KICK SOCCER COIN

WHITE PAPER

KICK SOCCER COIN

CONTENT

ABSTRACT

Currently the process of negotiating players between Football Clubs is extremely bureaucratic due to the various rules imposed by FIFA. The goal of the project is to serve "de-bureaucracy" by creating a virtual system where people around the world, outside the sports world as well as companies, agents and entrepreneurs, can virtually acquire percentages of athletes properly registered and licensed by KickerSoccer.

Along with this system, we will create the virtual platform of agent of Soccer players, where the unique and exclusive method of participation and payment will be the KickSoccer Coin. Kicksoccer is a crypto-currency based on Bitcoin, the work of Satoshi Nakamoto. There are several improvements include Masternode network, PrivateSend, for increasing fungibility and InstantSend which allows instant transaction confirmation without a centralized authority. KickSoccer integrates features inspired by Bitcoin's pioneering distributed ledger consensus technology as well as based on DASH and PIVX innovations. KickSoccer coin also has its own features, such as a Proof of Stake consensus algorithm, and a dynamic coin supply restrained by the burning of transaction fees.

Note that this paper, while an extensive introduction and explanation of KickSoccer, does not contain mathematical or cryptographical breakdowns or explanations. These can be found separately on the KickSoccer project's GitHub.

1 INTRODUCTION

The advent of the blockchain era occurred in 2009 with its implementation in Bitcoin by the entity known as Satoshi Nakamoto. Following Bitcoin's success, many competing cryptocurrencies—known as altcoins—have arisen. The potential of blockchain to revolutionise not only the way transactions are made, but the way business is conducted across many strata, has seen an explosion of interest in the technology. Currently, the cryptocurrency market is awash with tokens from parties of varying intent, motivation, and affliation. The myriad of tokens and projects—some novel and ambitious uses of blockchain, others in essence clones with catchy names—serves as a deterrent to widespread adoption of crypto as a legitimate, borderless alternative to at currency.

Bitcoin, despite its constant innovation, has so far failed to be widely accepted and adopted as a currency, and remains widely viewed as a store of value rather than means of conducting everyday business. As the world approaches a decade since the launch of Bitcoin, a definitive identity for cryptocurrencies has yet to emerge. This lack of identity has caused the public to view the crypto marketplace as a stock market 2.0. Its volatility and saturation intimidate potential adopters, who regard it not as an alternative to fiat currencies, but as a risky investment opportunity.

In keeping with the spirit of cryptocurrency's defining goal, KickSoccer aims to bridge the gap between the tech-savvy and tech-wary. It strives to provide a safe means through which not only investors, but the general public can conduct business without the need for financial institutions or middle-men.

KickSoccer aim is to provide the people of the ever more interconnected world with an expedient, private means to conduct business on their own behalf.

Currently the process of negotiating players between Football Clubs is extremely bureaucratic due to the various rules imposed by FIFA. The goal of the project is to serve "de-bureaucracy" by creating a virtual system where people around the world, outside the sports world as well as companies, agents and entrepreneurs, can virtually acquire percentages of athletes properly registered and licensed by KickerSoccer.

Along with this system, we will create the virtual platform of agent of Soccer players, where the unique and exclusive method of participation and payment will be the KickSoccer Coin. To do so, we will follow the following steps, which will be included in our RoadMap.

1.1 KICK SOCCER COIN SPECIFICATION

Name: KickSoccer Coin

Ticker: KSOC

Algorithm: X11

System: POS + Masternodes

Block Time: 2 minutes

Block Reward: 305 coins, halving every 5 years

20% staking reward

80% masternodes reward

Min amount for staking: not limited

Min age for stake: 30 minutes

Masternodes Creation: 10000 coins

Total Supply: 1 000 000 000 (One Billion coins)

Pre-Mine: 200 000 000 (Two hundred million coins)

2019

Q1

KSOC DEPLOYMENT

Creation of an exclusive cryptocurrency to be used in the platforms that ksoc will create.

Q1

KSOC POS

Inclusion of Ksoc in specialized websites of POS.

