Introduction to Blakecoin

Written by Bzyzny
February 8th, 2014
Revision 0.1

Table of Contents:

Credits:

BlueDragon747 – Creator and Main Developer of Blakecoin
Kramble – Developer of Blakecoin on FPGA
kR105 – Added Blakecoin support to Eliopool and compatible cgminer
Vorksholk & smolen – Ported Reaper for Blakecoin
melnikalex – Initial port of cgminer for Blakecoin
knorrly – Added Blakecoin support to Abe block explorer

I know this list is far from complete, I will try to add everyone who deserves credit. If you believe you deserve recognition or have suggestions for who does, please message me on bitcointalk.org. Thank you to everyone who has contributed to Blakecoin, it would not be what it is today without your help! Most of the information in this document is from various sources, I simply organized it into this document to make it easy for new users to get started with Blakecoin.

Introduction:

What is Blakecoin, and why should you care? There are already plenty of new alternatives to Bitcoin, why do we need one more? This is an important question, so I will do my best to answer it. I will start with the basic specifications and some background information, and then continue with more detailed explanations.

Blakecoin Specifications

- Blake-256 hashing algorithm
- 7 billion total Blakecoins, generated over approximately 400-1000 years
- Block reward is 25 + inflation (very small amount of inflation; it is based on block height and current difficulty)
- No halving or decrease in block reward
- 3 minute target block time
- Difficulty adjustment every 20 blocks (~ 1 hour)
- Block maturity in 120 blocks (plus 20 block buffer)

Blakecoin is the first cryptographic currency to utilize the Blake-256 hashing algorithm for its Proof of Work (PoW). This algorithm was one of the SHA-3 finalists and was chosen for several reasons. Although it was not the winner of the SHA-3 competition, Blake-256 has properties which make it better suited for use in crypto currencies than Keccak and the other candidates. Please refer to the “Benefits” section for more details.

BlueDragon747 launched Blakecoin October 6th, 2013. It was pre-announced and there was no premine. Originally mining was CPU only, but shortly after launch, GPU mining and FPGA mining became possible. For the first several weeks, only solo mining was possible. However, the Eliopool and MPOS pool software has been ported to support Blakecoin and there are now a handful of pools available. Development of the tools and software related to Blakecoin has been gradual but steady because quality control has been a primary focus of the developers. Presently the Blakecoin ecosystem is reaching a level of maturity that provides a strong foundation for future development and widespread adoption.

While Blakecoin is a general use crypto currency, Bluedragon747 is also working on an infrastructure to allow Blakecoin to be used as a currency ecosystem for online video games. Any online video game would be able to adopt the system, creating a micro economy for gamers. Imagine being able to make money from gaming by withdrawing the money you earn in the game, or being able to make micro payments for digital goods in games in a consistent manner. There are many possibilities with this kind of system. Since Blake-256 is relatively non resource intensive, it is possible to mine Blakecoin in the background while playing video games or doing other tasks on your computer without causing significant performance loss.

Benefits:

There are several benefits that Blakecoin provides and I will try to outline them here. Much effort and research was put into designing Blakecoin to be well rounded and practical for widespread and long term usage. To summarize, Blakecoin is efficient, focused on the long term, balances transaction speed with network security and performance, supports merged mining, and provides fair and adaptive incentives for miners.

The source code is based closely on Bitcoin 0.8.6, but several changes where made to make Blake-256 the core hashing algorithm. Blakecoin did not make many major changes aside from the hashing algorithm since stability and security are paramount. Bitcoin has been thoroughly tested and proven to be very secure and stable, so introducing experimental and untested code to Blakecoin was avoided as much as possible. However Blakecoin differentiates itself from Bitcoin significantly by using an improved hashing algorithm and using unique parameters for difficulty adjustment and block rewards.

The hashing algorithm Blake-256 was chosen for Proof of Work because it has several qualities which make it ideal for use in crypto currencies. Energy efficiency is a primary advantage; mining Blake-256 uses roughly 3% less electricity than SHA-256D and roughly 14% less electricity than mining Scrypt. Blake-256 is also capable of generating considerably more hashes per second than most, if not all, other hashing algorithms. This is advantageous for crypto currencies because of the Law of Large Numbers, which is a probability theorem. Simply put, the more hashes per block, the more likely it is that the block will be found near the target block time. It also helps pools to more accurately reward miners for their percentage of shares. The Blake-256 algorithm is also advantageous because it is a simplified and parallelized design. This means that it is highly efficient on GPUs and FPGAs, and if or when ASICs are made for Blake-256 it also will be highly efficient.

