Niobio Cash

Payment method, eSignature Platform, Contribution to Society and Entrepreneurship Environment

Version 2

February 2019

Overview

Niobio Cash is a cryptocurrency that provides privacy, efficiency, and safety. It can be used as a payment system for daily use. It has a finite supply, smooth emission, ring signatures, stealth addresses, proof of work by Cryptonight Heavy, an efficient difficulty adjustment algorithm: the Linearly Weighted Moving Average (LWMA) by zawy12, and dynamic blocks size. The development is active and has a large community of users supporting it. It seeks retribution to society and enrichment of the entrepreneurship around its network. It is a Brazilian project with a global focus.

Table of Content

1. Introduction

Inspired by an idea from Enéas Ferreira, which ran for Brazilian presidency several years ago, Niobio Cash was launched in November 2017. Ferreira's idea was to have a national currency bounded to Niobium supply. Niobium is a mineral of which Brazil has about 98% of global supply, making it a symbol of Brazilian's natural wealth. Niobio Cash is a decentralized blockchain derived from Cryptonote protocol.

Aiming to become a safe and private payment system, at the same time efficient and reliable, several improvements were applied to make it simple and easier to use. One of them is the so-called Niobot, a bot that brings a crypto wallet to all popular social media, such as Twitter, Telegram, Instagram and Facebook Messenger.

The term Niobio [NB01] is a reference to the chemical element niobium, which can be found in abundance in Brazil and is scarce in the rest of the world. Its atomic number is 41 and is represented by the symbol Nb. Found in minerals such as pyrochlore and columbite, the niobium is used in a variety of industries like superconducting materials, welding, nuclear industry, electronics, optics, numismatics, and jewelry.

Brazil is the world's leading producer of niobium, controlling about 85% to 95% of it. Brazil also exports ferroniobium, an alloy of approximately 70% niobium with iron.

2. Technical Specifications

Name	Niobio Cash
Symbol (Ticker)	NBR
Address Prefix	N
Genesis Block Date	November 02, 2017, 05:11:13 PM
Supply	336,000,000 NBR
Decimal Places	8 (divisible up to 10^8)
Block Time	240 seconds
Premine	0%
Development Fee	5% of block reward
Fund for External Scientific Research Projects	5% of block reward
Proof of Work Algorithm	Cryptonight Heavy
P2P Port	8313
RPC Port	8314
Difficulty Adjustment Window	61 blocks
Difficulty Retarget	Each block
Block Reward	~220 NBR and decreasing
Minimum Transaction Fee	0.00001 NBR for any transaction amount
Wallet Nodes Fee	0.25% of the transaction amount
Emission Curve	~31,5% August, 2018 ~65% by the end of 2024 ~87% by the end of 2030 ~95% nearly of 2043

