DarkSaga

An Open Source Decentralized Virtual Currency

WhitePaper v1.0.0.5

DarkSaga

An Open Source Decentralized Virtual Currency

January 30, 2021

1. Introduction

DarkSaga seeks to compete with traditional financial systems using an electronic cash system, the removal of trusted third parties, and automation of monetary policy controls. Many individuals do not have access to banking services. Businesses and consumers are burdened by significant transaction costs imposed by traditional banks, savings institutions, and payment processing networks. Central banking systems impose monetary policies to control the money supply and influence economic growth. DarkSaga eliminates these weaknesses by establishing an automated global financial system.

In this paper, we propose a system built upon existing decentralized cryptographic innovations designed to transform traditional financial systems. In addition, we describe a method to integrate automated monetary policies into the system.

2. Removal of Trusted Third Parties

We utilize a peer-to-peer electronic cash system without the need for banks and payment processing networks (trusted third parties). The system provides a secure decentralized payment network that automates recordkeeping and account creation. The system provides an integrated electronic medium of exchange (coins) and eliminates the need to produce physical currency.

Peer-to-peer electronic cash systems, also known as cryptocurrencies, consist of a distributed ledger (blockchain), coins, and a network of nodes. In general, transactions are validated by the nodes using cryptography and a consensus algorithm. DarkSaga utilizes the proof-of stake and proof-of-work algorithms, which incentivize users through a process of staking (discussed further below) and mining. The medium of exchange is a SagaCoin (SAGA).

Importantly, the system is self-sufficient and eliminates the need for trusted third parties. Users are not required to maintain savings or checking accounts. Rather, a record of account balances is maintained by the system according to each user's blockchain address, which can be obtained at any time at no cost to the user. Further, the need for payment processors such as Visa and Mastercard is eliminated using the system's peer-to-peer network.

3. Specifications

To ensure that the DarkSaga remains decentralized, transactions are validated using both Proof of Work (PoW) and a Proof of Stake (PoS) consensus mechanisms.

Proof of Work

PoW uses high-performance computers and equipment to validate transactions on the blockchain. The computers continuously work to confirm transactions by solving mathematical problems. Computers

compete to find the solution and the winner is rewarded in the native cryptocurrency. This process is also referred to as *mining*.

Proof of Stake

This method was developed as an improvement to PoW by removing the physical resources needed for mining. Instead of using computer hardware to compete for rewards, users are randomly selected to receive payment based on the number of coins that they hold. The more coins held by the user, the greater the chance to validate a transaction and receive a reward. This is known as *staking*.

Rewards are also be earned through the use of masternodes. Like staking, masternode operators are periodically rewarded for validating transactions on the network.

Masternodes

DarkSaga boosts network validation using masternodes. Individuals can operate a masternode after storing a sufficient amount of coins as collateral.

Each masternode becomes one of the nodes that support the blockchain. This way, the network remains decentralized. Masternodes support privacy and anonymity and serve to supplement rewards earned under the PoS model.

DarkSaga specifications:

- Algorithm: Scrypt
- Max Supply: 42,000,000
- Spacing: 2.5 Minutes
- 10 Minute Confirmation Time
- Port: 62620
- RPCport: 62720
- Block Rewards
- < 1,043,122 6 Saga per block (2 PoW, 2 PoS, 2 Masternodes)
- > 1,043,122 3 SAGA per block (1 PoS, 1 Pos, 1 Masternodes)
- Masternode collateral: 2500 SAGA
- Minimum Stake Age: 8 hours

4. Integrated Monetary Policies

As discussed in the introduction, governmental intervention is typically used in traditional financial systems to establish monetary policies that control the supply of money in circulation and control the rate of inflation. In addition, centralized authorities are responsible for the creation and distribution of money in the economy. To eliminate the need for these entities, we propose the use of the following tools to automate monetary policy within the system: finite supply, and reserve incentives.

Finite Supply

In a traditional financial system, an unlimited amount of physical currency can be created at any time at the discretion of governmental authorities. The ability to create an unlimited amount of money at any time creates a potential opportunity for abuse of the system. DarkSaga solves this issue by establishing a finite number of coins (42,000,000) that can be created.

Reserve Incentives

Because the total supply of network's coins is distributed to users at once, the currency is subject to

hyperinflation. The market becomes saturated with an excessive number of coins and demand cannot keep pace with the quantity supplied.

To combat this issue, two deflationary controls are built into the DarkSaga Network: staking and masternode rewards.

Staking

In a proof-of-stake systems, staking is used in conjunction with the operation of nodes to validate transactions and secure the system. Individuals are incentivized to run nodes and set aside coins (the stake) to earn rewards in the form of transaction fees collected by the network. In general, the rate of rewards paid are based on the number of coins staked by each user. Coins set aside for staking are removed from the circulating supply creating deflationary pressure (see figure 2 below).

Masternode Rewards

As discussed above, transactions on the DarkSaga's blockchain are maintained by a network of nodes. In addition to these nodes, masternodes are used to perform special functions on the network such as facilitating instant transactions.

Masternodes are also used as a deflationary tool. Like staking, individuals who run and maintain a masternode are rewarded with a portion of the transaction fees collected by the system. Unlike staking, users must set aside a specific amount of coins as collateral to run a masternode. The effect is the same as that of staking: coins are removed from the circulating supply to counter react the forces of hyperinflation.

DarkSaga requires users to collateralize 2,500 coins to operate a masternode.

5. Private Transactions

Darksend

DarkSaga utilizes Darksend, a decentralized mixing service based on the ConJoin protocol, to enable users to transact privately. Utilizing a system of masternodes, users mix coins in order to obfuscate the source of the coins. Users can specify the number of rounds of mixing to increase anonymity.

Stealth Addresses

DarkSaga stealth addresses allow individuals to provide third parties with a public address for payment. However, the stealth address differs from a typical public address in that it conceals the destination from the payer or the public. SAGA stealth addresses add an additional layer of privacy for users.

6. Additional Applications

SagaSend

SagaSend allows users to send BTC using SAGA. The function uses one or more cryptocurrency exchanges to help facilitate payments and to overcome the numerous regulatory requirements related to payment processors and atomic swap type functions. SagaSend creates a link between DarkSaga and Bitcoin allowing individuals to spend SAGA anywhere BTC is accepted.

Roadmap

EXCHANGES

- Fundraising
- Stex
- Graviex

COMMUNITY

- Community Growth
- Contests
- Airdrops
- Masternode Giveaways

SAGASEND

- SagaSend Development
- Beta Release

WALLETS

- Cosmetic and Security Updates
- SagaSend Update

SOCIAL MEDIA

- Twitter
- Discord
- Telegram
- Reddit
- Medium