So, what is new about Riecoin?

The process of money creation in Bitcoin - referred to as mining - involves executing software that utilizes your hardware running sha256 hashes until a certain criterion is met. This part of the mining process is called generating a "Proof of work". The whole mining process also has a critical role in processing transactions and providing security to the network. It is estimated that all the processing power devoted to Bitcoin mining represents more computing power than several of the largest supercomputers in the world combined. Wouldn't it be great to be able to use all that massive power for something else? Even special purpose hardware was designed for Bitcoin mining. Some consider this a waste of resources, while others argue that supporting a decentralized currency is hardly a waste. We believe that the mining process required for currency to work does not need to include hashing functions as a Proof of Work, and that a "more useful" calculation can be done instead. That's the point of Riecoin: the mining process, besides fulfilling its function to the operation of the network, generates series of prime numbers as a by-product. This prime numbers are of interest to [mathematicians and the scientific community](http://riecoin.org/faq.html#constellation). Riecoin is proof that it is possible to effectively harness all that massive computing power to something useful other than hashing functions. Above all, Riecoin was launched fairly! There were no instamine since the first 576 blocks had no reward. This allowed all users to have the chance to compile wallets despit their OS.

How does the "Proof of Work" work?

**Theory**

Finding a prime number p takes O( log(p) ^ 4 ) work, while verifying if it's prime requires O( log(p) ^ 3 ) using the Rabin-Miller test. That's not much difference, so finding prime numbers is not practical for a PoW.  
  
One possible solution for this is looking for prime number constellations (like twin prime numbers, or triplets, etc), that is n "consecutive" prime numbers. Consecutive in this case means that they are grouped as closely as possible minimizing the distance between the first and the last one. This takes O( log(p) ^ (n + 3) ), while verification still takes the cube of the log. This allows us to make the generation arbitrarily more difficult than the verification.  
  
Difficulty can be adjusted by changing the length of the prime numbers. Riecoin currently uses constellations of size 6 (also known as prime sextuplets) which have the form p, p+4, p+6, p+10, p+12, p+16. So each block represents six prime numbers.

**Practice**

Let S be the sha256 of the first part of the block header (the nonce is not needed).  
In binary, let basep be an 1 concatenated with eight 0's, concatenated with S, concatenated with as many 0's as needed to reach the required difficulty. Let Z be that quantity of 0's.  
  
Find X such that basep + X is the first prime of a prime constellation of size n, where n is hardcoded at 6. The value of X should not be larger than 2^Z: this last restriction removes any chance of using the same actual constellation as PoW for more than one block.  
  
Since S and basep can be calculated from the block header up to the time field, only X needs to be stored in place of the usual nonce.  
  
PoW verification is done using Rabin-Miller primality tests. The intention of the eight 0's before the hash is to minimize the influence that the value of the hash can have on the difficulty of finding a sextuplet.

How is Riecoin different from Primecoin?

* Primecoin uses the Fermat primality test, which has some flaws. Carmichael numbers are not prime and still pass Fermat's test for all bases, however those are relatively rare. Secondly, in general, if Fermat's test says a number is prime, it has at least a 50% probability of being prime. Primecoin uses only one Fermat test with base 2. While base 2 may provide more confidence than the general bound of 50%, still many composites will pass as primes. What's worst, is that Euler-Lagrange-Lifchitz test used for the other primes in the chain assumes the previous number in the chain is prime. So if the chain starts with a number that is not prime, then the Euler-Lagrange-Lifchitz test is not guaranteed to work, and all numbers in the chain may be composite.   
  **Short version**: Primecoin numbers are not guarranteed to be prime, they may be Fermat pseudoprimes to the base 2. There is an infinite list of Fermat pseudoprimes to the base 2 [(oeis.org/A001567)](http://oeis.org/A001567). Riecoin uses enough Rabin-Miller tests with random bases, so the probability of a number that is not prime being accepted by the majority of the Riecoin network is negligible.
* We propose the n/s "range explored (numbers) per second" metric instead of pps (primes per second) or shorter-chains per second. This is the quantity of numbers tested (whether by sieve of explicit primality test) and discarded as not constituting a valid PoW per second. While it is still difficult to compare this number for different difficulties, it is a much better metric: it can be used to meaningfully compare different algorithms, hardware speed, etc as long as you have the same diff. More n/s always means more blocks. For example a mining rig would be advertised as having X n/s@minimum diff. Something similar like "multipliers per second" might be possible for Primecoin, but it wouldn't scale as well when difficulty grows. In Primecoin, PPS is "just for fun" and shorter chains per second may not be accurate to compare the performance of algorithms for full-length chains per second.
* Assuming the [Riemann Hypothesis](http://www.claymath.org/millenium-problems/riemann-hypothesis) and the Hardy-Littlewood k-tuple conjectures are true, by using Hardy-Littlewood constants a miner can estimate the average time before a block is found, allowing profit calculations and to estimate the computing power of the network.
* In Primecoin there is no practical way of estimating the time before finding a block, moreover difficulty 10.1 is easier than 9.9 making it impossible to estimate how secure the network is.
* A centralized checkpoint system is implemented inside Primecoin. While it is disabled by default, if FUD about attacks start to spread, I believe some people will panic and enable it. A centralized checkpoint allows its controllers to perform double spends without any need for any % of hash rate. Can we be sure it will not be hacked and/or abused?
* Riecoin is capped to a fixed amount of coins (84M), but Primecoin has no limit. While it is arguable, we believe our deflationary model - similar to Bitcoin's - is better.
* 1min block speed would bloat the blockchain and create more orphans, stales. We have 2.5min which was tested for years in LTC. I don't know of any 1min coin that has years of testing. I think it's not true that 1min is fast enough for waiting in a line when you buy a coffee: with blocks targeted each minute, you have a 1 in 150 chance of having to wait more than 5 minutes for a block, this would still be unacceptable for some coffee stores. Also, with 2.5 each block requires more work, meaning we will have larger prime numbers sooner.