Q1

PRE SALES

Sale of a minimum lot of Ksoc to project developers.

2019

Q1

ONLINE STORE

An Online Store where payment is made exclusively with KSOC. Here you can find club jerseys, game tickets and merchandising.

Q4

PRE SALE (2ND STAGE)

Sale of a minimum lot of Ksoc to project developers.

Q1

AMBASSADORS

SIGN PARTNERSHIPS WITH SOCCER CLUBS AND PLAYERS.

Q2

SUPPORT SYSTEM

A 24/7 support system, via phone and email, so that our investors and currency users can report their issues.

Q2

MINING ASSET

New KSOC product for coin buyers.

Q2

E-SPORTS

Entry into the world of electronic games, with participation in teams and virtual games.

Q2

CROWDFUNDING PLATFORM

A platform where clubs can finance their projects, new? Works on KSOC!

Q2

KSOC CARD

What if at the Stadium, Pavilion or Bar you could pay with a KSOC Card? We are ready!

Q4

LIQUIDITY PROVIDER

Do you want to sell the KSOC you minted with your Mastermode? The liquidity provider will respond to that need.

Q3

VIRTUAL LEAGUE

A virtual Football League. Choose your team, your players and challenge your oponents. Make your investments in KSOC.

2021

Q4

PRE-SALES (3RD STAGE)

The last chance to buy KSOC before entering the foreign exchange market.

Q2

EXCHANGE MARKET

Now is possible to buy and sell KSOC in the exchange market.

2.0 MASTERNODE NETWORK

The KickSoccer network is two-tiered. The network is composed of the first, staking tier, in which all Kickosccer holders can participate in through staking their KSOC; and the more exclusive masternode tier. *This section is dedicated to the Masternod Network. For more on staking see section #.*

Masternodes are a set of incentivised nodes on a network within the KickSoccer network responsible for the handling of particular specialised tasks. The KickSoccer Masternode network has been carried over from Dash, though with the significant restructure to a Proof of Stake consensus algorithm.

The functions carried out by KickSocce masternodes are fundamentally similar, however, to those of Dash. As such, these nodes are an integral part of the KickSoccer digital ecosystem, and necessary to network functionality.

The Masternode network fulfils a range of functions independent of staking nodes. These distinct functions are limited to masternodes, and cannot be completed by a standard staking node. These responsibilities are distributed across the Masternode network, and no one masternode has power or authority in excess of others in the network.
This section dissects these Masternode network functions individually.

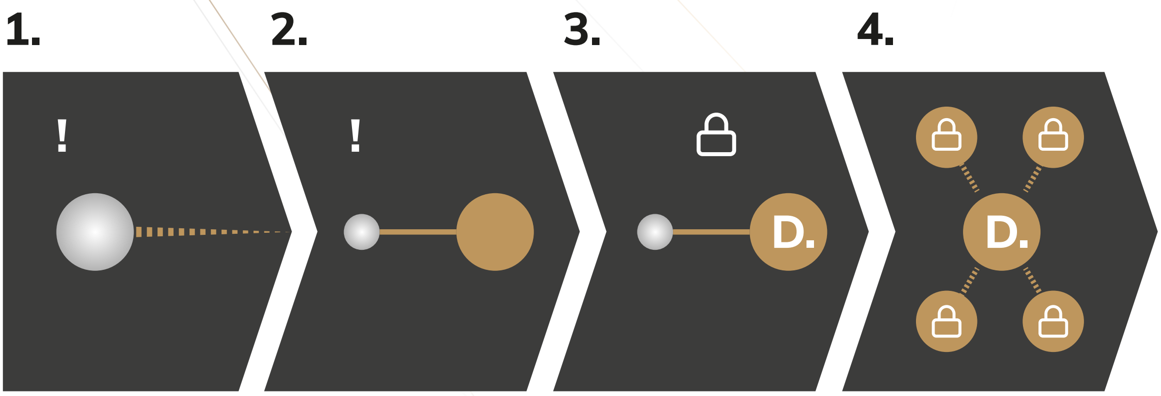
2.1 MASTERNODE NETWORK TECHNICAL FUNCTIONS

The Masternode network fulfils a range of functions independent of staking nodes. These distinct functions are limited to masternodes, and cannot be completed by a standard staking node. These responsibilities are distributed across the Masternode network, and no one masternode has power or authority in excess of others in the network.
This section dissects these Masternode network functions individually.

