SIBCoin: a privacy-oriented ASIC-resistant cryptocurrency



CRYP2NOVA

ver 0.3.0

November 15, 2017

Archived copy · cryp2nova.com



Abstract

SIBCoin is a peer-to-peer cryptocurrency, employing a reimagined version of Dash blockchain with several fundamental improvements. Introduction of a reinforced hashing algorithm Streebog makes the coin ASIC-resistant, ensuring a decentralized ecosystem. X-layer is a platform based on Coinprsim protocol, which allows for issuing and supporting custom-made digital assets.

Of the people, by the people, for the people!

CRYP2NOVA

Archived copy · cryp2nova.com

Introduction

Conventional money becomes obsolete

The modern financial system is broken. It has been like that for a while, ever since money has devolved from a medium of exchange into an instrument of control.

The reason this happened is that money no longer belongs to the public. Money, and by proxy economic activities and well-being of people, today is controlled by third-party entities who play their own game.

To reclaim the money elimination of intermediaries is absolutely necessary. Intermediaries used to be unavoidable because in a trustless environment interacting parties required a guarantor. Blockchain, disruptive technology underlying cryptocurrencies, provided humanity with a means to consistently maintain consensus pertaining to the state of distributed data ledger in a completely trustless environment. In the modern world algorithm of consensus is the only viable trusted guarantor.

This is the reason SIBCoin exists, to give everyone a fair chance in a free economy.

Cryptocurrencies are the future of money

SIBCoin's ultimate mission is not only to provide the people with a financial instrument that would facilitate transfer of value over the internet in trustless environment but to introduce the broader public to cryptocurrency, decentralised autonomous organisations and blockchain philosophy in general.

SIBCoin was conceived as a local altcoin and initially circulated only in Siberia proper. It emerged as the first cryptocurrency to cater to the needs of Russian-speaking community and perfectly filled the vacuum that existed on much of Eastern European territories due to certain cultural and linguistic barriers. With time SIBCoin was adopted not only by Russians and people living in neighbouring countries but even overseas.

SIBCoin does not aim to compete with national currencies. Its concept transcends nations. SIBCoin connects people sharing economic and cultural

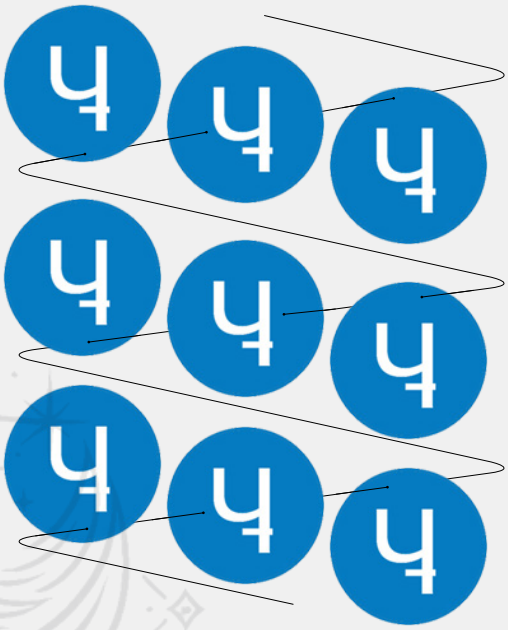
CRYP2NOVA

Archived copy · cryp2nova.com

proximity and welcomes to join its network anyone who shares ideals of de-centralisation, honest and transparent transfer of value and financial freedom.

The Coin

SIBCoin is a decentralised digital currency and a peer-to-peer payment processing system. It has no need for intermediaries, the regulatory function is carried out by a cryptographic mathematical algorithm. SIB-Coin users interact directly and form a de-centralised network, where all transactions are recorded in an open to public scrutiny and tamper-proof digital ledger distributed across all computers of the network and synchronized with the help of the afore-mentioned algorithm.



Technology-wise SIBCoin is a Dash fork with a number of significant tweaks. The first block was generated in 2015.

Coin specifications

- Compensation for the block is calculated as follows:

$$\frac{2222222}{(((\text{Complexity} + 2600) / 9)^2)}$$

- GPU mining.
- The average residence time of a new unit: 2.6 minutes.
- The difficulty is recalculated using the algorithm Dark Gravity Wave, which avoids some of the problems with big jumps in network capacity.

CRYP2NOVA

Archived copy · cryp2nova.com

- Compensation for the block is reduced by 7% each year.
- The maximum number of coins, estimated: 23–24 million, provided the growth of complexity and falling unit awards for up to 5 coins, according to the algorithm.
- Uses masternode mechanism.

Why Dash fork?

Blockchain stores permanent record of all transactions that have ever taken place on the network. These records are open to the public and can be accessed at any time. Unfortunately, pseudonymity provided by Bitcoin's network does not offer its users sufficient privacy. Dash, on the other hand, is decentralized and strongly anonymous, with tamper-proof instant transactions. This makes Dash blockchain technology an ideal starting point for a modern cryptocurrency.

Other important considerations behind this choice included increased transaction speed on the network, low fees, strong privacy protection and pre-existing instruments for building a tightly-knit global community incentivised to provide various services to the ecosystem (masternode network).

SIBCoin retains all the strong points of Dash blockchain while introducing several important enhancements of its own. The most important additions include Streebog hashing algorithm, which makes SIBCoin ASIC-resistant, X-Layer protocol and a host of services, which help integrate SIBCoin into the real sector of the economy.

CRYP2NOVA

Archived copy · cryp2nova.com

Features

Privacy

SIBCoin takes privacy very seriously.
Some regimes look at cryptocurrencies with growing suspicion or are even on the verge of heavily regulating or even banning them. Cryptocurrency is not an illegal or taxable asset. No one should be able to control or trace your cryptoactivity.

