NulleX Whitepaper 2.0

June 2018

NULLEX

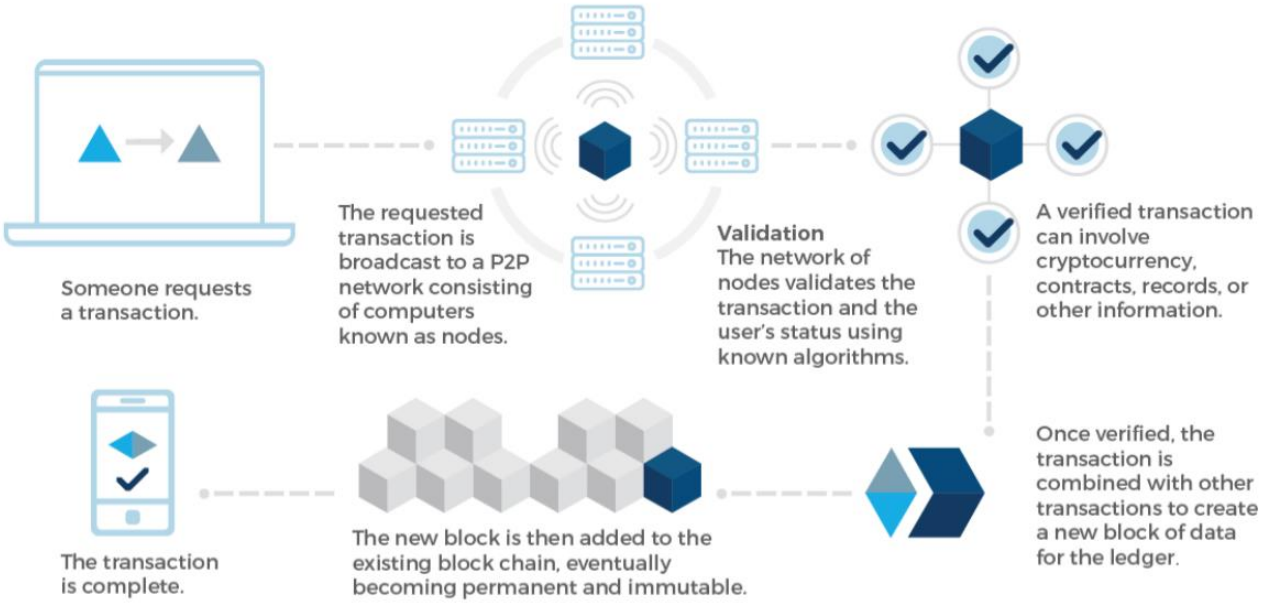
Legal Disclaimer

This white paper audits and analyzes certain aspects of The NulleX Core and its underlying Null Protocol, which will power the 'First zero-trace data privacy and protection ecosystem'. The white paper and the information stated herein is not legally binding and the white paper focuses exclusively on the activities of the NulleX Core Development Team and the function of The NulleX Core. This white paper does not constitute an offer of NulleX (NLX) nor an invitation for an offer to exchange any amount of NulleX (NLX). For a description of the risks associated with the NulleX Core Enterprise, please see the white paper section entitled 'Challenges'

Forward-Looking Statements: The white paper contains certain forward-looking statements. A forward-looking statement is a statement that does not relate to historical facts and events. The forward-looking statements are based on forecasts of future results and estimates of amounts not yet determinable or foreseeable. Such forward-looking statements are identified by the use of terms and phrases such as anticipate, believe, could, estimate, expect, intend, plan, predict, project, will and similar terms, including references and assumptions. This applies, in particular, to statements in this white paper containing information on future developments of NulleX Core or The Null Protocol, plans, and expectations regarding NulleX or its growth of value. Forward-looking statements are based on current estimates and assumptions that the author makes based on verified present knowledge.