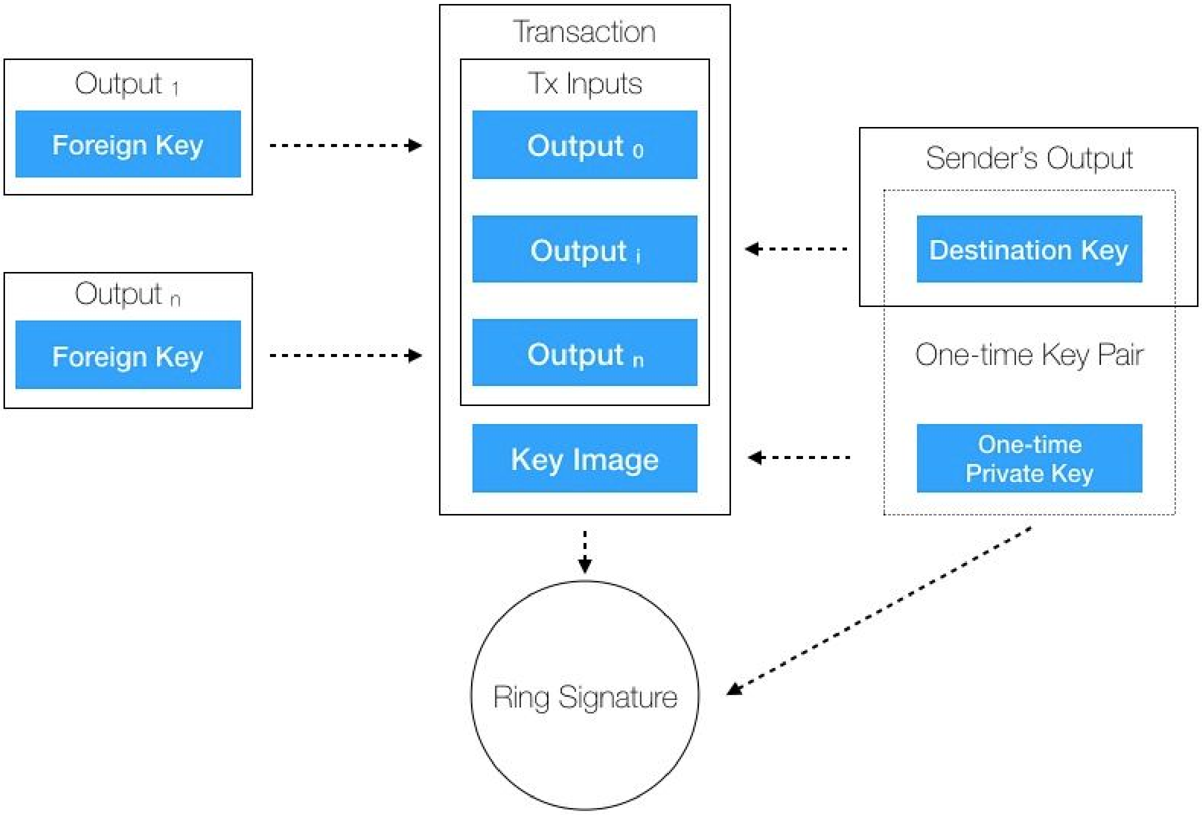
3. Technology

3.1 Ring Signatures

Ring signatures provide an effective way to hide specific transaction inputs by mixing them with many others, unrelated, public keys.

To assemble a transaction, the sender uses, as his transaction inputs, several outputs from other transactions where he is the recipient of the transfers. On his sending transaction, he signs it using his real inputs together with a set of others foreign outputs that have the same amount. This is made without the knowledge of the owners of these outputs. The coins on these foreign entries can even be already spent, they are there just to make the identity of the signer (sender) indistinguishable among a set of other possible senders.

In this process, all possible spenders will be equiprobable, even the previous owner has no more information than an observer. The statement proved by ring signatures is that the signer of a given message is a member of a group. One can only claim that one of the individuals of the group is the real signer but it is not possible to pinpoint which one.



The anonymity level dictates the resultant ambiguity degree of the ring. Higher values mean more possible spenders on the set of public keys, imposing greater difficulty to identify the real sender.

An anonymity level of n = 1 means that there is two mixed possible sender, therefore there is a 50% probability to guess which one is the actual one. A mixing level of 99 drops this probability to 1%. The improved privacy costs extra transaction fees, as the size of ring signatures, increases linearly as O(n+ 1). Using anonymity level 0 makes use of only the real sender's outputs, so this would easily turn a transaction trackable to anyone auditing the blockchain. Ordinary types of cryptographic, such as used by Bitcoin, signatures permit to trace transactions to their respective senders and receivers.

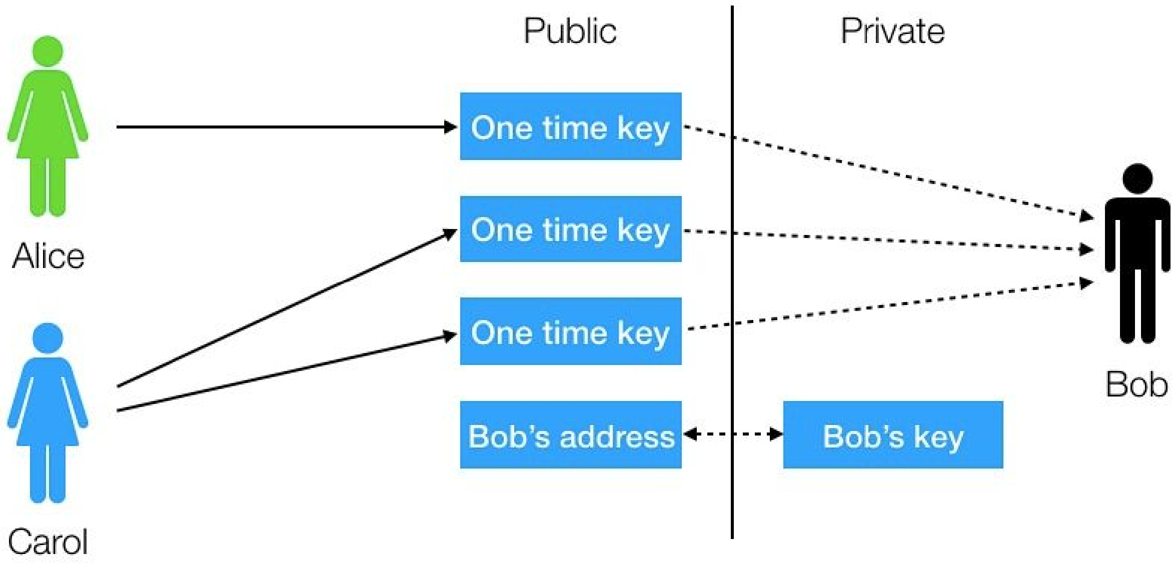
3.2 Stealth Addresses

Niobio Cash - derived from CryptoNote - provides a solution where a user, even publishing a single address, has all his receiving payments unlinkable. This is because the sender generates as a destination of each payment a one-time public key, derived from the recipient's address and sender's random data. So, unless the sender uses the same data for all transactions to the same recipient, in the blockchain each payment have a unique destination key. Even in the case of a poorly implement client makes use of same data, only the payments from this sender will be linkable, as it is hard to have a situation where multiple, unrelated senders share the same corrupted client.