As cryptocurrency's ledger is public and open for everyone, there is always danger of theft or extortion (just as with large sums of fiat money or gold). No one should be put under peril as a result of carelessness or ignorance. For that reason SIBCoin is as secure as a cryptocurrency can be.

PrivateSend

The PrivateSend technology that renders transactions untraceable is an extended version of the CoinJoin mixer. The core mechanisms of CoinJoin were enhanced by passive ahead-of-time mixing and a series of other improvements which led to one of the most robust coin mixers in existence.

The basic principles behind the mixers' concept are easy to grasp. Network transactions can be formed by multiple parties and made out to multiple parties. PrivateSend uses this fact to basically merge different simultaneous transactions together in a way where they cannot be uncoupled thereafter. So far PrivateSend has proven to be unbreakable.

For more information on basic concepts of PrivateSend, please read Dash whitepaper.

Archived copy · cryp2nova.com



Community

The concept of cryptocurrency is not exhausted by the underlying technology. A healthy crypto ecosystem is maintained first and foremost by the community. From its earliest days SIBCoin was known as a strong community project, gaining popular support first in its frigid Siberian homeland and with time all across the globe.

Along with community building tools SIBCoin has inherited with Dash blockchain, the project has introduced a number of its own innovative concepts which will be touched upon in this section.

Masternodes and InstantSend

SIBCoin employs a special full node structure — the so called masternode network. Masternodes bear certain functions other than just keeping the network synchronized. SIBCoin's masternode network doubles as a decentralised p2p exchange between SIBCoin and Bitcoin.

SIBCoin ecosystem offers financial incentivisation to masternode owners to keep the network up and running. Apart from economic incentives masternodes also offer their owners voting rights when the network encounters issues that require a node owners' consensus to be reached. Social significance of masternodes will only grow over time.

To create a masternode 1000 SIB have to be locked within a wallet for as long as masternode is operational. These coins can be withdrawn at any moment but this will strip the node of masternode status.

CRYP2NOVA

Archived copy · cryp2nova.com

SIBCoin's Masternodes function the same way they are meant to function in Dash network. For more information on basic concepts of Masternodes, please read Dash whitepaper.

Another important function carried out by Masternode network is securing instant transactions via InstantSend. Masternodes form quorums which allow users to send and receive instant irreversible transactions. A transaction lock takes only several seconds to be set currently on the network.

Streebog hashing algorithm

Ever since x11 was no longer ASIC-resistant and Dash miners started building ASIC farms, the coin slowly drifted to centralized mining model, mirroring Bitcoin itself. This is extremely detrimental to the very spirit of cryptocurrency and eventually to its economy.

SIBCoin contains a cryptographic hash function Streebog (GOST R 34.11-2012) so far resistant to exploitation by ASIC manufacturers. Thanks to this precaution we are getting as close as possible to the paradigm of "one-CPU-one-vote" outlined by Satoshi Nakamoto in Bitcoin's WP.

This add-on allows to improve decentralisation without forgoing security concerns. It also serves as groundwork for the potential official implementation in Russia as it conforms to the governmental security standards.

CRYP2NOVA

X-Layer

To facilitate further growth of SIBCoin ecosystem the need was identified to make SIBCoin's blockchain more interactive while not compromising its security. The idea behind X-Layer is not unique but it was proven to be sound, safe and effective.

In the core of X-Layer technology lies Coinprism technology, a software layer built on top of Bitcoin's blockchain that allows users create sidechains for their custom digital assets and currencies. Just like with Coinprism and Bitcoin, X-Layer transactions are SIBCoin transactions in a sense that they provide the very same level of security.

Archived copy · cryp2nova.com

Services

SIBCoin is highly service-oriented. It aims to provide a better alternative to the current systems of money transfer in Remittance and eCommerce. SIB-Coin's services are all free except for the usual transaction fees which makes it the cheapest way of transferring value.

Wallets

Access to SIBCoin's network can be done via a software wallet or online wallet (including a Tor version) both available on the official site. SIBCoin also offers the so called "Cash Chervonets", a "paper" wallet protected by a randomly generated secret code. "Cash Chervonets" may be issued in printed form.

Exchange and Payment Services

Moneypolo allows to replenish EUR and USD accounts with SIBCoins. Coinex accepts payments in SIB for telecom services and exchanges SIB to fiat for withdrawal with VISA/Mastercard.

There is also an option of buying SIBCoins directly with a bank card and making mass payments to bank cards. SIB's native SMS-service sends in reports on user's transactions.



Archived copy · cryp2nova.com

Telegram bot

Connect with SIBCoin network via a Telegram trader bot at @SIBWalletBot. This bot will sell you SIBCoin, process payments and provide you with vital crypto-trading information. Specific Seller and Buyer SIB bots are available at @SIBsellerBot and @SIBbuyerBot.

SIBCoin community ceaselessly reaches out to retailers and service-providers in real sector. Highest priority are payment processing services. SIBCoin is tirelessly working with partners and interested parties worldwide to establish the most convenient and consumer-oriented payment processing network.

CRYP2NOVA

Archived copy · cryp2nova.com

Future

In its ultimate form SIBCoin's network will have decentralized exchange service with all other popular blockchains and a decentralized marketplace akin to OpenBazaar. Online vendors will have instant access to SIBCoin's network via highly customizable and easy-to-use apps.

To root SIBCoin in real sector and ease interaction with fiat money a debit card linked to SIBCoin wallet will be issued.



CRYP2NOVA

Archived copy · cryp2nova.com



https://sibcoin.money/

CRYP2NOVA

Archived copy · cryp2nova.com