ABSTRACT

NulleX is an open source Blockchain technology [1] focusing on Data & Information privacy. NulleX is based on the work of Satoshi Nakamoto, The Dash Team, and further the PIVX Team. [2] With that brings various improvements and outstanding base code to provide a two-tier incentivized network known as the Null Array. It uses a proof of stake protocol to secure the network through the use of Null Controllers, Null Arrays and autonomous NApps. This will all allow for near instant transmission of data and information & a permanent storage capacity all without a centralized authority.

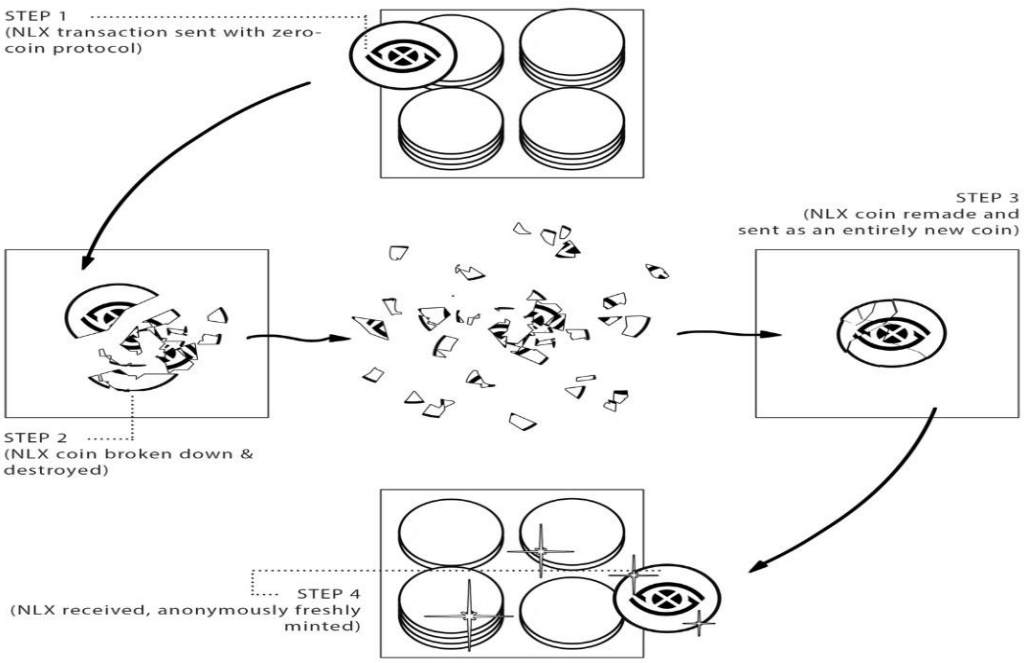


Introduction

When Blockchain Technology first emerged 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 there are different fundamental 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 Ecosystem' to be considered completely private we need to be able to offer to our users the possibility to transact on the network without the worry of having their history being analyzed. The main issue with modern privacy Blockchains is that during the transaction process the information mixes with a larger set of information available for mixing, which causes the output to be difficult to track back to the source. Having said that no matter how many layers of obfuscation, mixing, and encryption we apply there is always a way to work back and audit through the transactions in order to trace the sender and receiver of the data or information. To overcome this problem, the features outlined in this paper are being developed and implemented with the sole intention of ensuring and providing data protection and privacy in transmission and storage and creating BaaS [3].

