace online payments with a cheaper, anonymous and secured solution, while Ethereum's goal was to create a blockchain as a service due to its smart-contracts functionality.

Bitcoin has managed to mostly reach its goal, as it is accepted by new vendors each day. But the growth of acceptance and popularity also showed some weaknesses in its protocol. First, the transaction fees have skyrocketed as the network became more and more congested, especially for smaller-size transactions. Second, the mining algorithm, which is based on the sha256 hashing method, has proven easily solved by specialized hardware, moving the mining power from the average user to specialized mining farms owned by just a few, which leads to inequality and a loss of trust in the cyptocurrency.
Arionum tries to solve these bitcoin limitations by using a variable block size, which starts at just 100 transactions per block but increases by 10% of the average transactions number each time the last 100 blocks are filled to the maximum transactions number.
The specialized hardware issue is solved by using a combination of argon2i password hashing, an algorithm made to be resistant against GPU and specialized hardware, and a sha512 hashing for extra security. This means the mining is best done using the CPU, allowing the average user to mine without investing in specialized hardware or graphic cards and at the same time, penalizing the professional miners that have huge graphic card farms.
The fee problem is solved by having a fixed 0.25% fee on any transaction, therefore offering a much smaller fee per transaction than any other electronic payment system in the world.

Ethereum's smart-contracts functionality has been a huge success, allowing many companies to build software on ethereum's blockchain. The main product was the tokens used as ICO (initial coin offerings) which leveled the playing field for small companies looking for funding. The main problem is the hard implementation for non-programmers and the risks of fraud due to bad implementations of the smart contracts. Arionum hopes to create a different model, where the tokens are created in a graphical interface, with specific functionality and extra security procedures in place, allowing any non-technical user to be able to create a token in a matter of minutes. The proposed system is similar to NXT's implementation of assets.

Arionum uses the blockchain technology, where each new block is generated using the unique identifier of the previous block, allowing the transactions to be eternally locked in place in a tamper-proof way. Each block is generated, on average, every four minutes. The miners compete to get the first nonce and argon nonce combination, along with some extra hashing and division against the difficulty that results in a number less than 240. The first miner to submit the combination to a node wins the block and starts the block generation and propagation to the network. A transaction is considered confirmed after 4 new blocks have been generated after the block containing the transaction. This is done to ensure that the anti-forking system does not reverse the block containing the transaction.

The mining reward starts at 1000 coins per block and is decreased by 1% of the starting value every 10800 blocks (approximately every 1 month). This roughly translates to 8 years and 4 months of mining, after which the network will be self-sustainable due to the transaction fees. The reward system will generate a total of 545.399.000 coins during its lifetime.

Each customer can generate a wallet (or more) using the php based cli light wallet, the GUI light wallet, the node's api or by creating his own software based on the functions described in the node. Each standard wallet contains one public / private key pair and the wallet's address is derived from the public key. The keypair is generated using the ECDSA's secp256k1 curve as a signing algorithm, based on php's openssl implementation.

One of the main advantages of Arionum is that it was fully written in PHP, one of the most popular programming languages in the world. While php is not as fast as c++ for example, the high number of developers that can easily understand and develop PHP and Arionum compensates for this.

Arionum will be a fair, fast, secure and reliable solution for the end user.