The Peercoin Blockchain
– Briefing Paper –
January 2020

Introduction

Peercoin was launched in August 2012 and is the first blockchain to use the Proof of Stake security protocol. Peercoin also uses Proof of Work for the initial creation of coins.

From the outset, Peercoin was conceived by its developers as an underlying "backbone" for the crypto space.[1] In so doing, they were introducing a concept that has since become known as a 'settlement' or 'base layer'. This shows considerable foresight since at the time, Bitcoin was still being talked about in terms of becoming a currency in the literal sense.

Consequently, Peercoin has been designed to address aspects of Bitcoin that prevent base layer development, in particular: the deflationary element; its high energy consumption and the associated expense; the centralisation of control caused by that expense; the division of interests between block producers (miners) and coin holders; and the reliance of security on transaction fees.

Peercoin's development is ongoing, but its development team believes that these goals are nearing completion, and that Peercoin offers an economic and security model that is secure, cost effective and decentralised. The Team believes that the Peercoin protocol, as described below, merits consideration of inclusion in wider discussions as to the future of the blockchain-based economy.

Peercoin's economic and security model

Cryptocurrencies must have scarcity to have value. Proof of Work is based on the scarcity of electrical power. Peercoin's Proof of Stake is based on scarcity of *time*. Peercoins held in wallets accrue time ("coin days") to enable minting (staking), which is how Peercoin produces blocks and maintains security of the blockchain. Coin days are broadly comparable to the hash rate in POW mining, and accumulating coin days means more minting power.[2] As an incentive to mint, coin holders receive an average of 1% interest in the form of new Peercoins, known as a minting reward.

[1] Peercoin's then lead-developer Sunny King said in October 2013: "I think the cryptocurrency movement needs at least one 'backbone' currency, or more, that maintains high degree of decentralization, maintains high level of security, but not necessarily providing high volume of transactions. Thinking of savings accounts and gold coins, you don't transact them at high velocity but they form the backbone of the monetary systems".

[2] Coin days are subject to security limits. Each time a block is produced, coin holders must wait 30 days before minting again; this is to prevent minters from producing blocks continually, and so keep minting power decentralized. And Peercoins held for 90 days are capped in their minting power; this is to prevent a potential attacker from accumulating power in the network by storing up coin age over an extended period.

Because scarcity of time is not energy dependent, Peercoin holders do not need special or expensive equipment to mint; any device connected to the internet can be used. This allows Peercoin's minting power to be **spread geographically**, and prevents the centralisation of block production seen with Proof of Work security, such as the formation of mining farms. These farms may compromise network security further by relocating to countries where electrical power is cheaper and exposing the network to local politics.

Peercoin restricts Proof of Work to the initial creation of coins which mainly took place in 2012 and 2013; this enabled Peercoin to **avoid centralised initial distribution**, as seen with "initial coin offerings" where coin creators control the allocation of coins. To ensure the openness of Peercoin's creation and distribution, its source code was made publicly available nine days before the launch, so Peercoin's developers had no advantage in mining new coins.

Peercoin's Proof of Work is declining as more mining power is directed at the network, from an annual inflation in the coin supply of 8% in 2013, to 2.8% in 2019. Although Peercoin is designed to allow mining without time limit, since mining helps decentralisation via the sale of coins to new owners, its impact will reduce to a trickle in the coming years. Bitcoin's mining is also declining; its Proof of Work inflation halves every four years and will cease when 21 million bitcoins are created. But Bitcoin has no further means of generating coins; it will have a finite supply. Given that wallets and passwords can be lost by their owners, this makes Bitcoin a deflationary asset.

Peercoin is designed to **avoid such deflation**, as the minting reward allows for a 1% inflation rate which will continue indefinitely, since it is linked to block production. Limited inflation, which is decentralized via coin holders, is at the heart of Peercoin's economic and security model, since coin growth incentivises coin holders to mint, while the steady coin injection discourages hoarding associated with fixed-supply currency models.[3]

Proof of Stake minting also **eliminates the division of interests** between coin holders and miners by aligning the security of the network with the ownership of coins. This is because Peercoin holders are themselves responsible for securing the network, as opposed to Proof of Work that depends on miners who can switch to other networks where mining profits are higher.

[3] In the present version of Peercoin, v 8.4, the 1% inflation rate relates only to coins actively minting. As of Version 9, the 1% inflation will apply to the whole coin supply. This will be achieved by linking the proportion of minting coins to the minting reward, so the fewer that mint, the greater the minting reward for those that do (there may be an upper cap on the reward, to prevent undue accumulation of coins by minters). In practice, rising rewards are expected to incentivise more minting, which then lowers the rewards to an equilibrium.

Peercoin's separation of security from mining means that **security is not affected by market price**. Since minting costs no more than running an ordinary computer, minters don't have to drop out in a price crash or during periods of low market activity.

Low energy consumption means Peercoin needs **no market in transaction fees**. Fees are necessary in Proof of Work to supplement block rewards which decline over time and so keep miners profitable. With Peercoin, minters are rewarded in proportion to their coin holdings by the block reward, eliminating reliance on transaction fees. Transaction fees are still applied in Peercoin, but only to **deter spam transactions**. The fee is fixed at a nominal rate of 0.01 Peercoins per kilobyte of data usage and, upon the transaction being made, the fees are burned by the protocol, which returns the fees' value back to the Peercoin network. There is no reason to increase Peercoin's transaction fee, since the network creates no such need. And a further benefit is that Peercoin won't compete for fees with **secondary layers**.

Conclusion

The growth of the crypto space has made it evident that blockchains will not be able to execute all functions; instead, they will rely on secondary layers or side chains. Many cryptocurrencies are seeking to alter their protocols in line with this realisation.

Peercoin's competitive edge is that it requires no such change in thinking or protocol, because it has been conceived and developed as a base layer *from the beginning*.

The Peercoin network has been growing for this purpose for seven years, focusing on getting the right economic model, combined with decentralised security that can be sustained over the long-term. This makes Peercoin well placed to be a significant contender for base layer solutions.

For further information:

foundation@peercoin.net
peercoin.net