This is a great advantage against Bitcoin protocol, in which this burden is left to the user to handle, generating every time a different receiving address.

In CryptoNote based blockchains, there is no address reuse by default, while in Bitcoin the default is to reuse keys unless the user takes an action to avoid it.

To make this work two different elliptic curve keys are required from the recipient, that is why a standard CryptoNote address is twice as large as a Bitcoin address.



By combining unlinkable stealth addresses and untraceable ring signatures, Niobio Cash achieves a new level of privacy in comparison with the original Bitcoin scheme.

3.3 Smooth Emission

Unlike bitcoin's approach of halving the block reward at a fixed interval of blocks, Niobio Cash keeps the traditional CryptoNote method of smoothly reducing the emission at each block. The formula takes the remaining number of coin units yet to be generated and applies a binary right shift operation based on a speed factor.

BaseReward = (M − A) >> S

Where M is the maximum amount of coins that can be generated, A is the already generated amount of coins in the network, and S is the *emission speed factor*.
Niobio Cash implements the following values:

M = 336000000 units
S = 20

Example

Taking block number 117200, the generated coins at that time was 105727372.91318126 NBR. From total supply of 336000000, the remaining coins still to be mined are 230272627.087 NBR.

This number, without the decimal point, and converted to binary is shown below. The 20 bits delimited in brackets are removed by the 20 bits right shift operation.

1010001110011110010110001100101111O[01101101001101100000]

The remaining bits converted to decimal and with the decimal points in place give the reward for next block (117201): 219.60509022 NBR.

10100011100111100101100011001011110 => 21960509022 => 219.60509022

Note

Niobio Cash used a *speed factor* of 18 until the hard fork to block version 5 at height 93000. The details of this emission reduction are specified in NCIP 0007 [NCIP0007].

3.4 Dynamic Block Size

Block size limit exists for preventing the blockchain from being flooded by large blocks containing mostly bogus transactions. Bitcoin uses a hardcoded limit and this brought another problem for its network: it imposed a cap on the capacity of processing real, honest transactions.

This problem impacted the Bitcoin in such a way that several independent Bitcoin forked coins has emerged, expanding the block size limit, as Bitcoin itself was unable to get a consensus and hard fork to update its own limit.

CryptoNote technology, used by Niobio Cash, manages the block size limit in a way that eliminates this limitation. The “hard-limit” for the size of accepting blocks is 2 · M*n*, where M*n* is the median of the last n blocks sizes. This protects the blockchain from flooding while still allows the block size limit to grow over time and with the demand of the network.

4. Niobio Cash Improvements

4.1 Difficulty Adjustment Algorithm

The goal of a Difficulty Adjustment Algorithm (DAA) is to keep the time interval between blocks as close as possible to a target rate. This is achieved by manipulating the network difficulty the miners must face to find a suitable hash for the blocks.

Original CryptoNote approach calculates a new difficulty at each block by summing the work spent by the nodes for a range of blocks and dividing it by the time elapsed from the beginning to the end of this process. Due to inaccurate or untrusted timestamps, these measures can include unreal intervals that might be improbably small or even negative. To avoid misconfigured or malicious timestamps, the algorithm sorts the timestamps and cut-off the outliers (i.e. 20%). The range of the rest values is the time which was spent for 80% of the corresponding blocks.

This protection, however, proved itself inefficient against many kinds of hash attacks and timestamp manipulations.
Niobio Cash developers worked closely to a mathematician, author of former DA Algorithms, providing feedback and suggestions to elaborate a new version of the algorithm, together of a group of others cryptocurrencies developers. The result was the LWMA - Linearly Weighted Moving Average [LWMA].

> "LWMA sets difficulty by estimating current hashrate by the most recent difficulties and solvetimes. It divides the average difficulty by the Linearly Weighted Moving Average (LWMA) of the solvetimes. It gives more weight to the most recent solvetimes. It is designed for small coin protection against timestamp manipulation and hash attacks. The basic equation is:
>
> *next_difficulty = average(Difficulties) * target_solvetime / LWMA(solvetimes)*"

Source: https://github.com/zawy12/difficulty-algorithms/issues/3

Niobio Cash, keeping the recalculation of difficulty at each block, implemented LWMA and two other protection measures, reducing significantly the impact of hash attacks and preventing manipulation of block timestamps.