2.1.1 SWIFTX

The Masternode network allows for near instantaneous transactions, as short as a single second. With transaction times provided by SwiftX, KickSoccer is able to compete with similarly fast crypto currencies, as well as transactions of credit and bank cards. SwiftX transactions take place independently of the network proper, as they are isolated to the Masternode network.
This function takes place via a quorum between masternodes. When a SwiftX transaction is proposed, the inputs of said transaction are locked by a random delegate masternode, making them spendable only through a specific transaction. All confiicting blocks or transactions would then be rejected. The hash of the locked transaction is broadcast by the delegate via ZeroMQ (a high-performance asynchronous messaging library) over the Masternode network, near-instantly achieving consensus and eliminating the need to await confirmations without the risk of a double-spend.

A BASIC DEMONSTRATION OF SWIFTX TRANSACTION

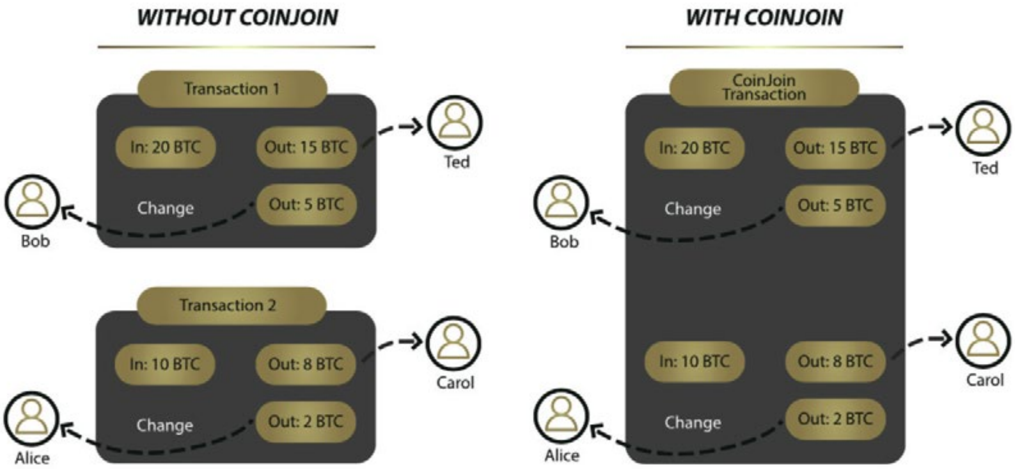


Key
Grey: default node
Gold: masternode
Gold with D: delegate masternode
!: SwiftX Transaction

1. A default nodes does a SwiftX transaction.
2. The SwiftX transaction is transmitted to the Masternode network.
3. A random masternode become a SwiftX delegate and blocks the transaction.
4. The delegated masternode passes the blocked transaction to the network, where all unlocked blocking incidents are denied.
The benefit of SwiftX lies in the ability to make transactions as points of sale comparable to current systems, such as Visa. The difference is that SwiftX is decentralized, with no point of failure.

2.1.1 COINMIXING

As with Dash's PrivateSend, KickSoccer coin-mixing feature was initially built upon CoinJoin. Coin mixing—also known as tumbling—involves the obscuring of transaction via the dividing of funds to protect their source. Not moving the sum total of a transaction directly from source to target, but rather complicating it via dividing it into mixed transactions, makes it much more dificult to track any one mixed transaction. This process serves to maintain the fungibility of units of the currency.



This image demonstrates the basic idea behind CoinJoin wherein two transactions are merged into one.

