AudioCoin (ADC) - A Digital Currency For The Music Industry

The music industry has evolved to a point where streaming services (excepting Japan) account for the majority of revenues.

The strategy is currently in process with a number of music industry related organisations (including media, live events, brands, technology providers and brand protection companies).

Latest updates will be posted at https://audiocoin.eu along with our discord channel at https://discordapp.com/channels/342879339202740224/342879339202740224

AudioCoin (ADC) Coin Technical Details

Algo: Scrypt POW/POS

1. Name of Coin : AudioCoin

2. Abbreviation of Coin : ADC (see github.com/aurovine/audiocoin)

3. Max number of coins (Including POS phase) : 10.5 billion total

4. Timings of block (in seconds) : 60 seconds

5. Coins per Block (during pow phase) : 4000 coins per block reduce 5% every week

7. Block number when POS starts : Block number 87752
http://www.presstab.pw/phpexplorer/ADC/block.php?searchinput=87752

8. POS interest per year : Stealth Based up to 18% per year (1.5% per month)

9. Premine in number of coins : 5% or 525 million
(Premine is exclusively for Aurovine Eco-system, 3rd party platform incentives, Dev/Bug Bounties, Rewards, Marketing and Faucets.)

Block Explorer
https://chainz.cryptoid.info/adc/

Technical Overview

Much of our development could not have been accomplished without the open source work already completed by Sunny King and Scott Nadal in developing the Peercoin crypto-currency and of course Satoshi Nakamoto's Bitcoin. Excerpts from the Peercoin whitepaper by kind permission of Sunny King.

We have subscribed to the premise of a proof of stake design for the coin. Under this hybrid design proof-of-work mainly provides initial minting and is largely non-essential in the long run. Approximately 20% of the coin supply will be available for distribution and mining during the proof-of-work stage. The security level of the network is not dependent on energy consumption in the long term thus providing an energy-efficient and more cost-competitive peer-to-peer crypto-currency.

Proof-of-stake is based on coin age and generated by each node via a hashing scheme bearing similarity to Bitcoin's but over limited search space. Block chain history and transaction settlement are further protected by a centrally broadcasted checkpoint mechanism.

Introduction

Since the creation of Bitcoin (Nakamoto 2008), proof-of-work has been the predominant design of peer-to-peer crypto currency. The concept of proof-of-work has been the backbone of minting and security model of Nakamoto's design.
In October 2011 the Peercoin developers realized that, the concept of coin age could facilitate an alternative design (known as proof-of-stake) to Bitcoin's proof-of-work system.

Coin Age

The concept of coin age was known to Nakamoto at least as early as 2010 and used in Bitcoin to help prioritize transactions, for example, although it didn't play much of an critical role in Bitcoin's security model. Coin age is simply defined as currency amount times holding period. In a simple to understand example, if Bob received 10 coins from Alice and held it for 90 days, we say that Bob has accumulated 900 coin-days of coin age. Additionally, when Bob spent the 10 coins he received from Alice, we say the coin age Bob accumulated with these 10 coins had been consumed (or destroyed).

In order to facilitate the computation of coin age, the Peercoin developers introduced a timestamp field into each transaction. Block timestamp and transaction time stamp related protocols are strengthened to secure the computation of coin age.

Proof-of-Stake

Proof-of-work helped to give birth to Nakamoto's major breakthrough, however the nature of proof-of-work means that the crypto-currency is dependent on energy consumption, thus introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees.

A solution had to be found that would offset the need for energy consumption in order to have a decentralized crypto-currency.

The Peercoin developers moved forward with a proof-of-stake model that was discussed among Bitcoin circles as early as 2011.

Roughly speaking, proof-of-stake means a form of proof of ownership of the currency.

Coin age consumed by a transaction can be considered a form of proof-of-stake. The Peercoin developers realized that proof-of-stake could indeed replace most proof-of-work's functions with careful redesign of Bitcoin's minting and security model.

This is mainly because, similar to proof-of-work, proof-of-stake cannot be easily forged. Of course, this is one of the critical requirements of monetary systems - the difficulty of counterfeiting.

Block Generation under Proof-of-Stake

In the hybrid design, blocks are separated into two different types, proof-of-work blocks and proof-of-stake blocks.

The proof-of-stake in the new type of blocks is a special transaction called coinstake (named after Bitcoin's special transaction coinbase). In the coinstake transaction the block owner pays himself thereby consuming his coin age.

The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-of-work blocks. However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved. The hash target that stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (in contrast to Bitcoin's proof-of-work target which is a fixed target value applying to every node). Thus the more coin age consumed in the kernel, the easier meeting the hash target protocol.

Minting based on Proof-of-Stake

A new minting process is introduced for proof-of stake blocks in addition to Bitcoin's proof-of-work minting. Proof-of-stake block mints coins based on the consumed coin age in the coinstake transaction.

Main Chain Protocol

The protocol for determining which competing block chain wins as main chain has been switched over to use consumed coin age. Here every transaction in a block contributes its consumed coin age to the score of the block. The block chain with highest total consumed coin age is chosen as main chain.

This is in contrast to the use of proof-of-work in Bitcoin's main chain protocol, whereas the total work of the block chain is used to determine main chain.

This design alleviates some of the concerns of Bitcoin's 51% assumption, where the system is only considered secure when good nodes control at least 51% of network mining power. First the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, thus raising the cost of attack for such powerful entities. Also attacker's coin age is consumed during the attack, which may render it block contains a duplicate pair as another previously received block, we ignore such duplicate-stake block until a successor block is received as an orphan block.

Energy Efficiency

When the proof-of-work mint rate approaches zero, there is less and less incentive to mint proof-of-work blocks. Under this long term scenario energy consumption in the network may drop to very low levels as disinterested miners stop mining proof-of-workblocks. The Bitcoin network faces such risk unless transaction volume/fee rises to high enough levels to sustain the energy consumption. Under the hybrid design even if energy consumption approaches zero the network is still protected by proof-of-stake. We call a crypto-currency long-term energy-efficient if energy consumption on proof-of-work is allowed to approach zero.

Conclusion

Proof-of-stake designs have become a more competitive form of peer-to-peer crypto-currency to proof-of-work designs due to the elimination of dependency on energy consumption, thereby achieving lower inflation/lower transaction fees at comparable network security levels.

We reserve the right to make modifications to this code for the good of the community and coin. ADC is not designed for speculation, rather a real world application to solve problems and create a level playing field for music industry stakeholders (artists, labels, fans, services). We encourage a collaborative community to help us make the coin succeed with fair rewards for both Development and Coin adoption.

Acknowledgement

References

Babaioff M. et al. (2011): On Bitcoin and red balloons.
Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)
Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.(http://www.bitcoin.org/bitcoin.pdf)
King S. & Nadal S. (2012): PPC White Paper. (http://peercoin.net/whitepaper)