4.2 Proof of Work Algorithm

The original CryptoNight hashing algorithm was initially used by Niobio Cash. However, due to the event of specialized ASIC chips, the proof of work algorithm was changed to a modified version called CryptoNight Heavy (https://github.com/curie-kief/cryptonote-heavy-design) which brought ASIC resistance.
The ASIC chips may be a move forward on the technology progress, giving miners more hashing performance at a lower cost of GPU. It seems to be a good thing to have a general replacement of current devices by ones that consumes less power, at the same time being cheaper, giving more opportunities from new miners. The moment, however, is not appropriate for Niobio Cash embrace ASIC chips. The manufacturing of these types of equipment is still on the hands of a couple of companies, bringing the risk of centralization of miners. Many miners may have difficulties to import them to their countries, affecting the balance of fair distribution of hash rate.
Many cryptocurrencies projects made this very same movement, diverging only on the target algorithm chosen for the task.

4.3 New URI Scheme for Payment Requests

The purpose of the URI scheme is to enable users to easily make payments by simply clicking links on webpages or scanning QR Codes.

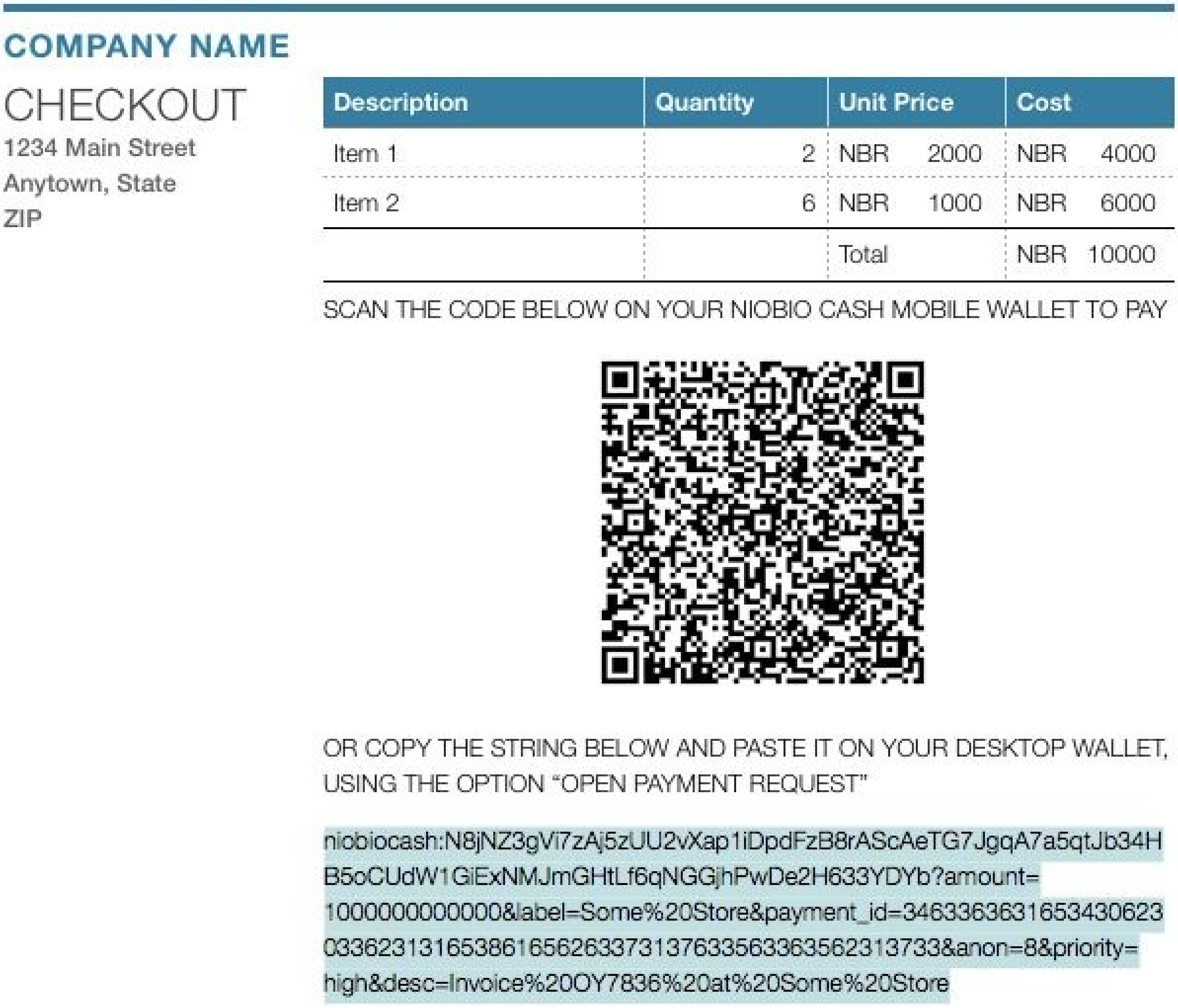
Usually, QR codes generated to be ingested by mobile wallets contain only the destination address of the payment. This requires the user to fill all other information such as amount, fee, and payment id.
Niobio Cash implements a way to encode a full payment request into the QR code. A regular payment request is a string containing the information of the receiver and the payment amount, among others included by the Niobio Cash improvement. An example of a payment request looks like this:

```
niobiocash:↵
N8jNZ3gVi7zAj5zUU2vXap1iDpdFzB8rAScAeTG7JgqA7a5qtJb34HB5oCUdW1GiExNMJmGHtL
f6qNGGjhPwDe2H633YDYb?↵
amount=1000000000000&↵
label=Some%20Store&↵
payment_id=3463363631653430623033623131653861656263373137633563363562313733&↵
anon=8&↵
priority=high&↵
desc=Invoice%20OY7836%20at%20Some%20Store
```

