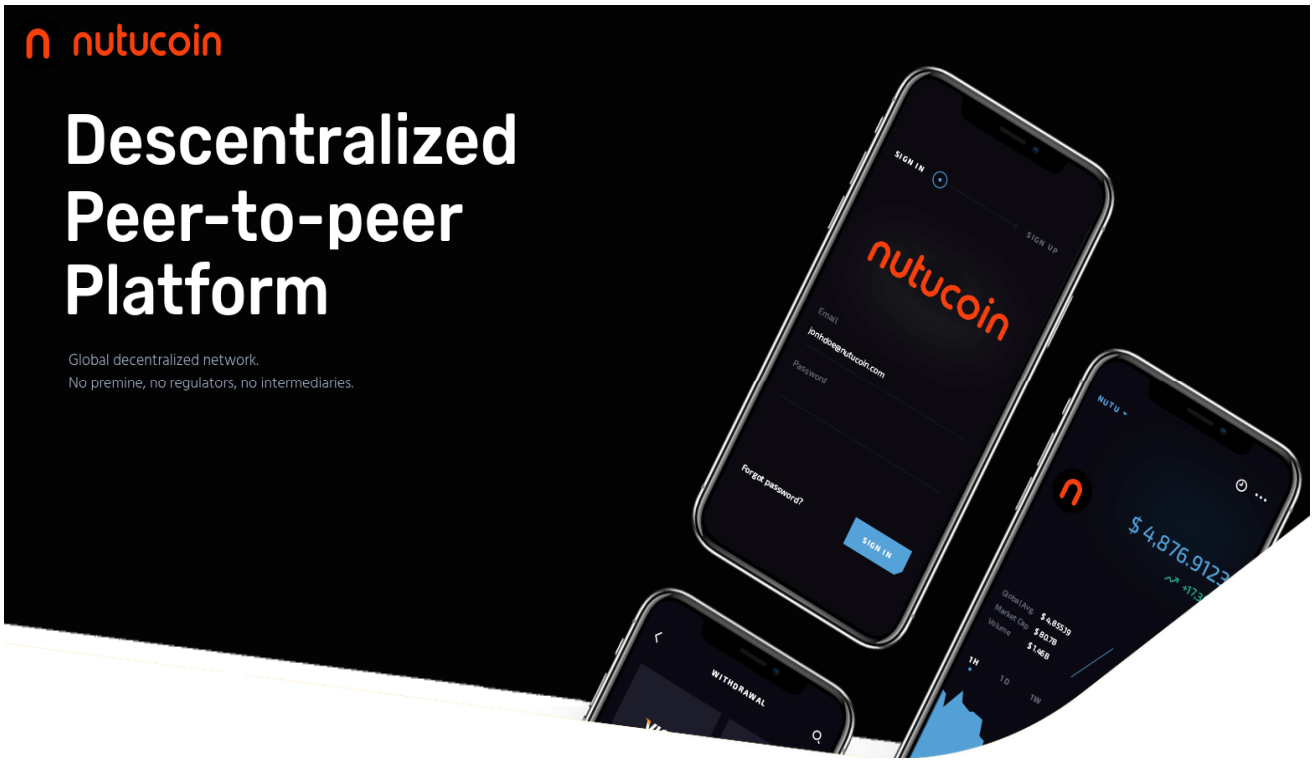

White paper

(Version 1.0)

Content

1) Introduction

In 2008, the world was going through a global financial crisis. A lot of actions were taken to save the economy. Most of them were led by the governments and the banks. This led to lost their credibility from the public. By the end of that year, a mysterious crypto man, named Satoshi Nakamoto, had a vision that would forever change the way we understand the economy. He published a Bitcoin white paper "*Bitcoin: A Peer-to-peer Electronic Cash System*" for the first time.

His vision soon proved to be a viable solution for various present-day economic issues. The magnitude of this innovation proved to be so powerful that it could transfer the power from the hands of government-controlled and centralized institutions into the hands of the people. A new and decentralized governed economic system became a reality that many hope to be implemented. Today, we are all progressively witnessing the miracle of that vision becoming true, as more and more people as well government backed companies/industries have expressed interest in the blockchain industry and in its decentralized governance.

Blockchain technology will not replace jobs or make life harder. The technology is here to simplify life. This technology will make life easier and more secure, with the backing of trusted certified information.

