2.1.3 Proof of Work/Proof of Stake

The Proof of Work (PoW) system, in regards to cryptocurrency, was first designed and built by Satoshi Nakamoto, the creator of Bitcoin. The idea inherently refers to a piece of data which is difficult to produce but yet simple for others to look at and verify, allowing for a network or individual to easily prove validity. In Bitcoin, the PoW system helps to ensure the security of the network through block mining. Each node currently deciding to participate in mining is required to go and solve a computationally difficult problem to ensure the new block's validity. The first successful node is allocated a reward.

The PoW system, as a whole, is fair throughout in the sense that a miner with p fraction of the total computational power can win the reward and create a block with the probability p. An individual contributing more computational power will earn the reward more often than an individual contributing less, in spite of the fact that luck plays a factor. Even so, there are some glaring flaws throughout. For one, 51% attacks are a real possibility. Although it gets more difficult to launch a successful one as the hash rate of the network grows, the fact that the Neoscrypt algorithm is essentially designed to be inefficient makes it easier for a very dedicated individual to do so. Besides this, the fact that any PoW network is essentially supported by physically scarce resources—both specialized hardware and electricity—makes the network uneconomical from a resource standpoint.

The Proof of Stake (PoS) system, on the other hand, was first designed and implemented by Peercoin. The idea is simple—instead of mining power, the probability to create a block and receive the associated reward is proportional to the user's ownership stake. An individual stakeholder who has p fraction of the total number of coins in circulation creates a new block with p probability. The reasoning behind the protocol is that the users with the highest stake in the system would have the most interest overall to maintain a secure network. If the network is attacked, it stands to reason that they would have the most to lose. Also, the only way to mount a successful 51% attack on the network in a PoS system would be to acquire a 51% stake of the currency, which would be almost impossible or incredibly expensive for an up-and-coming currency.

The PoS network employed by Sigil is much more advanced than most, as it utilizes a new algorithm created by John Doering called 0% Proof-of-Stake. Essentially, what it does is add another layer of security to the Sigil network by allowing only coins that have sat in your wallet long enough to mature to stake. This "maturity" period starts from the moment that your incoming transaction was broadcast, and lasts for approximately one day. It is not possible to generate a PoS block for inputs that are immature. After this wait, your coins will begin to stake, undergoing a process similar to PoW mining as they attempt to generate a PoS block. The time that it will take to generate this block varies, and it's impossible to predict how much time it will take. Besides luck, it depends on:

- The current difficulty of the network
- The number of coins currently in your wallet
- The number of days your coins have been allowed to mature

Perhaps the most important factor, though, is the idea of "staking power", or "weight." Essentially, the longer that your coins have been maturing in your wallet without generating a PoS block, the more "weight" they have. The formula to calculate this "weight" is simply: (# of Coins) * (Coinage – 1) = Coinweight. The Coinage is calculated individually for every transaction. Any immature transaction will have zero "weight", and not stake at all. Every successful PoS block generation will also reset the "weight" to zero, as if the coins were immature, and the process starts from the beginning. The maximum possible "weight" is reached after sixteen days.

The main difference between traditional PoS and 0% Proof-of-Stake is simple: in a traditional PoS network, you can launch your wallet whenever you want, sync up, generate a few stakes, and shut down until you see fit to stake again. There is no motivation to keep the wallet open, as "weight" is not a factor, and thus your staking doesn't necessarily support the market. If the same strategy is tried with Sigil, doing the same means losing most of your possible PoS blocks, as your coins are not allowed to keep staking.

The optimal strategy in regards to generating the most PoS blocks is to first of all split your coins into smaller portions and place them in separate wallets, so that they can stake independently. If left on its own, the wallet will do this automatically over time, but it's still faster to do manually. Secondly, you want to stake as often and soon as possible, and thus the best way to do so is to keep the wallet open whenever possible. Not only do you get the most Sigil doing so, but you also constantly replay blocks, transactions, messages, and help to secure and maintain the network throughout.

In spite of all this, a PoS network does come with some vulnerabilities. Because of the fact that the network is not aware of anything except for the blockchain, there is nothing physical anchoring the blockchain in reality. As a result, there are many methods that can influence and harm the network. One specifically is called a "bribe" attack, in which the attacker performs a spending transaction he wants to reverse later, builds up