The string is broken into many lines to make it easier to read, but they all fit into one line.
The destination address is put right after the prefix ***niobiocash:***. Following the basic format a complete set of parameters can be used to enrich the experience of the customer using a desktop, web or mobile wallet:

- *amount*: Amount of base Niobio Cash units;
- *label*: Label for that address (e.g. name of receiver);
- *payment_id*: Payment ID in hexadecimal format;
- *anon*: Anonymity level;
- *desc*: Message that describes the transaction to the user;
- *priority*: Priority of the transaction. It can be used values "low", "medium" or "high", with progressively higher fees. Actual values of the fees is a choice of client implementation.

The payment request string can be copied and pasted on the desktop or web wallets or can be used to generate a QR code to be scanned by a mobile wallet.
A basic checkout page for an e-commerce or a point of sale can follow the example below.



COMPANY NAME

CHECKOUT

1234 Main Street
Anytown, State
ZIP

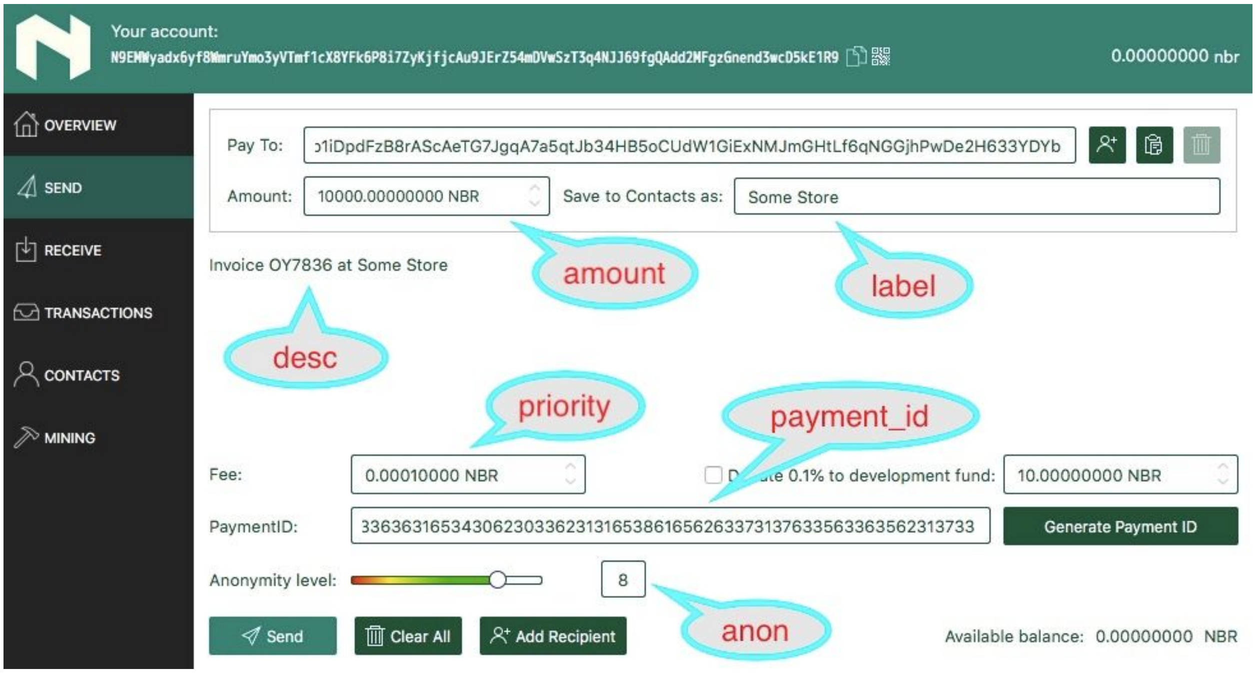
Description	Quantity	Unit Price	Cost
Item 1	2	NBR 2000	NBR 4000
Item 2	6	NBR 1000	NBR 6000
		Total	NBR 10000

SCAN THE CODE BELOW ON YOUR NIOBIO CASH MOBILE WALLET TO PAY

OR COPY THE STRING BELOW AND PASTE IT ON YOUR DESKTOP WALLET, USING THE OPTION "OPEN PAYMENT REQUEST"

```
niobiocash:N8jNZ3gVi7zAj5zUU2vXap1iDpdFzB8rAScAeTG7JgqA7a5qtJb34H
B5oCUdW1GiExNMJmGHtLf6qNGGjhPwDe2H633YDYb?amount=
1000000000000&label=Some%20Store&payment_id=3463363631653430623
0336231316538616562633731376335633635623137733&anon=8&priority=
high&desc=Invoice%20OY7836%20at%20Some%20Store
```

That way the user has no need to fill in any information. On a mobile wallet he just scan the code and click "Pay" or "Send" on his screen.
Here is a screenshot of the above payment request imported on a desktop wallet.