The world is undoubtedly evolving, and we need to actively keep up with the times and the emerging technological advancements that structure our lives. Blockchain technology can be applied in everything, from the way we store and process data, the way we see a movie, the way we listen to the music, the way we communicate with each other, even the way we shop, etc.

2) Age of Nutucoin

Understanding the need of bringing Blockchain technologies into real life, a group of developers, designers and administrators gathered together and launched **NutucoinV2** (hereafter called **Nutucoin** or **Nutu** or **NTU**), a new blockchain project with ultimate aim *'make life easier'*.

3) Blockchain features

3.1) Proof of Work consensus

The main reason that Nutucoin chooses Proof of Work (PoW) consensus is to make sure that miners don't cheat. It will be expensive for a malicious miner to attack the network. If a miner attempts to attack the network, they still have to consume lots of electricity, but they will have no way to pay that electricity off.

There is no way to trust that everyone in the network is honest. So, there has to be some way to prevent miners from creating new blocks that benefit themselves. The way it works is that you have a bunch of people all trying to guess the answer to the math problem and no one knows who is going to get the correct answer first. Whoever does get the right answer first gets a reward, but only if all the other miners agree to accept that transactional record (If it becomes apparent that a certain miner is creating fraudulent transactions then the other miners can collectively refuse to accept their contributions).

This is why the process of creating a new block is designed to be energy intensive, so that there is a cost associated with creating each new block. This prevents miners from simply creating a whole bunch of new fraudulent blocks with the hopes that maybe they'll get accepted, because the cost of doing so offsets the potential reward. It helps to think about proof of work as a possible solution to email spam. If there was a requirement for each computer to spend a minute on a PoW problem before every piece of mail was sent, then only people with genuine messages would agree to expend the effort. One minute of computer time is a very low cost for an individual, but the guy who is blasting 10 million spam emails couldn't afford to wait 10 million minutes to do so.

So going back to Nutucoin, the chance of each individual miner being the one to solve each block is pretty small, and since it takes a lot of effort to solve the blocks they can't just spam the network with solutions. This means that they are incentivized to only expend the effort if their contribution is going to be accepted by the network.

3.2) ASIC resistance

ASIC stands for Application-Specific Integrated Circuit. They are designed to execute only one task, but they do it as well and effectively as possible. Therefore, they have high computing power. They

bring more profit than GPUs and also take up most of the network hash rate. It causes risks of coin centralization when the power is concentrated in the hands of the limited number of users.

In order to stop ASICs from dominating the network and to secure Nutucoin blockchain better, X16RV2 is chosen. X16RV2 is an algorithm invented by Ravencoin developers. It is the combination of 17 different algorithms, including BLAKE, BMW, Groestl, JH, Keccak, Skein, Luffa, Cubehash, Shavite, Simd, Echo, Hamsi, Fugue, Shabal, Whirlpool, SHA512 and Tiger.

Each algorithm is assigned a number or a letter according to the following table:

Table 1: Number/Letter and algorithm mapping

Number	Hashing algorithm
0	BLAKE
1	BMW
2	Groestl
3	JH
4	Keccak
5	Skein
6	Luffa
7	Cubehash
8	Shavite
9	Simd
a	Echo
b	Hamsi
c	Fugue
d	Shabal
e	Whirlpool
f	SHA512

Tiger algorithm is not assigned a specific number or a letter, but it is used in three different parts of X16RV2. It will be executed before the Keccak (4), Luffa (6), and SHA-512 (f) algorithms.

Table 2: The combination of Tiger algorithm with other hashing algorithm

Number	Hashing algorithm
0	BLAKE
1	BMW
2	Groestl
3	JH
4	Tiger first; Keccak after
5	Skein
6	Tiger first; Luffa after
7	Cubehash
8	Shavite
9	Simd
a	Echo
b	Hamsi
c	Fugue
d	Shabal
e	Whirlpool
f	Tiger first; SHA512 after

The order is changed depending on the hash of the previous block. The output of current block becomes the block input of the next block - leading to a new order in mining algorithms. The last 16 characters of the previous hash block determines the order of the next hashing sequence.

