White Paper Version 2

PengolinCoin

[PGO]

A Truly Private and Decentralized Cryptocurrency

Abstract

Concern over privacy violations is greater now than in any time in recent history. Comprehensive data and privacy protection laws have not kept up with technology, leaving significant gaps in protections. Centralized banking and monetary systems all keep records of your personal information, account numbers and transaction history. Which, in turn, is monitored by the governments of the world. Your money, who you receive it from, where you are sending it, and your balance, is not private. Along came Bitcoin, but did you know that when you send someone Bitcoin, you are sending them an entire transaction history from your account, including balances? This is hardly the privacy people are entitled to. The solution? PengolinCoin. Unlike traditional ways to send currency globally across borders PengolinCoin is fast and inexpensive. PengolinCoin will use the latest privacy technology zk-SNARK and Sapling protocols. It is the perfect way to send or receive money in today's world.

1. Introduction

Traditional ways of making purchases, such as with credit cards, are not private. Not only does the credit card companies and banks have your personal information but the metadata they sell to third parties can also be used to identify you. This metadata is "anonymized" and transactions, names, and other personal information, are erased before being sold to third party companies. However, research has shown you can be identified with more than 90 percent accuracy just by looking at four purchases, three if the price is included. With just a few data points, it is often possible to ascertain the identity of an individual, even though the data has been scrubbed of identifying information. Recently, it was unveiled that metadata or basic transactional information was being collected by the U.S. government, from millions of Americans not suspected of a crime. A new solution is needed, and that solution is Blockchain Technology. But it is important to understand that not all Blockchains are alike. We at PengolinCoin know that well-informed investors are looking for Blockchains that are both decentralized and anonymous. Some blockchains come close to having these features; but alas, they fall short. For example, the People's Bank of China issuing a Blockchain-based digital currency. This new digital currency will be controlled by the government and therefore privacy and anonymity cannot be guaranteed. It will actually give the Chinese government unprecedented visibility on how its people spend money. PengolinCoin is the privacy coin project that eliminates these concerns. PengolinCoin will use zk-SNARK and Sappling privacy protocols to make transactions private, anonymous, and secure.

Zk-SNARK and Sappling Protocol Technology

The acronym zk-SNARK stands for “Zero-Knowledge Succinct Non-Interactive Argument of Knowledge,” A user can prove possession of certain information, for example, a secret key, without revealing that information, and without any interaction between the prover and verifier.

The Sapling Protocol, uses zk-SNARKs proofs to allow both shielded and unshielded transactions on the blockchain. This is accomplished by utilizing a Spending Key and a Viewing Key. The spending key is synonymous with a private or secret key. The Viewing Key is what is called a user’s public key. The holder of this key can view sent and received transactions. A single Viewing Key enables a user to create new addresses that aren’t related to the ones before it thereby maintain privacy of the user.

Proof of Stake (PoS)

PoS is a type of consensus mechanism in which users of a blockchain-based network have to stake some portion of their coins or tokens, in order to have a chance at verifying transactions in a block. In a PoS system, a forger is chosen via a two-stage pseudo-random process. The main thing that is taken into consideration when a forger is selected for verifying transactions is whether they have a stake in the network. If they have staked their funds, then the amount of their stake is also used to determine their eligibility to validate blocks. Furthermore, the PoS algorithm discourages malicious activity on blockchain networks because a forger would lose their entire staked amount should they try to act dishonestly or tamper transactions. The advantages of using a PoS system is that it’s energy efficient, because unlike a PoW system, there is no mining process involved which consumes a lot of power/resources (electricity), no expensive hardware, no need to learn mining command lines, and everyone can do it!

Hot Staking

PGO can be hot staked by simply installing the core desktop wallet, depositing at least one coin into the wallet, and unlocking the wallet in Staking Only mode. Deposited coins will start to stake after 21 confirmations. With hot staking, the wallet needs to be kept online and running in order for staking to function. Cold staking is already set up in the wallet and will be available in the near future. Rewards are determined by how much you are staking, how long you have been staking, and a randomness factor.

Masternodes

A masternode is an incentivized node, on the PengolinCoin network, with a full copy of the PengolinCoin blockchain. Masternodes are responsible for blockchain validation, and transaction speed. Also, masternodes enhance the functionality and security of the PengolinCoin blockchain. To run a masternode a user must store 100,000 PengolinCoins.

The masternode must always be connected, must use a separate, static IP address, and have some technical competency. A masternode will pay out more consistently while staking is more random. This consistency is to incentivize users to run masternodes because they are an important part of the well-being of the network.

Technical Details

Name: PengolinCoin

Ticker = PGO
Total supply = 100,000,000
Pre-mine = 15,000,000 (11,000,000 used for swap)
Block reward = +/- 22
Block time = 60 seconds
PoS Consensus
Decimal point = 8

Road Map

March 2020

- PengolinCoin launched on March 23, 2020
- Bitcointalk: https://bitcointalk.org/index.php?topic=5234832
- Official mining pool
- Website
- Block explorer
- Social network accounts
- First exchange

April 2020

- White paper v1
- Promotion campaign
- Listing on exchanges
- Community growth

July - September 2020

- Implement new blockchain and new code
- Transition to PoS/Masternodes
- Swap old PGO for new PGO
- Listings on masternode hosting platforms

- Promotional campaign (v2)
- Marketing

September - End of 2020

- New top 100 exchange listings
- Code updates
- Add zk-Snarks and sapling privacy protocols

Long-Term Strategy

- Develop blockchain and cryptographic technologies
- Develop own codebase
- Continually grow community
- Ongoing marketing campaigns
- Increase revenue
- Implement bounties to bring mass adoption
- More partnerships
- Grow the team
- We will continue to separate PengolinCoin from the pack

Join the Excitement!

Links

- Website:

  https://www.pengolincoin.xyz/

- Blocks Explorer:

  https://blockexplorer.pengolincoin.xyz/

- Source Code:

  https://github.com/pengolincoin

- Windows GUI Wallet:

  https://github.com/pengolincoin/PengolinCoin-Core/releases/tag/v2.0.0.1

Social Networks:

- Telegram:
  https://t.me/pengolincoin

- Bitcointalk announcement:
  https://bitcointalk.org/index.php?topic=5234832.msg54081541#msg54081541

- Discord:
  https://discord.com/invite/XTk8u4w

- Twitter:
  https://twitter.com/PengolinC

- Facebook:
  https://www.facebook.com/PengolinCoin-105101314474751

- Reddit:
  https://www.reddit.com/user/PengolinCoin

- Medium:
  https://medium.com/@cryptorigvin

Contact: Contact@PengolinCoin.xyz

****