As KickSoccer is Proof of Stake, rather than Proof of Work, significant alterations were necessary in order to implement a coin-mixing service optimally into the KickSoccer code. Since KickSoccer Core wallet version 1.0.1 KickSoccer has moved away from the CoinJoin methodology of coin-mixing, replacing it with **Zerocoin** —a more sophisticated coin-mixing protocol with heavily improved privacy baked into the cryptography of the protocol. This limits

The ZeroCoin logo

Zerocoin newly mints currency **(zKSOC)** and allocates it to pools in order to draw from when a wallet receives zKSOC. These pools represent a substantial amount of the total KickSoccer Coins. Thus, with zKSOC there is no necessity to obscure a coin's origin, **as zKSOC carry no data pertinent to a unit's history, maintaining fungibility while being untraceable.**

KickSoccer will continue pioneering new technology to remain at the very forefront of privacy in the crypto sphere. The next frontier for KickSoccer in this space is the addition of Bulletproofs and the replacement of the RSA-2048 Factor system currently in place with a more modern solution.

For more on the KickSoccer ZeroCoin protocol, Bulletproofs, and zKSOC see section #.

2.2 MASTERNODE DECENTRALIZED GOVERNANCE

2.2.1 PROPOSAL VOTING TBD

2.3 MASTERNODE ACQUISITION

Operating a masternode on the KickSoccer Masternode network is an attractive option to those invested in KickSoccer. Masternodes are incentivised, paying out KSOC to the operator in return for their service. Masternodes are run via the standard KickSoccer wallet, albeit with some additional input.

To be eligible to create a masternode, several requirements must be fulfilled. A masternode necessitates the following:

10,000 KickSoccer coins be sored on the masternode controlling wallet. These KickSoccer coins must remain unspent so long as they are associated with a masternode wallet—this should be a separate wallet from one used to make transactions. Spending, or otherwise removing these KickSoccer coins will remove the status of the host wallet as a masternode, taking with it the eligibility for masternode rewards. The necessity of these 10,000 KickSoccer coins serves several purposes, including ensuring a high enough percentage of nodes remain staking, and that the masternode host is likely to reliably provide a masternode service for the network over time, rather than simply dabbling. Most importantly though, it ensures no single entity can simply host enough masternodes to achieve the 51% necessary to corrupt the governance, jeopardising the KickSoccer DAO.

An unchangingstatic IP is also necessary to operate a masternode. Dynamic IPs cannot participate in the network as consistent contact with a verified masternode is necessary to function in the Masternode network. This means the internet connection of the masternode host must also be reliable, as the masternode needs to remain online dependably. On top of this, each masternode requires a unique IP, so hosting two masternodes cannot be accomplished without a secondary IP address. In the event this requirement is not possible, it is recommended the user simply stakes their KickSoccer coins instead. This pays out a similar amount to a masternode, though downtime in connectivity is harmless if encountered.

· For more on staking see section #.

A dregree of technical compentency is also preferable, as although resources are available for the setting up of a masternode, the process requires editing of a .conf file, allocation of a new wallet address, and other actions executed by Linux command console. Support for setting up a masternode can be gained through KickSoccer support support channels.

- *Instructions on setting up a masternode can be found here: http://kicksoccercoin.com/wp-content/uploads/2018/11/Kicksoccer-masternode-setup-guide.pdf*

- *KickSoccer support can be reached on the KickSoccer Discord in the #support channel, or at https://discord.gg/gHGBkVj*

Masternodes can be run on Linux machines, through a server host, or through devices such as the Raspberry Pi. Ultimately, despite the decision, the security of the masternode host is integral. Private key management, the setting up of a firewall, a physically protected machine, and other security measures are strongly advocated for, both for the sake of the network, and the 10,000 KickSoccer coins of the host.
As with anything KickSoccer, there is no need to go it alone when setting up a masternode. Support can always be found from the KickSoccer community. Any questions can be posed to the community in the Discord support channel.

3 MASTERNODE - STAKING REWARD SYSTEM

As a two-tiered network, KickSoccer incentivises participants of both the staking and Masternode tiers to maintain the health of the network. Via PoS, users contributing towards the network are rewarded either for staking in-wallet, or for storing their 10,000 KickSoccer coins as collateral for a masternode to support the network. While both of these are a means of acquiring rewards over time, the amount and means difiers.