The idea that ASIC resistance is important for crypto currencies has become widespread, however it is based on a fallacy. The premise is that ASICs are expensive and therefore make mining impractical for the average person. However, the production of ASICs is inevitable if a coin becomes popular enough, as is the case with Litecoin. Although Scrypt did a good job of stalling the creation of Litecoin ASICs, they are soon to be released. The properties that made Scrypt ASIC resistant are now the same properties that will make Scrypt ASICs exorbitantly expensive. Therefore in the end, trying to make a coin resistant to ASIC implementation only serves to make it more infeasible for the average person to mine it once ASICs are produced. This is why Blakecoin has been designed to be ASIC friendly. The simplistic nature of the Blake-256 algorithm makes it easier and cheaper to implement in silicon, so if or when Blake-256 ASICs are manufactured, they will be considerably less expensive and also considerably more power efficient than SHA-256 or Scrypt ASICs. GPU mining is excellent because it provides the flexibility to mine just about any coin, but ultimately it is a test bed to determine which coins are good enough to warrant production of dedicated hardware. One more advantage of Blakecoin in this regard is that due to it's support for merged mining, the efficiency of an ASIC would be compounded since it will be possible to mine multiple coins at once.

The block reward system is unique to Blakecoin, it is the first to have the foresight to continue giving incentive to miners far into the future. The total amount of BLC (Blakecoin) to be mined will be 7 billion, which seems like a lot until you take into account that it will take hundreds of years to mine them all. While it may be unlikely that this type of technology will be used that long, Blakecoin allows for the possibility. The inflation rate is very small, but provides an incentive for miners to continue mining even when the difficulty increases substantially. The base block reward is constant to help provide a stable economy and network. Halving the block reward causes shocks to the market and to the network hashrate, which can be bad for the long term viability of a coin.

It is reasonable that your first reaction may be, “Why would Blakecoin have inflation, if the advantage of crypto currencies is that they are deflationary?”. It is important to point out that the inflation rate is very small, and almost negligible. Presently the inflation added to each block is around 0.003BLC. The inflation is based on the current difficulty and current block height. It's purpose is to reward miners for continuing to mine long term and to provide incentive to continue mining even when difficulty increases substantially. A rough estimate for the inflation added to each block in ~10 years would be less than 20BLC (for total block reward of 45BLC), assuming the difficulty would be around 10 million (about 2000x the current difficulty). This system will help to smoothly ease the transition for miners as difficulty increases, rather than causing a sudden and large drop in coins earned. BlueDragon747 is also considering placing a cap on inflation, so that even if the difficulty skyrockets, the inflation will not dilute the market. Like everything else about Blakecoin, it is designed for long term stability.

Many of the newer crypto currencies have target block times near 1 minute or less, but Blakecoin uses 3 minute target block time for several reasons. It is well known at this point that block times less than a minute tend to cause issues like more orphaned blocks, problems with network synchronization, and bloated blockchains. The 3 minute target was also chosen because it provides higher security since it requires more effort to perform a 51% attack than networks with faster block times. Finally, in order for merged mining of other Blake-256 based coins to work, the block time of Blakecoin must be greater than the block times of the merged mined coins. This means that any merged mined Blake-256 coin can have a block time of 3 minutes or less.

Support for merged mining is a primary focus of Blakecoin, because it is another way to increase efficiency. The division of mining resources, which is prevalent in the Scrypt coin community, is detrimental for several reasons. Each network is in competition, and therefore must supply their own hashing power. This results in each coin network being significantly less secure than if the hashing power of multiple coins where combined. Merged mining reduces the duplication of work and increases security for all the coin networks that a mined together. This also is beneficial to miners since you do not have to choose only one coin to mine, you can mine several at once. This is a significant advantage since it can be difficult to know which coin will be most profitable.

In conclusion, there are numerous benefits to Blakecoin that make it unique and innovative. This overview is far from complete but should provide a good starting point for people interested in learning about Blakecoin. I will continue to add more information and generally improve this document, so please remember to check for newer revisions.

Links:

Blakecoin Official Website: **http://blakecoin.org**

Main Blakecoin Thread: **https://bitcointalk.org/index.php?topic=306894.0**

Blake Algorithm Info: **https://131002.net/blake/**

Blakecoin Pools:

- **http://eu1.blakecoin.com**
- **http://ny1.blakecoin.com**
- **https://blakecoinpool.org**

Blakecoin Exchanges:

- **https://www.atomic-trade.com/**
- **https://c-cex.com/index.html**

BLC