Let's take the example of Nutucoin hash at the block 10:

"7675d5e8ba85c5b175d583cb9c8edc82b785362d21e5c86a**e13f36437b9e3150**"

The last 16 characters of the above hash is **e13f36437b9e3150**. So, the next block sequence will be:

Whirlpool(e) -> BMW(1) -> JH (3) -> Tiger first; SHA512 after (f) -> JH(3) ->Tiger first; Luffa after (6) -> Tiger first; Keccak after (4) -> JH (3) -> Cubehash (7) -> Hamsi (b) -> Simd (9) -> Whirlpool (e) -> JH (3) -> BMW(1) -> Skein(5) ->BLAKE(0)

3.3) Nutucoin Difficulty Retargeting System (N-DRES)

In Bitcoin, the standard block difficulty readjustment is set to adjust only every 2016 block. The problem with this scheme is that it gave rise to multipool mining. Multipool mining is a process of jumping from one crypto to another most profitable one at that moment. Then, the miners dump the mined coins to buy back Bitcoins. True, this actually happened back then when the price of Bitcoin Cash (BCH) arose .

Miners will only focus on economic incentives. When BCH becomes more profitable, miners almost abandon Bitcoin network to mine BCH. Once BCH adjusts its difficulty, miners will then jump back to mine Bitcoin. People think that it is 51% attack, but it's actually nothing. It is a seesaw of hashing power being delivered between Bitcoin and Bitcoin Cash based on their profitability. This is a serious problem with Bitcoin, but it gave the birth of Nutucoin Difficulty Retargeting System (N-DRES), the in-house algorithm developed by Nutucoin developers.

N-DRES will adjust difficulty every block using information from the previous blocks. It uses multiple exponential moving averages and a simple moving average to achieve the smoother difficulty re-target mechanism. N-DRES is immune from multipools as it retargets difficulty every single block. Besides, N-DRES will make blockchain more and more secure, make block time more and more consistent, make transactions faster and faster, make miners attracted more and more, make blockchain more and more reliable, etc.

3.4) Anti-quantum computers

Besides being immune from multipools, N-DRES is designed to resist quantum computers or a sudden spike in the network hash rate. This means that if suddenly there are any quantum computers or huge hash rates on Nutucoin network, a NTU block cannot be mined faster than 90% of the block time (around 135 seconds). Therefore, it will be fair enough for all participants in the network and it will make quantum computers or huge network hash rate unable to get any benefits from its advantage over other miners.

3.5) SegWit

SegWit is short for Segregated Witness. It was the biggest Bitcoin protocol upgrade to date, which wrapped several improvements and fixes into one. Nutucoin developer applied this kind of protocol (SegWit) at the time of their blockchain starting.

It got rid of transaction malleability. It solved this problem by moving the “witness” data of a transaction, which includes the signature, to a new part of a blockchain block. As such, it paved the way for the Lightning Network and other layer two protocols, which will be implemented in Nutucoin blockchain in the future.

Besides, SegWit also offered a modest block size limit increase to a theoretical four megabytes, or a more realistic two megabyte limit, depending on the types of transactions included in blocks. This means that users with SegWit-supporting wallets pay lower transaction fees.

3.6) Hierarchical Deterministic Wallet (HD Wallet)

A standard cryptocurrency wallet is used to store the cryptocurrency tokens or coins. It has a public address which an user can give to others to receive funds from them, and a private key which an user uses to spend the stored tokens or coins.

This public and private combination mechanism ensures safety of the cryptocurrency tokens or coins but comes with an additional overhead for users. Whenever, they generate a random pair of private and public addresses (or keys), they must back up their new pair of addresses. As the number of transactions increases, this process becomes cumbersome for the user.

HD Wallets solve this problem by deriving all the addresses from a single master seed (hence the name hierarchical). All HD wallets use a variant of the standard 12-word master seed key, and each time this seed is extended at the end by a counter value which makes it possible to automatically derive an unlimited number of new addresses.

HD wallets eliminate the need for the user to constantly generate and wait for the secure keys to be generated, so they only need to worry about taking the backup.

3.7) Block Pruning

The Nutucoin blockchain data contains all transaction history from the day Nutucoin was created to till date. With 4MB block size maximum and 2.5 minutes block time, the size of the chain will grow larger and larger. Hence the storage capacity needed to run a full node will keep increasing in the future.

In order to overcome this issue, Nutucoin developer implemented block pruning. Block pruning allows users to run a smaller version of full blockchain. It does this by deleting the older data that it no longer requires while downloading the latest blockchain. Running wallet in prune mode simply throws away previous transaction and old chain history which in turn saves disk space.

