Fractalcoin
A cryptocurrency with percentage fees and Slingshield

Jordan Earls <earlz@earlz.net>

Abstract: Fractalcoin, a fork of Bitcoin, is the first cryptocurrency to implement percentage based fees and Slingshield difficulty adjustment. This combination uses mining pools mining multiple coins to secure the network and ensure that a successful double spend attack will require up to 71% of the network hashing power, rather than 51%.

Introduction
Since it's inception, bitcoin and most of it's forks have faced a dillemia in ensuring that their network remains secure against double spending as rewards for mining drop, especially when rewards are zero. Lower than expected transaction volume has proved to make relying on fixed transaction fees a risky endeavor for coins using only proof-of-work mining. Fractalcoin combats this problem by using percentage based fees of 0.1% to 0.5%, depending on the exact make up of the transaction. This introduces another problem however.

When Dogecoin and other coins had dynamic payouts based on a psuedo-random number generator, it was observed that many multipools stripped loyal miners of their rewards by only mining when the block reward is known to be high. This caused problems with the network difficulty rating by causing it to constantly spike high and then drop down very low. Digishield was created to solve this so that the network is never stuck with slow blocks. Slingshield is a modification to Digishield to further optimize the algorithm to account for multipools only mining when the rewards are made high by transaction fees. This has the effect of making the network secure against even an attempted 51% double-spend attack as well as ensuring that loyal miners are not put at a disadvantage compared to multipools.

Percentage Fees
Percentage based fees are used in Fractalcoin to ensure mining remains lucrative without introducing a significant inflation rate over a long period of time. The percentage based fees are 0.5% when sending coins to an address not in the list of inputs. The fee is 0.1% when sending coins to an address in the list of inputs. Percentage based fees ensure that miners want to include all of the transactions in a block that they can, ensuring all miners are working toward the good of the network.

Slingshield
Slingshield is a fairly simple modification on top of Digishield. Whenever a block contains no transactions, the difficulty adjustment is identical to Digishield. Slingshield becomes activated when transactions in the block outputs coins. Slingshield works by increasing the block target time of 1 minute by a factor of the expected transaction fees. Because of the multipools that will begin mining Fractalcoin when the fees rise though, blocks with many coins spent will not actually take longer to solve.

Slingshield works on the amount of coin outputs, not directly on fees. However, spending so many coins has mandatory transaction fees of at least 0.1%. The fees may by up to 0.5% depending on the exact transaction. So, sometimes spending 100 coins might have a

transaction fee of 0.1 coin, 0.5 coins, or somewhere in between. Slingshield is calibrated to assume the fees will be the lowest value of 0.1%. Slingshield adjusts difficulty by a 0.5% increase for each 1% increase in the expected minimum reward for a block with such transactions. This ensures that there is ample reward to make Fractalcoin lucrative for mining in that block, despite the difficulty increase.

Example
Imagine that the current block's difficulty is 210 and the current block reward is 1 coin. Alice wants to send Bob 100 coins, so she creates a transaction. This transaction might have fees of 0.5%, so lets say the fee is 1.05 coins. The minimum a transaction spending so many coins could be would be 0.21 coin though, which is what Slingshield works on.

So, the block is modified and the total block reward is now at least 1.21 coins. The reward increased by 21%. Slingshield sees this and as such, increases the difficulty of the block by 20%. Multipools see the lucrative reward and switch their miners to Fractalcoin. The multipools increase the network hashing rate suffeciently that the block will still probably be found within 60 seconds.

Double-spending
Alice decided to be evil and wants to double spend those coins she sent Bob. So, she begins to construct her own fork of the Fractalcoin blockchain but with a conflicting transaction in the last block, so that if she builds it successfully she can undo the transaction sent to Bob. However, she immediately realizes that 51% of the hashing power isn't enough. Because of the difficulty increase by 20% and the multipools that hopped on for the lucrative block, her fork is quickly outdone by the legitimate network.

She then has one more idea. Maybe she can't double spend the blocks, but she can throw them away. So, she constructs her own fork with a conflicting transaction that basically throws the coins away. These aren't factored into amount of coins output by the block, so Slingshield doesn't kick in, and she successfully mines the block. However, the transaction she's trying to do has already increased the difficulty, so even though she could mine the block, hers is weaker and as such is instantly orphaned. Alice becomes very sad that she can't double spend her coins.

Adoption
Because percentage based fees are hard to support on some kinds of infrastructure, percentage based fees do not come into effect until 27 days after launch, and are not mandatory until 28 days after launch.

Conclusion
Slingshield and percentage based fees is a successful mechanism by which to take the profit seeking nature of multipools and cause them to tangibly increase network security. This solves the age-old multipool “problem” by ensuring that multipools actually benefit the network, no matter how long they stay mining for at a time. Digishield ensures that a massive decrease in network hashing power is quickly handled and Slingshield ensures that an expected massive increase in network hashing power is properly utilized to secure the network.