Your account:
N9EMWyadx6yf8WmruYmo3yVTmf1cX8YFk6P8i7ZyKjfjcAu9JErZ54mDVwSzT3q4NJJ69fgQAdd2MFgzGnend3wcD5kE1R9
0.00000000 nbr

Pay To: ɔ1iDpdFzB8rAScAeTG7JgqA7a5qtJb34HB5oCUdW1GiExNMJmGHtLf6qNGGjhPwDe2H633YDYb
Amount: 10000.00000000 NBR
Save to Contacts as: Some Store
Invoice OY7836 at Some Store
Fee: 0.00010000 NBR
□ Donate 0.1% to development fund: 10.00000000 NBR
PaymentID: 3363631653430623033623131653861656263373137633563363562313733
Anonymity level: 8
Available balance: 0.00000000 NBR

5. Niobio Cash Unique Features

A number of actions have been taken or planned by the developers and contributors of the Niobio Cash open source project.

5.1 Entrepreneurship Environment

One of the main goals of driving project development is the incentive for independent initiatives to create business related to the Niobio Cash blockchain.

5.1.1 Community's Incentive and Support

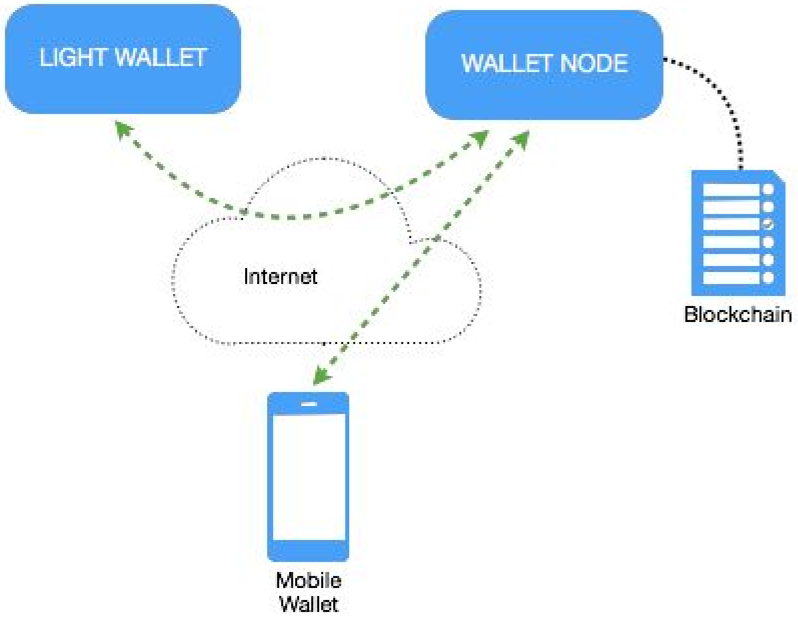
A considerable effort is made to enhance tools and provide resources to connect and interact with Niobio Cash blockchain, making it easier for developers and merchants to create their business and applications. It is given broad disclosure about the policy of the project to increase entrepreneurship around it.
The team provides free technical support, accept requests for new API endpoints, and disseminate new ideas that can be developed by anyone.

5.1.2 Wallet Nodes

Smartphones' wallets and desktop users with poor Internet connection need to obtain data from the network while it is impractical to them to download the full blockchain.
Wallet Node is a special use of full nodes which provide data for light wallets. Light wallets are those wallets without a local copy of the blockchain. They can be desktop wallets or mobile

wallets. A Wallet Node provider helps the network to attend those kinds of wallets, giving the owner of the Wallet Node the option to charge a fee for his service.

The figure below illustrates the functional environment of a Wallet Node.



A Wallet Node is essentially a full node with a special purpose. The ability to charge a fee from the connected wallets, when they make a sending transaction, is activated through a pair of command line options. There is an upper limit for the fee charged, per transaction.

It is essential to encourage community-based entrepreneurship, attracting players to become a Wallet Node provider, monetizing from their service and expanding network capacity so it can support the growing number of mobile wallets.

5.2 Contribution to Society

Collecting funds from a fee on block reward, the Niobio Cash projects has the goal to connect cutting edge technologies with blockchain innovation, bringing economic and social progress to Brazil. These funds will be directed to researchers in Brazilian natural resources, such as Niobium.

The project also contributes to the local economy, as a generator of opportunities in entrepreneurship around the blockchain technology.