Before users can start to prune Nutucoin blockchain, they will still need to download the entire transaction history up to that point, after which the reduction in storage can begin. At the current maximum block size of 4MB per block, block pruning would take up 2200MB (around 2.2GB) of hard disk space. Doing so would make older hard drives, or even SD cards and usb sticks a potential viable alternative to store the blockchain.

4) Coin Specification

Nutucoin network started at block ‘0’, with an amount of 4.325.000 NTU in circulation, representing the amount of coins that were already mined in NutucoinV1. The coins were spread among the miners who supported the network prior to this fork. Each miner received the exact same amount of coins that he owned before the fork.

Table 3: Nutucoin specification

Specification	Value
Total Blocks	10,000,000 (around 13,477,606 NTU)
Swapping Number	4,325,000 NTU (Coins mined before the fork to Nutucoin)
Block Size	4MB (Max)
Block Time	150s
Reward	6 NTU, reduce 10% each year, no reduction when it reaches 0.4 NTU
Dev fee	0% dev fee for 1st year; 10% reward after 1st year
Port	49638
RPC Port	49639
Legacy Address start with	N
p2sh-segwit address start with	S
Bech32 address start with	BN
Private key start with	P or Q

Example:

+ **Year 1**: 6 NTU per block from which 0.000 NTU will serve as Dev fee; the miner will get 6 NTU
+ **Year 2**: 5.4 NTU per block from which 0.540 NTU will serve as Dev fee; the miner will get 5.4 - 0.54 = 4.86 NTU
+ **Year 3**: 4.86 NTU per block from which 0.486 NTU will serve as Dev fee; the miner will get 4.86 - 0.486 = 4.374 NTU
+ etc…

5) Dev fee allocation

Dev fee will be automatically activated after the first year with 10% deduction from miner's reward. The allocation for Dev Fee is as follows:

+ **30%**: the reward for founders.
+ **30%**: used to build the Nutucoin blockchain and other product features related, which includes team recruiting, training, and the development budget.
+ **30%**: used for Nutucoin branding and marketing, including continuous promotion, advertisement activities, etc.
+ **10%:** kept in reserve to cope with any emergency or unexpected situation coming up.

