# Kylacoin

### An Open Source Peer-to-Peer Electronic Cash System

Revision: 2, Date: April 7, 2023

### Introduction

Kylacoin is a cryptocurrency designed to act as money and a form of payment system outside the control of a person or a group, that operates free of any central control or the oversight of banks or governments. Kylacoin can be obtained through a process called proof-of-work mining, or simply mining. Anyone can sell it and buy it without an intermediary like a bank. Kylacoin enables peer-to-peer exchange of value in the digital realm through the use of a decentralized protocol with the help of cryptography. Kylacoin transactions are verified by the network nodes through cryptography and recorded in a public distributed ledger called a blockchain. Kylacoin is a medium of exchange, such as the US dollar, but is digital and uses cryptographic techniques and its protocol to verify the transfer of funds and controls the creation of monetary units.

# Proof-of-Work

Proof-of-work is a type of consensus mechanism that requires network users to devote computing power to complete a task, whoever completes the task gets a reward and secures a block with the transactions that were sent to the network, and also gets the fees of those transactions, this process is called mining. The difficulty of mining increases when there are more miners on the network, and decreases when there are a few miners, this method is called difficulty adjustment, which helps the speed control of releasing the currency.

### Transactions

A transaction is the way to send money from one wallet address to another. Anyone can create and send a transaction from their wallets at any time, transactions are temporarily stored in the memory pool, a miner can choose to mine a block with transactions with higher fees and higher priority to get confirmed, once a transaction is confirmed, the receiver can spend it.

### Coinbase

Coinbase is a form of transaction without an input that generates money and is paid as a reward to the miner who completes the proof-of-work task.

## Verification

Keys come in pairs consisting of a private key (secret) and a public key (address). Everyone knows your public key and will be able to send money to it, but only you can spend it with your private key, everyone else will verify your signature with your public key.

### Blockchain

Every mined block is linked to the previous block and has the hash of the previous block. In this way, only blocks can be mined on top of the previous block with a new height, and it prevents inserting blocks in the middle of the chain. The chain always grows and includes the history of all transactions since the start of the project, and every node of the network will have a copy of it.

### **Peer-to-Peer Network**

Kylacoin uses a peer-to-peer network to send transactions and mined blocks to other nodes. Each node validates the transactions and blocks, individually; there is no need for a central authority to be involved. With the help of cryptography, Kylacoin is an anonymous banking system.

### **Smart Contracts**

A smart contract is a form of agreement between users on the blockchain that is based on predefined criteria and executed as inputs to transactions, which enables the owner of it to spend it.

Kylacoin supports a wide range of smart contracts using its powerful scripting language.

### Pay-to-Public-Key-Hash (P2PKH)

P2PKH script is one of the simplest Kylacoin's smart contracts. It allows someone to send coins to a Kylacoin address that only the owner of the private key corresponding to the public key hash can spend the amount.

#### **Multi-Signature Scripts**

Multi-signature scripts are more complex than P2PKH scripts because they require multiple signatures. A transaction can only be spent when the required number of signatures are provided. For instance, 2-of-3 is a common multi signature setup that enables three parties with three public keys to hold KCN as a group. It requires two signatures for Kylacoin to be spent.

#### **Time-Locked Transactions**

Time-locked transactions are valid after a specified time. They can be combined with other validations, for example, a script may demand three signatures to spend before a given time. After this duration, only one signature is needed.

### Pay-to-Script-Hash (P2SH)

The P2SH standard allows users to send money to the hash of any script. This reduces the cost of sending to a complex smart contract while maintaining privacy. With the SegWit protocol, the P2SH standard includes Pay-to-Witness-Script-Hash (P2WSH).

#### **Other Smart Contracts**

As of right now, Kylacoin does not allow hosting tokens on its chain, but will be working to create a token system on Kylacoin's blockchain.

# **Advantages of Smart Contracts**

#### Transparency

Smart contracts enable users to get the same information at once, reducing the chances of any possible manipulation of the clauses of the contract. Allowing contracts and agreements to be made without the need to know each other and avoiding possible breaches of conditions or mistakes in the management and execution of the contract.

#### Autonomy

Smart contracts do not need brokers or other intermediaries to confirm the agreement. Therefore, they eliminate the risk of manipulation by third parties.

#### **Cost Reduction**

The absence of intermediaries in smart contracts results in cost savings.

#### Speed

Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

### Improvements

#### **Proof-of-Work Algorithm**

SHA3 is a member of Secure Hash Algorithm family of standard hashes by NIST released on August 5, 2015, based on the Keccak algorithm; Kylacoin uses the double SHA3 (SHA3D) algorithm instead of SHA2 (SHA256D). SHA3D has a round count that is high enough to give it a massive security margin and uses better sponge construction. SHA3D is also resistant to length extension attacks. SHA3D can be implemented in an ASIC or an FPGA.

#### **Transaction guarantee**

Kylacoin is improved to make sure every transaction gets confirmed without delay. This is done by sending the hash of all transactions in the memory pool to other nodes upon creating a connection, the nodes that are missing transactions will request the complete transaction from the node that has that transaction. This way, all nodes will always have a copy of all transactions in the memory pool even if they go offline for a while. Once the transactions are confirmed, they will be cleared from the memory pool.

### Wallets

Kylacoin is developed with a full node decentralized core wallet with a graphic user interface.

Light wallets will be coming next.

# Security

Whoever holds the private keys can spend the money in that corresponding address. As long as you keep your private keys safe, everything is safe.

# Supply

Kylacoin has the maximum supply of 21,000 coins for the lifetime of the project. After we reach the maximum supply, no more coins will be released, and miners will only be rewarded with the fees of the transactions.

Because the block time is 60 seconds for faster confirmations, we chose to keep the block reward reasonably low initially at 0.005 KCN, and will be halving every 4 years.

Kylacoin was launched fairly without any premine or ICO; we announced the project a few minutes after the blockchain started working, on bitcointalk<sup>1</sup>. Every penny is released through mining.

As of version 1.2.0, we have added a 10 percent developer reward to the blocks, which helps us with the development of the project, recruiting people, and keeping up the servers.

### Team

My name is Jeremy (JayBitron), and I'm leading this project with the help of friends and the community, I'll be recruiting more people as the project grows.

## Conclusion

We described some of the features of Kylacoin in this whitepaper and will be updating it once in a while to include all new features of Kylacoin as we develop it further.

#### Links

Webiste: kylacoin.com

New BitcoinTalk thread: https://bitcointalk.org/index.php?topic=5434692.0

@ 2023 Kylacoin, All rights reserved.

<sup>&</sup>lt;sup>1</sup> https://bitcointalk.org/index.php?topic=5384582.0