Dual-Purpose Mining Innovation: Primecoin, Curecoin, Gridcoin

Bitcoin’s proof-of-work algorithm has just one purpose: securing the bitcoin network. Compared to traditional payment system security, the cost of mining is not very high. However, it has been criticized by many as being “wasteful.” The next generation of alt coins attempt to address this concern. Dual-purpose proof-of-work algorithms solve a specific “useful” problem, while producing proof of work to secure the network. The risk of adding an external use to the currency’s security is that it also adds external influence to the supply/demand curve.

Primecoin

Primecoin was announced in July 2013. Its proof-of-work algorithm searches for prime numbers, computing Cunningham and bi-twin prime chains. Prime numbers are useful in a variety of scientific disciplines. The Primecoin blockchain contains the discovered prime numbers, thereby producing a public record of scientific discovery in parallel to the public ledger of transactions.

- Block generation: 1 minute
- Total currency: No limit
- Consensus algorithm: Proof of work with prime number chain discovery
- Market capitalization: $1.3 million in mid-2014

Curecoin

Curecoin was announced in May 2013. It combines a SHA256 proof-of-work algorithm with protein-folding research through the Folding@Home project. Protein folding is a computationally intensive simulation of biochemical interactions of proteins, used to discover new drug targets for curing diseases.

- Block generation: 10 minutes
- Total currency: No limit
- Consensus algorithm: Proof of work with protein-folding research

- Market capitalization: $58,000 in mid-2014

Gridcoin

Gridcoin was introduced in October 2013. It supplements scrypt-based proof of work with subsidies for participation in BOINC open grid computing. BOINC—Berkeley Open Infrastructure for Network Computing—is an open protocol for scientific research grid computing, which allows participants to share their spare computing cycles for a broad range of academic research computing. Gridcoin uses BOINC as a general-purpose computing platform, rather than to solve specific science problems such as prime numbers or protein folding.

- Block generation: 150 seconds
- Total currency: No limit
- Consensus algorithm: Proof-of-work with BOINC grid computing subsidy
- Market capitalization: $122,000 in mid-2014

Anonymity-Focused Alt Coins: CryptoNote, Bytecoin, Monero, Zerocash/Zerocoin, Darkcoin

Bitcoin is often mistakenly characterized as "anonymous" currency. In fact, it is relatively easy to connect identities to bitcoin addresses and, using big-data analytics, connect addresses to each other to form a comprehensive picture of someone's bitcoin spending habits. Several alt coins aim to address this issue directly by focusing on strong anonymity. The first such attempt is most likely *Zerocoin*, a meta-coin protocol for preserving anonymity on top of bitcoin, introduced with a paper at the 2013 IEEE Symposium on Security and Privacy. Zerocoin will be implemented as a completely separate alt coin called Zerocash, in development at time of writing. An alternative approach to anonymity was launched with *CryptoNote* in a paper published in October 2013. CryptoNote is a foundational technology that is implemented by a number of alt coin forks discussed next. In addition to Zerocash and CryptoNotes, there are several other independent anonymous coins, such as Darkcoin, that use stealth addresses or transaction re-mixing to deliver anonymity.

Zerocoin/Zerocash

Zerocoin is a theoretical approach to digital currency anonymity introduced in 2013 by researchers at Johns Hopkins. Zerocash is an alt-coin implementation of Zerocoin that is in development and not yet released.

CryptoNote

CryptoNote is a reference implementation alt coin that provides the basis for anonymous digital cash. It was introduced in October 2013. It is designed to be forked into different implementations and has a built-in periodic reset mechanism that makes it unusable as a currency itself. Several alt coins have been spawned from CryptoNote, including Bytecoin (BCN), Aeon (AEON), Boolberry (BBR), duckNote (DUCK), Fantomcoin (FCN), Monero (XMR), MonetaVerde (MCN), and Quazarcoin (QCN). CryptoNote is also notable for being a complete ground-up implementation of a crypto-currency, not a fork of bitcoin.

Bytecoin

Bytecoin was the first implementation spawned from CryptoNote, offering a viable anonymous currency based on the CryptoNote technology. Bytecoin was launched in July 2012. Note that there was a previous alt coin named Bytecoin with currency symbol BTE, whereas the CryptoNote-derived Bytecoin has the currency symbol BCN. Bytecoin uses the Cryptonight proof-of-work algorithm, which requires access to at least 2 MB of RAM per instance, making it unsuitable for GPU or ASIC mining. Bytecoin inherits ring signatures, unlinkable transactions, and blockchain analysis–resistant anonymity from CryptoNote.

- Block generation: 2 minutes
- Total currency: 184 billion BCN
- Consensus algorithm: Cryptonight proof of work
- Market capitalization: $3 million in mid-2014

Monero

Monero is another implementation of CryptoNote. It has a slightly flatter issuance curve than Bytecoin, issuing 80% of the currency in the first four years. It offers the same anonymity features inherited from CryptoNote.

- Block generation: 1 minute
- Total currency: 18.4 million XMR
- Consensus algorithm: Cryptonight proof of work
- Market capitalization: $5 million in mid-2014

Darkcoin

Darkcoin was launched in January 2014. Darkcoin implements anonymous currency using a re-mixing protocol for all transactions called DarkSend. Darkcoin is also notable for using 11 rounds of different hash functions (blake, bmw, groestl, jh, keccak, skein, luffa, cubehash, shavite, simd, echo) for the proof-of-work algorithm.

- Block generation: 2.5 minutes
- Total currency: Maximum 22 million DRK
- Consensus algorithm: Multi-algorithm multi-round proof of work
- Market capitalization: $19 million in mid-2014