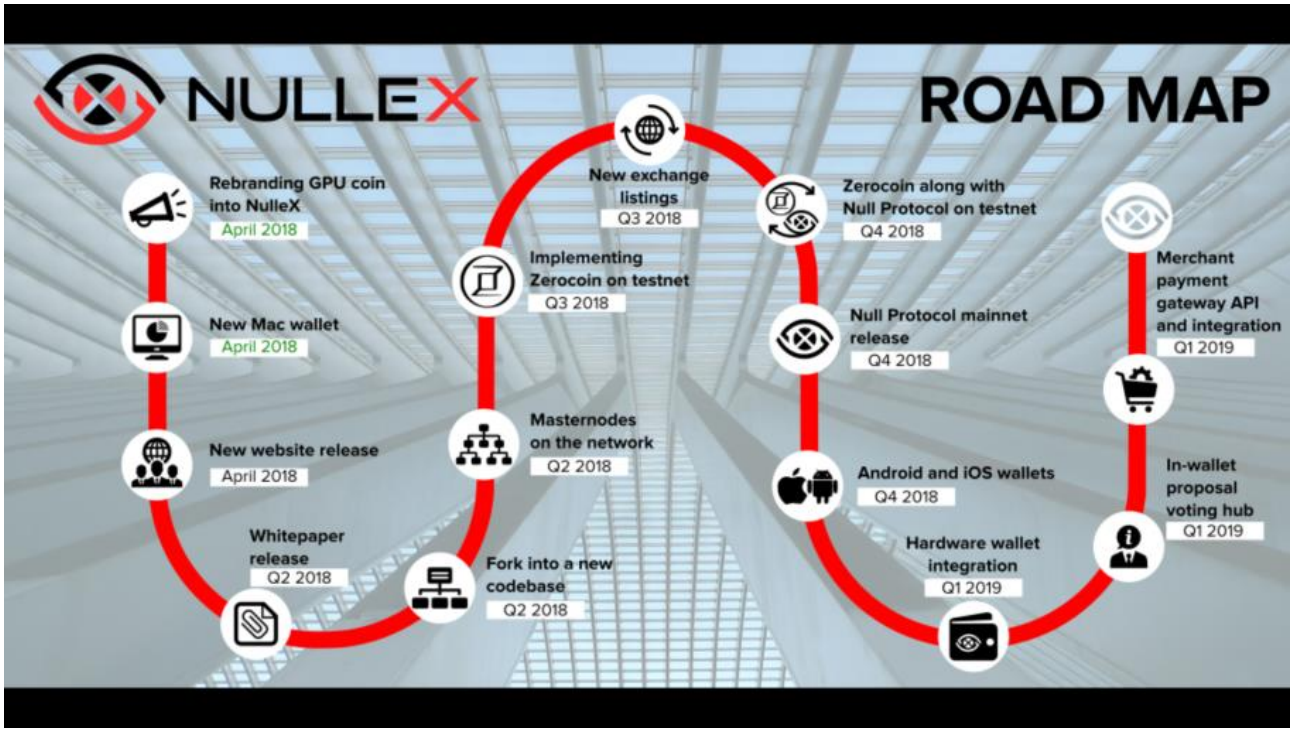
The Solution to total privacy called:
"The NulleX Core" & "The Null Protocol"

In order to overcome the issue of achieving total privacy & therefore not leaving any online trace we offer a Blockchain solution known as the "NulleX Core" & 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 and with an auditable amount therefore leaving an online trace. **Can this also be eliminated?** The concept behind the Null Protocol is that the coins/tokens or data 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 both the sender and the receiver since newly minted coins will have no previous online or digital trail whatsoever. The Null Protocol will allow for Data and information to be transmitted and stored anonymously.



NulleX Overview

The NulleX Network 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 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 an anonymous, zero-trace scenario.



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.

Null Controllers

To achieve consensus; Proof of Stake 3.0 (PoS) requires nodes running a wallet software proving that it has coins in the Blockchain in order to verify a block of transactions. The
Participating nodes receive an amount of blocks proportional to their stake per set period as a form of reward. This means that with lots of participating nodes (with roughly even amounts of coins) the network becomes very secure due to the increased difficulty of owning a majority of coins in the network.

Null Array Verifiers

Null Arrays are full nodes, just like in the Bitcoin network, except that they must provide a level of service to the network and have a bond of tokens to participate. Tokens are never forfeited and are safe while the Null Array is operating. This allows participants to provide a service to the network and earn tokens to be used along with the Null Protocol to transfer data or information. These nodes are very important to the health of the network. They provide clients with the ability to quickly synchronize and propagate the data throughout the network, whilst maintaining the integrity of the application layer.