- *For more on masternodes see section #2*

3.1 REWARD BALANCE: MASTERNODE - STAKING

The reward balance between a masternode and a staking wallet is overall not significantly skewed. Generally, the masternode will pay out reliably, where staking involves more variance. This reliability is to incentivise masternodes, as they are integral for the health of the network.
A masternode has several qualities that set it apart from a staking wallet:
- It requires 10,000 KickSoccer coins be left unusable by the holder to remain functioning as a masternode.
- It must be left connected at all times.
- It requires a separate, stable IP address to the user's wallet intended for use.

***Note:** Some aspects of the setting up of a masternode can be complicated for less technically-minded users.
These lack of freedoms mean that if the reward were to be identical to staking, the likelihood of anyone choosing to host a masternode would be significantly lower.
With that said, there are advantages to staking over hosting a masternode. These include:
- The ability to opt in and out of staking as the user pleases.
- Can be done regardless of held KSOC/zKSOC amount.
- The option to divide up holdings between addresses.
- No requirements on specific denomination (masternode 10,000 requirement).

There also exists the possibility to earn more than a masternode holding the same amount of KickSoccer coins due to the random nature of staking. On the flipside, this may also mean one is rewarded less than the average expected amount for staking at the held amount.

At the same time, zKSOC offer an increased incentive for stakers over KickSoccer coins. Here is a breakdown of the minted currency in the event of KSOC and zKSOC staking node respectively:
KickSoccer staker finds block: masternode reward 80%, staking reward 20%
zKSOC staker finds block: masternode reward 80%, staking reward 20%.

3.2 REWARD RATE VARIANCE: KSOC - ZKSOC

As seen in the previous section, KickSoccer coins and zKSOC rewards differ in both staking and masternode rewards. This discrepancy is part of an incentive to have users in the PIVX network support Zerocoin, which by nature cannot function without participation. Liquidity of zKSOC over the Zerocoin protocol is also necessary for it to function swiftly. Non-locked volumes of zKSOC need to be available for the protocol to draw on at all times, lest transaction time become needlessly extended. This is due to the wait on both transaction confirmations, and a confirmation of another zKSOC mint of the same denomination to meet the maturity requirement—non-issues providing the zKSOC liquidity is supported.
These mechanics of Zerocoin are explained in more detail in section 6, though the variance in rewards between KSOC and zKSOC is a necessity for the health of the KSOC network. Careful consideration has been invested into fairly balancing the rewards for both KSOC and zKSOC, but as privacy and expediency are the ultimate goals of KSOC, the health of the Zerocoin network is paramount.

4.1 HALVING

Halving every 5 years.

5 PROOF OF STAKE CONSENSUS

Unlike its predecessors—Bitcoin, Litecoin, and Dash—the KickSoccer coin network functions on a **Proof of Stake consensus algorithm**, which was introduced in a paper by Sunny King and Scott Nadal in 2012. The original concept relied heavily on the notion of "coin age", or how long a UTXO (Unspent Transaction Output) has not been spent on the blockchain. In this way, it difiers from Proof of Work by not focusing on and rewarding miners, but rather **rewarding anyone willing to participate in the running of the network.** The protocol was further refined in PoS version 2 for BlackCoin by Pavel Vasin (Rat4) with several potential security fixes, such as the potential of a malicious node to abuse coin age to perform a double spend; or the potential for honest nodes to abuse the system by staking only periodically, negating coin age from consensus11. The robustness of the Proof-Of-Stake was further enhanced in a version 3 of the protocol at the end of 2016, and most recently, Zerocoin Proof of Stake (zPoS) was implemented by PIVX in 2018.

Simply put, staking is making computing resources available to the network, which may "select" the node to generate the upcoming block on the chain based on delimited competition. In the case of KickSoccer, these limits are demarcated by considering the balance (UTXOs) staked by the wallet—every staking node is competing trying to create a valid block, very much like in PoW. Nodes, however, are technically limited in the number of trials in a given time (eliminating the need for higher computing power) and the dificulty to get a valid block is inversely proportional to the amount being staked. A higher balance means a higher chance of satisfying the dificulty criteria, validating the block, and being rewarded.