How do I mine?

You can use the built-in miner using the classic "setgenerate true", or (preferred) you can use the external cpu-miner rminerd, fork of Pooler's cpu-miner.At the moment only a CPU miner exists, but I'm sure a miner that makes use of the GPU will eventually be released.

How does pooled mining work?

Having shares simply be blocks with lower difficulty does not work for pooled mining. Finding a prime sextuplet with small primes is not helpful towards the general goal of finding one with the network's required size.  
  
So the way to implement it is by making pool shares be prime constellations of the same difficulty as desired, but with less primes. So for example if the requirements for a block are a sextuplet with difficulty n, then a quintuplet with the same difficulty could constitute a valid pool share (or quadruplet, or whatever the pool operator wishes).  
  
Note that finding a quintuplet is O(log p) times easier than finding a sextuplet.  
  
Pooled mining works because of the many quintuplets found, eventually one will be part of a sextuplet, thus being a valid block. One drawback of this implementation is that miners may optimize they prime number generation for quintuplets instead of sextuplets, finding more shares but less blocks. If only some miners did this, they would be receiving more than they deserved share of the reward, and if all did this, the reward would be fair but mining this way in a pool would be less profitable than solo mining. To avoid this problem, the pool software must validate that the shares do have the potential to be blocks according to some precomputed sieve. Careful crafting of this sieve will ensure that tuning the mining algorithm for finding blocks instead of shares is still the most profitable way to mine in the pool.

What is the value of finding prime number constellations?

Lots of mathematicians study prime numbers. Many conjectures on prime number constellations and prime number distribution in general rely on the [Riemann Hypothesis](http://www.claymath.org/millenium-problems/riemann-hypothesis), which has a prize of 1M USD for anyone who can prove (or disprove) it. If they are willing to give that much money, it means exploring them should have some value. It's not like we are solving the Riemann Hypothesis with Riecoin, but we will be verifying Hardy-Littlewood k-tuple conjectures (at the moment, for k = 6). Even if the only value of Riecoin's proof of work algorithm is getting people interested in prime numbers, it already is worth trying.

Rabin-Miller primality tests are probabilistic. What if a composite number is accepted as prime?

The probability of a client accepting one number that is not prime is one in 2^80 for each prime in the constellation. This is very low. But this applies to each client, and since each client uses different random bases for testing, the probability of 2 clients accepting a block with a fake prime is 1/2^160. This number is really really low, and it's only for 2 clients: it approaches 0 exponentially as we add clients to the equation. So in the highly unlikely case that someone accepts a fake block, it will surely be orphaned later. It really is not likely that anyone can use this as an attack vector.

Will Riecoin break any world record?

It might. According to [this](http://www.gigablast.com/get?q=&c=dmoz3&d=152016814139&cnsp=0) the record for a prime sextuplet is 559 digits, which should be 1857 bits. Riecoin's starting (and minimum) difficulty is 304 bits, so if it ever reaches 1857 then every new block would be a record breaker.

Update: it did! [click here to download the records](https://sites.google.com/site/anthonydforbes/ktuplets.htm?attredirects=0)

Why 6-tuples and not 5 or 7?

The more the better because it makes verification easier relative to mining. But 7 would have been too difficult to mine, have in mind we need numbers of least 256 bits to hold the hash, and then some more. Minimum difficulty is 304 bits.