The Null Applications

Null Applications (NApps) are decentralized, anonymous and self-executing applications that leverage the NulleX Network to register user participation, execute smart contracts, store information, manage permissions and relay usage data across the network in anonymous, zero-trace scenarios. Null Applications will play an important role for business data privacy & protection.

The Null Protocol

Currently in the development phase. The Null protocol proposes to serve as the link-layer to the Zerocoin [4] protocol to enable anonymous data transfer and storage. Achieved by complex formula that separates the TX, mixes the pieces of the TX, then reassembles the TX through portions of delivery over the coming blocks.

The data TX is segmented, destroying the original data TX, creating many new TX. It is then delivered to the Blockchain to begin consensus.

$$E = \left(\frac{C}{2^N}\right) * 1 + \left(\frac{2^N - C}{2^N}\right) * \left[\left(\frac{C_K}{2^{N_K}} * 1\right) + \left(\frac{2^{N_K} - C_K}{2^{N_K}} * \frac{N_K}{2}\right)\right] * K$$

Once several blocks [5] of consensus are achieved on the portions. They are distributed through the network based on current block sizes available. Calling on available NLX balances.

$$E_P = \frac{C}{|S|} * 1 + \frac{|S| - C}{|S|} * \left[\frac{C_K}{2^{N_K}} * 1 + \frac{2^{N_K} - C_K}{2^{N_K}} * \frac{N_K}{2}\right] * K$$

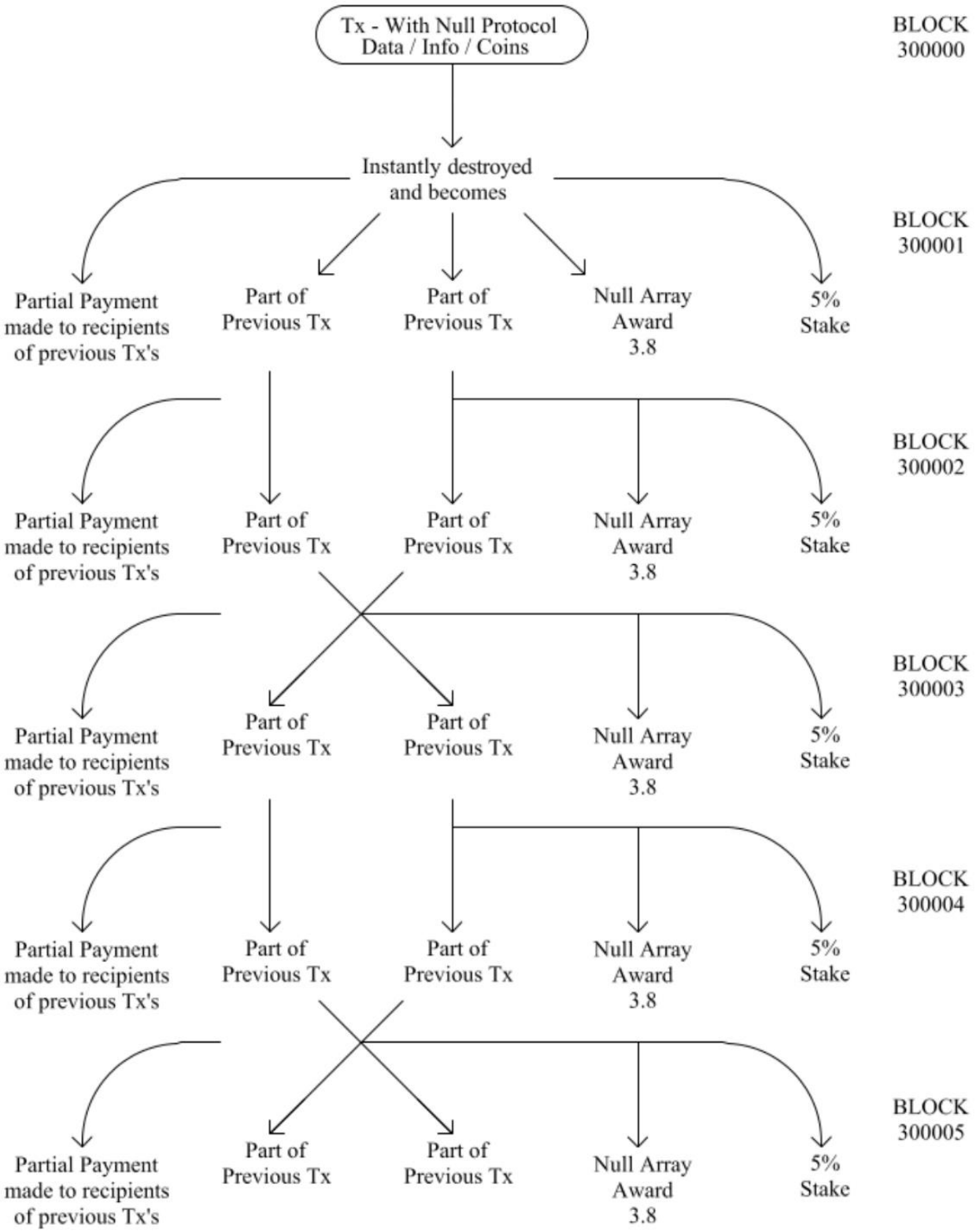
Once distributed the network will set to putting it back together.

