NulleX Whitepaper 1.0

February 2018

NULLEX

The technical notes represented on the following pages are intended to describe and officially document the concepts behind NulleX Blockchain. This document provides and explains in detail the technical aspects of the **Null Protocol** which will power the 'First zero-trace financial privacy ecosystem' and other key features which are core areas of the project.

INTRODUCTION

When Blockchains were first introduced one of the main features intended was to achieve a degree of privacy in order to protect the identities of the sender and the receiver whilst performing online transactions. We have been exploring this area for a while now and although we have different market solutions that offer a good degree of anonymity we are actually not yet able to completely eliminate the most important aspect that matters to privacy which is the ability to eliminate any online trace. When we say to 'eliminate' we mean to completely remove any possible trace and not hide or cover up with layers of protection. We believe that in order for a 'Privacy Coin' to be considered a completely private financial ecosystem we need to be able to offer to our users the possibility to execute transactions without the worry of having their financial history being analyzed. The main issue with modern privacy coins is that during the transaction process the coins mix with a larger set of coins available for mixing and this causes the output to be difficult to track back to the source. Having said that no matter how many layers of obfuscation and mixing we apply there is always a way to work back and audit through the transactions in order to trace the sender and receiver.

TECHNICAL NOTES

The Solution to total privacy called 'The Null Protocol'

In order to overcome the issue of achieving total privacy & therefore not leaving any online trace we offer a solution known as the **Null Protocol**. Some of the currently available anonymity engines reveal the TX participant to others and the amount which has been transacted, some don't allow an auditable supply but all of them place the transactions at a certain time therefore leaving an online trace. Can this also be eliminated? The concept behind the **Null Protocol** is that the coins received from a sender are completely freshly minted and therefore there is no trace or history left behind. This concept offers to the sender/receiver a scenario of total privacy and anonymity. The coins received are brand new and freshly minted which means that no one will be able to know where they came from. This process will ensure an extremely safe degree of confidentiality through a strong mathematical guarantee to the sender/receiver since new minted coins will have no previous online or digital trail whatsoever.

The **Null Protocol** is composed of three main layers - The Null Blockchain, the Null Array and the Null Applications. The Null Blockchain allows the user to transact securely and privately while leaving no auditable trace. The Null Array is a large and global network composed of Null Array Verifier (NAV) nodes. NAV nodes are network nodes spread around the world that offer unique services to the NulleX network and are compensated for their services directly by the network. Null Application (NApps) are decentralized, anonymous and self-executing applications that leverage the Null Protocol to register user participation, manage permissions and relay usage data across the network in an anonymous, zero-trace way.
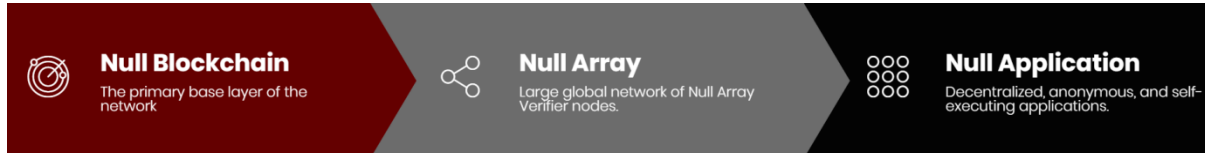

The Null Blockchain

The Null Blockchain allows the user to transact securely and privately while leaving no auditable trace. The primary base layer of the network, The Null Blockchain is a secure, decentralized and independently verifiable ledger used to store your finances and usage data. Using a unique cryptographic solution called Null Protocol, data can be stored and accessed by its owner and verified by the network, while keeping the data hidden from the rest of the world.

The Null Array Verifier

The Null Array is a large global network composed of
Null Array Verifier (NAV) nodes. NAV nodes are
network nodes spread around the world that offer a
unique service to the NulleX network and are
compensated directly by it. These services include
the strict oversight of the destruction and minting
of NulleX coins to protect against financial
counterfeiting, enforcing the governance rules of the
NulleX network, maintaining the integrity of the
application layer, facilitating ultra-fast payments
between peers, voting on development proposals, and
others.
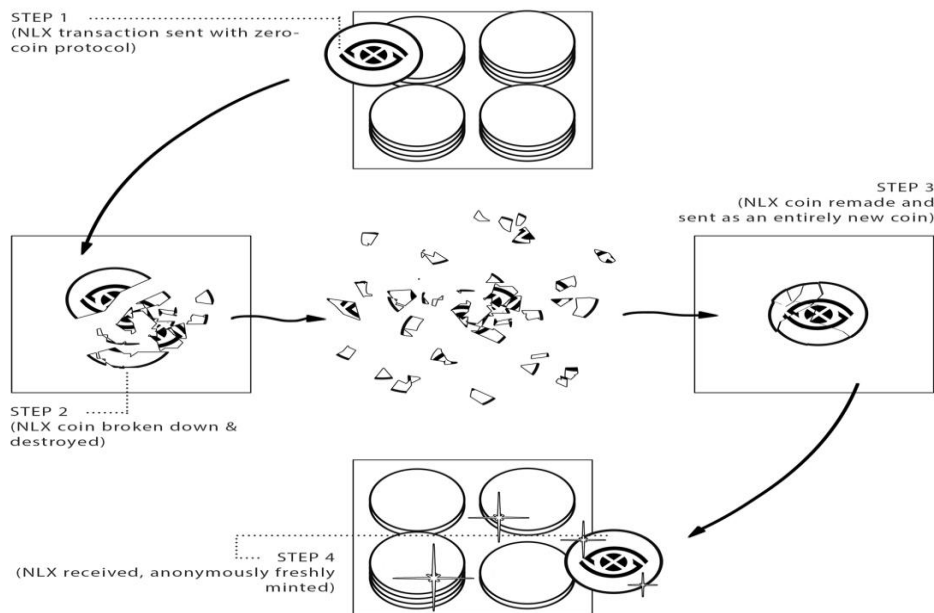
The Null Application