6) Nutucoin application

6.1) Overview

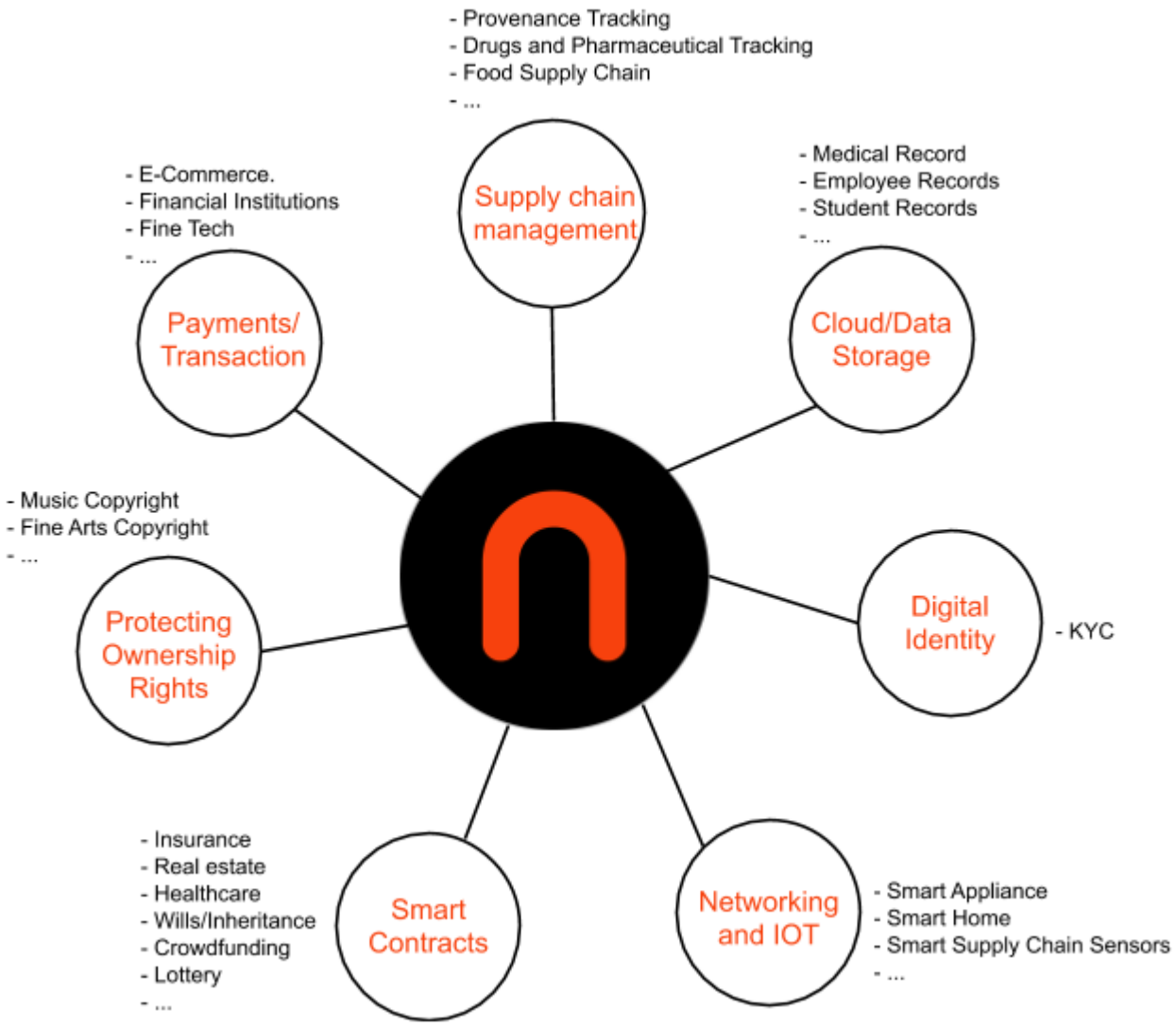

Figure 1: Overview of Nutucoin application

6.2) Remaferpa

Remaferpa, a logistics company in Brazil, and Nutucoin agreed to forge a partnership that would record all their data onto Nutucoin Blockchain. By this way, Remaferpa data can be accessed whenever they want on a secure blockchain without the risk of ever losing it. 100% transparency information about every truck and employee's activities in a cost-efficient way will be displayed clearly for Remaferpa and their partners. This will help not only to reduce unnecessary costs, but also to maximize their profits.

Besides, Nutucoin is planning on introducing a payment method feature into their application, Remaferpa 360, which uses Nutucoin as a payment currency for their services.

7) Nutucoin wallet

In order to fulfill rapid customer's need change, Nutucoin will support following cross-platform wallets:

- Desktop wallet
  - ü Windows OS.
  - ü Linux OS.
  - ü Mac OS.
- Android Mobile wallet
  - ü Light version.
  - ü Full node version.
- iOS Mobile wallet
  - ü Light version.
  - ü Full node version.
- Web wallet
- REST API

The initial release will be the English version. More languages will be added over time.