$$E_{NP} = \left[\left(\frac{C_K}{2^{N_K}} * 1\right) + \left(\frac{2^{N_K} - C_K}{2^{N_K}} * \frac{N_K}{2}\right)\right] * K$$

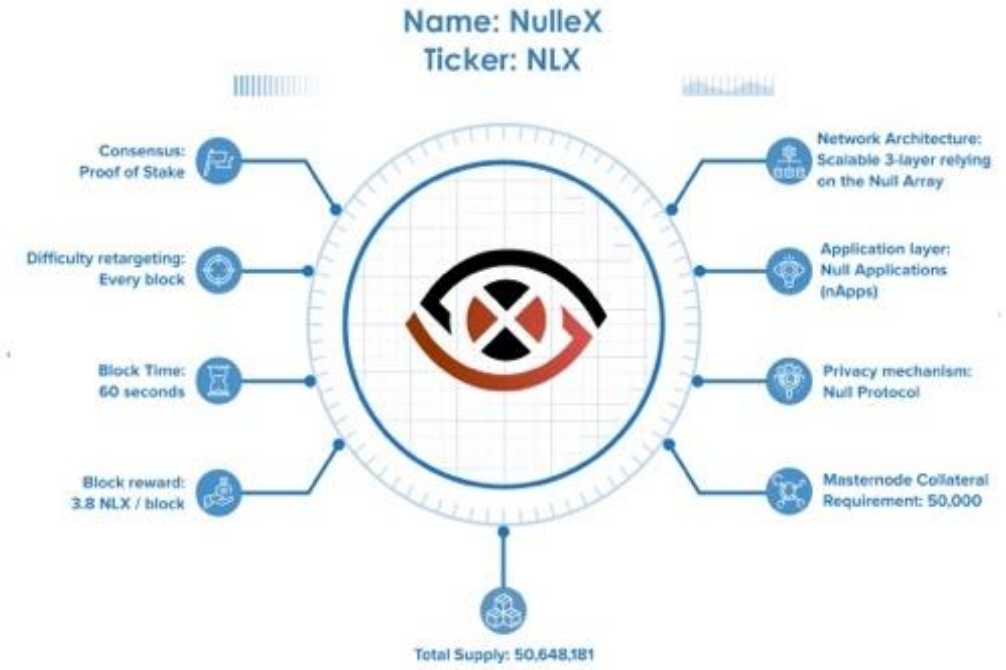
The network will deliver the portions to the receiver of the data TX over several blocks [5] with no single time-stamp or traceable output vs input.