Staking is significantly less demanding on resources than PoW mining, as there is no need to push towards ever increasing dificulty, and the associated increase in computing power to solve it. As such, PoS is an environmentally friendly alternative to PoW.

While the environmental factor alone already helps PoS stand out against PoW, there is another factor to be considered: maintaining a fair, distributed power across the network, which should be a high priority target of any cryptocurrency. With the expanding dificulty in mining that necessitates more powerful rigs that cost more to run, the ability for people to feasibly operate such rigs becomes more exclusive.
Such things as the costs of hardware, electricity consumption spent on computing, and further consumption on cooling, rule out a great many locations as suitable for mining. Inevitably, this results in a great deal of power held by miners, of which fewer and fewer are able to remain competitive, not only leading to a monopoly in rewards, but in control over networks

5.1 KISKCOSCER COIN PROOF STAKE - IDENTITY AND SECURITY

KickSoccer utilises staking as it's a strongly held position within KickSoccer that a fair alternative to PoW is necessary for a decentralised currency to be valid, feasible, and welcoming to newcomers. The design of the KickSoccer **PoS** and **Private zPoS** systems are intentionally tailored to mature in such a way that growth of the network and further adoption work in favour of the network, rather than bog it down and focus power on a select group. PIVX transactions will remain expedient, with elastic block sizes coming soon to ensure this—or instant if electing to use SwiftX; they will remain private—only getting even harder to trace as new implementations following zKSOC, such asI2P, and dandelion go live; and they will remain decentralised.

Criticisms towards PoS consensus networks do exist, such as potential double spending, and vulnerabilities to **long-range** and **nothing and stake** attacks. Staking/masternode rewards require 100 consecutive confirms, making them spendable after 101 block confirms; this protects against network dominance via malicious staking involving exponential growth were a vulnerability ever to be found and exploited.

· For more on nothing and stake see section #

It was estimated by a KickSoccer developer that an attacker would need to own 70.7% of staked coins for a 50% chance of **double of spending** or invalidating a single block—a number practically impossible to acquire.

Another proposed PoS vulnerability is a **long range**, or **history** attack, wherein early blocks are rewritten, compromising the blockchain. For this reason, checkpoints—blockchain markers set at intervals preventing any alteration/forking prior to them—are used to maintain the valid chain, and help by protecting against **long-range** attacks.

A successful PoS attack would greatly de-value the attacker's assets when discovered, whereas a successful PoW attack may cost an attacker only electricity. Also, KickSoccer staking can be decentralized amongst all of its users and cannot be traced by electricity use, whereas mining is usually centralized by mining cartels, concentrated in regions with cheap electricity, and is traceable by high constant power demand.

5.2 STAKING KSOC AND ZKSOC

Both KSOC and zKSOC can be staked on the KickSoccer network, with the staking of zKSOC via zPoS, rewarding users for utilising KickSoccer privacy features. Staking either KSOC or zKSOC on the KickSoccer network requires at least 1 of the smallest unit of either KickSoccer coins (0.000000001) of zKSOC (1) held within, the wallet to be synchronised with the network with block information up to date, and for the wallet to be unlocked for staking.

While staking is active, it doesn't necessarily ensure users will mint new KSOC/zKSOC right away. As participating in PoS means a node may hash a block to contribute to the blockchain at any point, and depending on the quantity being staked (the more staked, the higher the chance of being selected).

For this reason, variance exists in KickSoccer staking as rewards are not allocated regularly, but are randomly awarded per the hashing competition of the PoS consensus model.
• For more on staking rewards see section 5.

A guide for setting up a KickSoccer wallet for staking can be found here:
https://kicksoccercoin.com/

WWW.KICKSOCCERCOIN.COM

Edificio Ramazzotti Avenida do Forte,
6 - Piso 2 2790-072 Carnaxide Portugal

KICK
SOCCER COIN