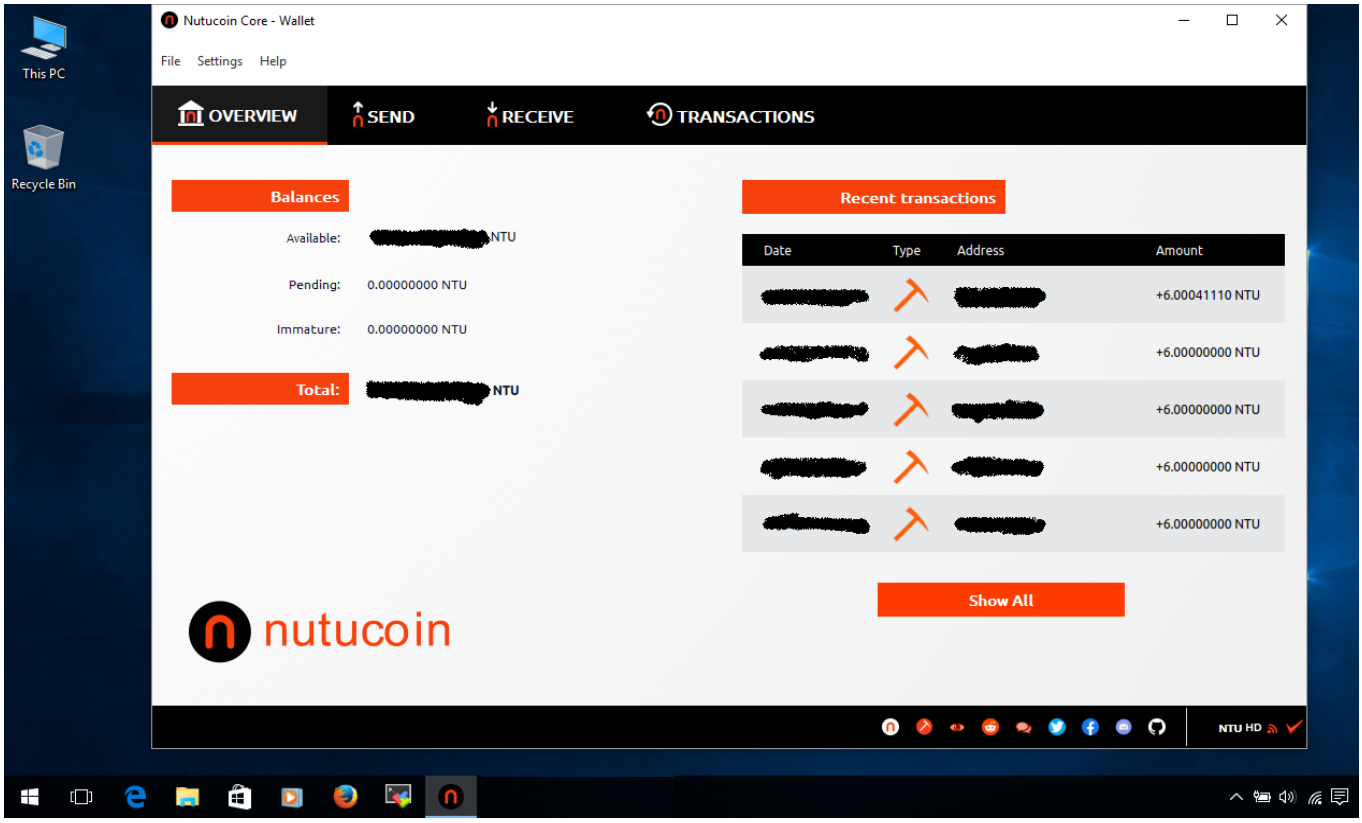

Figure 2: Nutucoin Desktop wallet on Win 10

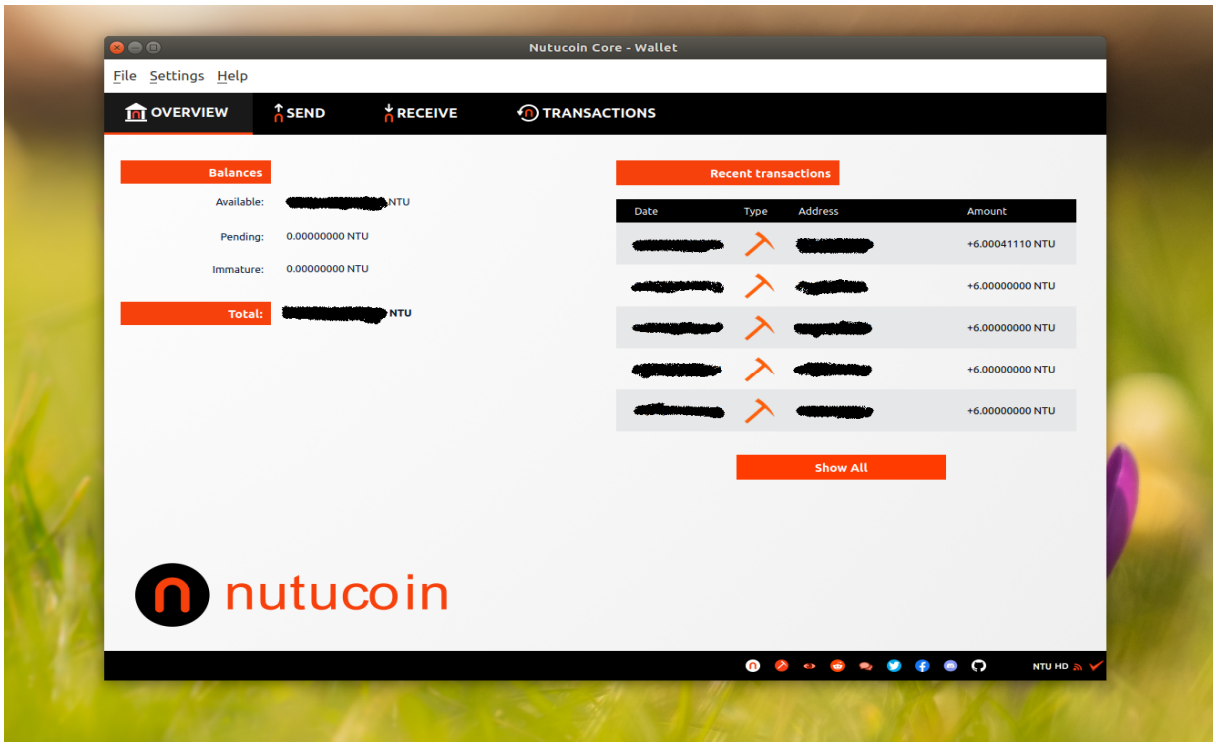