Chain Control - Null Protocol

$$E = (1-p)\left[\left(\frac{C_K}{2^{N_K}} * 1\right) + \left(\frac{2^{N_K} - C_K}{2^{N_K}} * \frac{N_K}{2}\right)\right] * K +$$
$$p\left[\frac{C}{|S|} * 1 + \frac{|S| - C}{|S|} * \left(\frac{C_K}{2^{N_K}} * 1 + \frac{2^{N_K} - C_K}{2^{N_K}} * \frac{N_K}{2}\right) * K\right]$$


Tx - With Null Protocol Data / Info / Coins
BLOCK 300000
Instantly destroyed and becomes
BLOCK 300001
Partial Payment made to recipients of previous Tx's
Part of Previous Tx
Part of Previous Tx
Null Array Award 3.8
5% Stake
BLOCK 300002
Partial Payment made to recipients of previous Tx's
Part of Previous Tx
Part of Previous Tx
Null Array Award 3.8
5% Stake
BLOCK 300003
Partial Payment made to recipients of previous Tx's
Part of Previous Tx
Part of Previous Tx
Null Array Award 3.8
5% Stake
BLOCK 300004
Partial Payment made to recipients of previous Tx's
Part of Previous Tx
Part of Previous Tx
Null Array Award 3.8
5% Stake
BLOCK 300005
Partial Payment made to recipients of previous Tx's
Part of Previous Tx
Part of Previous Tx
Null Array Award 3.8
5% Stake

Technical Specifications & Features



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 (NAV) Collateral: 50,000
Guaranteed zero confirmation transactions, called Swift X
Wallet built-in Block Explorer and Wallet Repair Tools
Integrated BIP38, Multi-signature, and Multi-send Functions
Long-Term Development & Support

Case Uses

1. Understanding Blockchain Potential.
https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf

2. DApps
https://steemit.com/cryptocurrency/@heyitskolin/dapps-explained

3. Blockchain and Government Services.
https://techcrunch.com/2016/11/21/blockchain-technologies-could-transform-government-services/

4. Why Blockchain matters to healthcare security.
https://healthitsecurity.com/features/why-blockchain-technology-matters-for-healthcare-security

5. Blockchain in the automotive sector.
https://www.coindesk.com/bmw-ford-gm-worlds-largest-automakers-form-blockchain-coalition/

6. 10 ways Blockchain could be used in Education.
https://oeb.global/oeb-insights/10-ways-blockchain-could-be-used-in-education/

7. Unlocking Blockchain for the Aviation Industry.
https://blogs.systweak.com/2018/03/unlocking-blockchain-technology-for-aviation-industry/

8. IBM and Blockchain.
https://www.ibm.com/blockchain/

9. Why blockchain may be your next supply chain.
https://www.forbes.com/sites/joemckendrick/2017/04/21/why-blockchain-may-be-your-next-supply-chain/#40945a7413cf

10. 7 ways Blockchain will change the legal Industry forever.
https://www.techradar.com/news/7-ways-blockchain-will-change-the-legal-industry-forever

11. The Blockchain for Real Estate Explained.
https://www.forbes.com/sites/forbesrealestatecouncil/2018/04/23/the-blockchain-for-real-estate-explained/#5518ae67781e

12. How blockchain can be used in small business.
https://www.entrepreneur.com/article/305853.

13. Blockchain – Combating insurance fraud
https://www.insurancebusinessmag.com/uk/news/technology/blockchain-what-is-it-and-what-does-it-mean-for-insurance-95638.aspx