5.3 eSignature Platform

Seeking for decentralization in services that are traditionally centralized, the Niobio Cash project is implementing a system to certify the authenticity of documents in its blockchain. Documents such as certificates and diplomas could be validated against his checksum included in transactions on the blockchain. A university, for example, would publish their alumni diplomas on their systems, generating their checksum and including the hash on a transaction, signed with their GPG key. When a contractor receives a diploma or certificate from former alumni, it will be possible for him to easily verify its authenticity using a web interface.

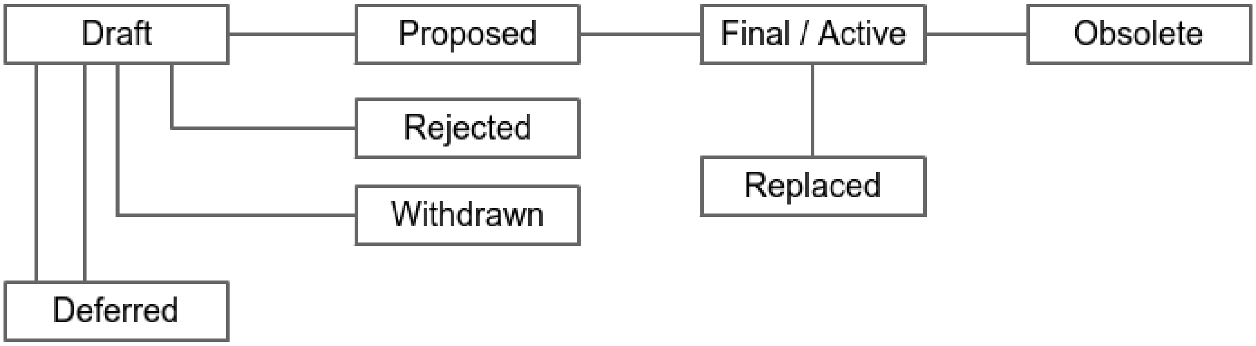
6. Enhancement Tools and Processes

6.1 NCIP - Niobio Cash Improvements Proposals

A Niobio Cash Improvement Proposal [NCIP0001] is a design document providing information to the Niobio Cash community, or describing a new feature for Niobio Cash or its processes or environment. The NCIP should provide a concise technical specification of the feature and a rationale for the feature.

NCIPs will be the primary mechanism for proposing new features and documenting the design decisions that have gone into Niobio Cash. The NCIP author is responsible for building consensus within the community and documenting dissenting opinions.

The typical paths of the status of NCIPs are as follows:



6.2 Bug Bounty Program

Developers are encouraged to contribute by finding and fixing bugs and vulnerabilities on Niobio Cash source code. In return, a reward is offered in units of Niobio Cash cryptocurrency. The amount of the rewards is variable, according to the complexity of the solution, and the potential impact of the error or vulnerability found.

The program includes the core daemon code, the wallets for desktop and command line, and the RPC wallet.

6.3 Project Based Reward Program

This rewards program is project based. It is focused on developing new applications or platforms around Niobio Cash, or even new features for the core code or wallets.

Its goal is to expand the usability of the cryptocurrency, reaching a broader range of users and segments of economic players.