Figure 3: Nutucoin Desktop wallet on Ubuntu 18

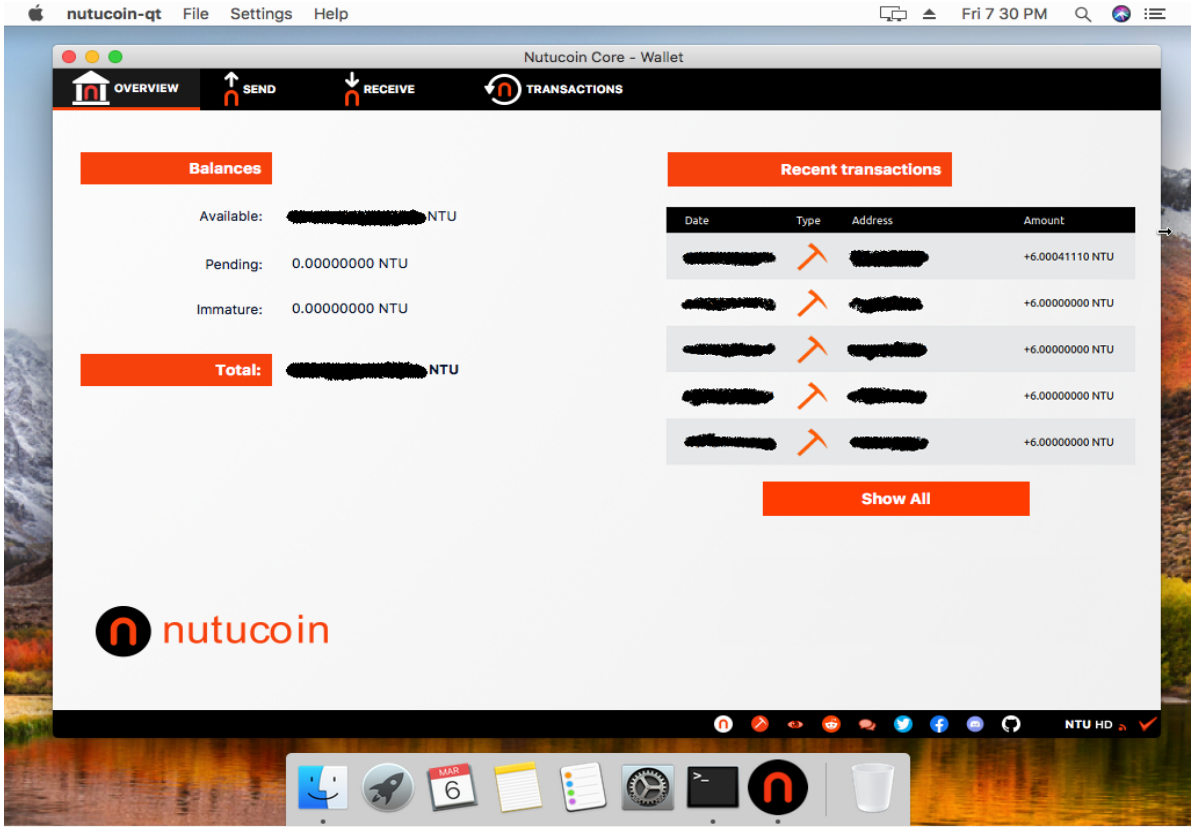

Figure 4: Nutucoin Desktop wallet on Mac OS 10.13 High Sierra