Challenges & Risks

Different industries are trying to adopt Blockchain technology into their current systems and these applications will cause the need for standard Blockchain technology regulations. There are four key areas that attract the attention of governments around the world including virtual currencies (tax issues), data encryption, privacy, and identity management. Currently the approach towards Blockchain technology regulations has depended largely on each individual countries attitude towards Blockchain technology rather than their being a standardized approach across all governments. In the United States, the federal government has not exercised any power to regulate Blockchain technology but it does intend to allow state governments to introduce their own regulations, which can cause individual differences. Meanwhile in the EU, Europe has a more welcome and positive approach towards Blockchain technology and regulations. In the case of China however although the Chinese government aspires to be a leader in Blockchain technology it's regulations are not currently conducive to Blockchain technology innovation, for instance Bitcoin transactions are currently prohibited in China.

Understanding Benefits and Risk of Blockchain

1. http://www.rmmagazine.com/2017/03/06/understanding-the-benefits-and-risks-of-blockchain/

2. https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/#40a245131670

3. https://medium.com/@preethikasireddy/fundamental-challenges-with-public-blockchains-253c800e9428

4. https://m.nasdaq.com/article/five-challenges-blockchain-technology-must-overcome-before-mainstream-adoption-cm899472

5. http://usblogs.pwc.com/emerging-technology/the-blockchain-challenge/

Appendix

[1] Mutual distributed ledgers (MDLs) have the potential to transform the way people and organizations handle identity, transaction and debt information. MDL technology provides an electronic public transaction record of integrity without central ownership. The ability to have a globally available, verifiable and tamper-proof source of data provides anyone wishing to provide trusted third party services with the ability to do so cheaply and robustly. Blockchain technology is a form of MDL
[2]NulleX has an open task and development environment with a highly accessible development team utilizing multiple social networking channels, including Discord, Telegram, and Twitter. GitHub is also utilized for team collaboration and work-flow. The development team is welcoming of anyone and everyone to join its cause, regardless of technical expertise. Please contact us on discord - https://discord.gg/6NjS8aT
[3] BaaS – Blockchain as a Service
https://www.bbva.com/en/what-is-blockchain-service-and-why-might-it-interest-your-company/
We propose the creation of professionally hosted Blockchain nodes. (2019) these fully managed nodes can be controlled by individual users who wish to outsource the operation and maintenance of their own full nodes. These services can be further extended for use by businesses who wish to benefit from secure access to full nodes, for all their employees, without needing to have in-house technical expertise to manage Blockchain nodes that facilitate users transacting various Blockchain services via local lightweight clients.
As a premium Blockchain As A Service (BaaS) product, ordinary users can purchase access to professionally hosted and managed Blockchain of their choosing to benefit from secure and encrypted access with high priority bandwidth channels for public, private or semi-private B2B networks. **Future development planned, not in the roadmap as of yet**
[4] Zerocoin Protocol Whitepaper -
http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf
[5] "Several Blocks" This refers to the number of blocks it will take to complete the process. This will depend on network activity and the amount of operating "Null Array Verifiers"
[6]Pos V3.0 Whitepaper -
https://www.dropbox.com/s/c3yldgd67yve7pt/Blackcoin%20POS%203.pdf

Important information:

1. See http://NulleX.io for Team info, wallet downloads, more information, and this whitepaper.

The following white papers can be referenced to discover some features of NulleX that were developed by these teams and not mentioned in this white paper.

Bitcoin White paper
https://bitcoin.org/bitcoin.pdf

Dash White paper
https://github.com/dashpay/dash/wiki/Whitepaper

PIVX White paper – Including Sea saw Rewards Mechanism
https://pivx.org/what-is-pivx/white-papers/

Kudo's to these teams for their hard work on the original source code. Thanks from the NulleX Core Development Team

White paper written by:

Trystan Partridge – Lead Developer – NulleX Core Development Team
Erik Feriotto – Business Strategist – NulleX Core Development Team
Tim Heintzberger – Marketing & Social Media - NulleX Core Development Team