Null Applications (NApps) are decentralized, anonymous and self-executing applications that leverage the Null Protocol to register user participation, manage permissions and relay usage data across the network in anonymous, zero-trace scenarios. Use your favourite GPS app, message your friends and shop online without having to worry about anyone looking over your shoulder.

NULLEX TECHNICAL DATA
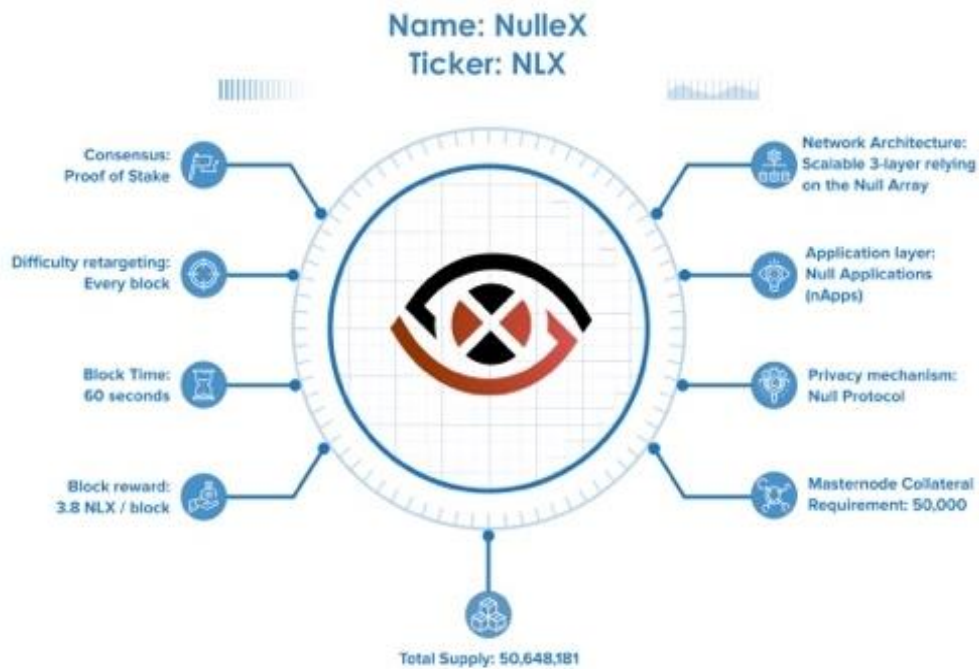
Consensus: POS (Proof of Stake)

Difficulty Retargeting: Every Block

Block Time: 60 Seconds

Block Reward 3.8 NLX/Block

Network Architecture: Scalable 3-layers relying on the Null Array

Privacy Mechanism: Null Protocol

Null Array Nodes (NAN) Collateral: 50,000

The Null Array Nodes (NAN)

A Null Array Node is a computer which processes transactions on a Blockchain and, as a result, is rewarded with coins for doing so.

The Null Array are nodes that run the same wallet software on the same Blockchain to provide extra services to the network. These services include coin mixing for increased privacy of transactions, instant transactions and a decentralized governance that provides a decentralized budgeting system with immutable proposal and voting systems.

For providing such services, Null Arrays are also paid a certain portion of reward for each block. This can serve as a passive income to the null array owners minus their running cost.

This is achieved by requiring a node owner to hold a certain amount of coins to ensure they have a vested interest in the Blockchain and thereby ensure they run their node in a responsible fashion.

In order to run a Null Array the requirement is of 50,000 coins. The Rewards will be 3.8 NLX every block for running a Null Array.

FUTURE PLANS

The NulleX Team in the upcoming months will focus on the release of the Null Array Nodes on the network by Q2 2018, at least one new Exchange listing within 2018, the implementation of ZeroCoin along with the Null Protocol on Testnet in Q4 2018 and the development of IOS/Android mobile wallets.

SUMMARY

The purpose of NulleX is to solve the privacy requirements that are demanded in the current financial Cryptocurrency/Blockchain industry which currently doesn't offer total privacy with a zero-trace scenario. Nullex application 'Null Protocol' will serve this purpose and will offer to users an environment where any transaction will not leave any online trace and therefore will achieve total anonymity.