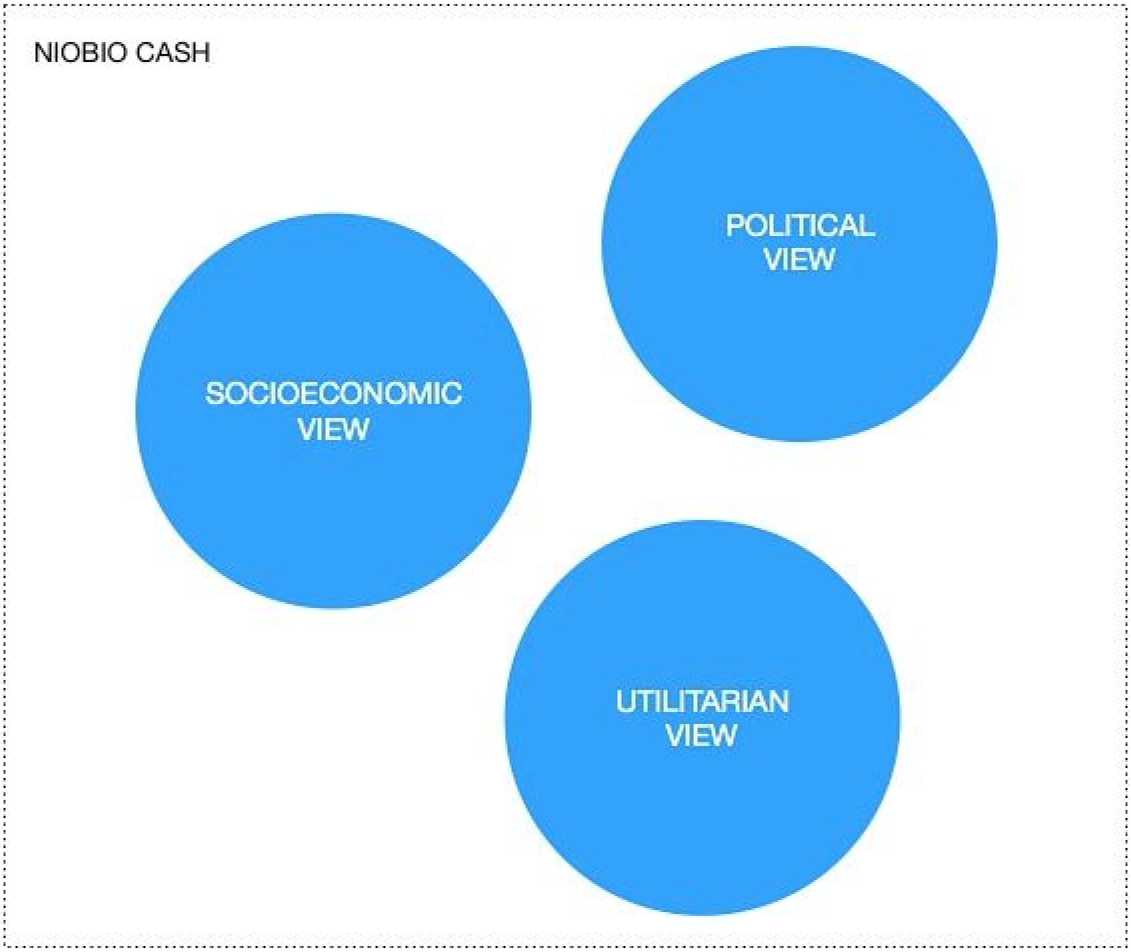
Freelance developers and companies can apply for these projects. The candidates will set the minimum amount in Niobio Cash units they are willing to accept to deliver them. On the other side, users will donate for their preferred projects, in a crowdfunding model. Once the minimum amount is reached the project will be kicked off, and the coins collected will be transferred once the final milestone is delivered.

Projects not able to collect the minimum amount on a certain period of time, informed on the project's definition, will be declined and the coins already collected will be distributed evenly between the other still active, but not started, projects.

A percentage of the collected coins will be deduced before being transferred to developers or companies. This fee will be used to pay the costs of the voting platform and will be clearly informed on the web site and social media.

7. Final Considerations

Niobio Cash is a base system driven by three different visions that give sustentation to each other, representing its political, socioeconomic and utilitarian views of what this project wants to add and contribute to the growth of society.



Utilitarian View: As almost cryptocurrency, Niobio Cash is providing tools to make it an easier way of payments. The project seeks improvements in usability and user experience. Progress has been made to mobile interaction between customers and merchants, such as improved QR Code system, and integrated wallet across most popular social media - Telegram, Twitter, Instagram, and Facebook.

Socioeconomic View: This is the vision of the project for the entrepreneurship around the Niobio Cash ecosystem. The APIs are getting enhancements and new methods to respond to e-commerce integration the way current developers are used to doing with other traditional payment systems. This allows a smooth and short learning curve, faster and safer implementations as a result. Ideas are constantly discussed on the community, where skilled

people can embrace them and create a business. This already happened and some companies were founded on the basis of Niobio Cash. The technical team provides full support and knowledge without any costs for who wants to become a entrepreneur.
On this pillar it is also included the so called *give back*. It's a small action to provide some return to the society from the wealth being generated from the community work. A fund is planned to be designated to projects focused on scientific researches, specially those bounded to natural resources from Brazil.

Political View: This is the vision of how Niobio Cash project can project the image of the country globally. The intention is to bring and develop knowledge on blockchain technology locally, making Brazil a protagonist of the upcoming revolution provided by technology together with the political changes on financial system brought by Satoshi's initiative. This cannot be done by a single project or team, so the most effort should be on bringing attention of developers and help them understand the technology, increasing the overall skills from brazilian community of developers.

8. References

[NB01] Niobium: Wikipedia, https://en.wikipedia.org/wiki/Niobium

[NCIP0001] - Niobio Cash Improvements Proposals: NCIP 0001, NCIP Purpose and Guidelines, Helder Garcia, https://github.com/niobio-cash/ncip/blob/master/ncip-0001.mediawiki

[NCIP0007] - Niobio Cash Improvements Proposals: NCIP 0007, Reduction of Emission Speed Factor, Helder Garcia, https://github.com/niobio-cash/ncip/blob/master/ncip-0007.mediawiki

[LWMA] - Linearly Weighted Moving Average: LWMA difficulty algorithm, *zawy12*, https://github.com/zawy12/difficulty-algorithms/issues/3

9. Document Versioning

Version 1	November 2017	Soldati, Marconi DeSousa, Carlos
Version 2	February 2019	Garcia, Helder Villani, Frederico