Gridcoin

Crypto-Currency using Berkeley Open Infrastructure Network Computing Grid as a Proof Of Work

Rob Halford (contact@gridcoin.us)
May 23rd, 2014

Abstract

A distributed crypto-currency utilizing a hybrid proof-of-work design based on scrypt, skein, groestl and cubehash for the security portion of the proof of work, and Proof Of Boinc for the remaining portion of the Proof Of Work.

Target Audience

Cryptologists, Scientists, Engineers, Financial Analysts, Accountants, Investors, Programmers, and crypto-coin enthusiasts.

Introduction

After Bitcoin (Created by Satoshi Nakamoto in 2008) evolved and matured, waste heat has increased exponentially to secure blockchains of itself and clones. The mining operation generates heat by testing millions of combinations of blockhashes. To replace this operation with a more useful proof-of-work, Gridcoin introduces a novel algorithm based on work done in Boinc projects, in addition to requiring a multi algorithm hash solution that is more secure than bitcoin's single sha256 hash algorithm.

Mining participants may choose any official boinc project including but not limited to Cancer Research, HIV, Alzheimer's, World Community Grid, Malaria, Mad Cow, DNA sequencing, 3d farm rendering, nanotechnology, protein structure modeling, Quantum chemistry, Drug

discovery, Microgravity, Neutron star search, Cryptographic research, Large Primes, weather models, and much more.

Distributed Peer To Peer Model

Gridcoin uses a peer-to-peer network structure with no central authority to check the validity of blocks, no central authority for checkpoints, and no single point of failure for any operations. A failure from a single boinc project will NOT cause Gridcoin to stop operating. No credit check outage will cause Gridcoin to stop operating. No central authority will disrupt production operations.

Proof Of Work Verification System

When users participate in Boinc projects, they are required to join Team Gridcoin (Designating ownership of Boinc Credits). As they perform work on projects, they generate cobblestones, or individual clock cycle credits of work for that project. The BOINC distributed servers share these credits and calculate a Recent Average Credit, or Total Credit Average over 30 days. Gridcoin uses the RAC figure as an indicator of the magnitude of work performed by node-project.

Proof Of Mining

In order for a Gridcoin node to mine, they must request a block template to be filled in with a Boinc CPID, Project Name, RAC, Email Hash, Boinc Public Key, and proof that the block is not in the chain already within the public Proof Of Boinc Lookback period (dynamic difficulty adjustment). If any of these steps fail, the miner will not mine, or the block will not be accepted by the network.

Fraud

To prevent fraudulent blocks from being accepted, for example, when a miner purports to own an account, or falsifies the recent credit, or attempts to mine without a valid project, the block will be verified by another 3rd party node on the network. The 3rd party node calls netsoft-online, a very well distributed BOINC credit check farm. If the block can be verified, the block will be accepted and confirmed; and this identical process repeated by a minimum of 6 nodes before becoming a permanent part of the block chain. If the block cannot be confirmed because the internet is down or the credit node is down, Gridcoin will move into its disaster recovery mode. In DR Mode, the node searches for a previous instance of the CPID. If the CPID is

found in the chain, gridcoin will validate the block within a tolerance parameter based on the historical data. In this way, Gridcoin can tolerate outages.

Anonymity and Theft of Accounts

Since some Boinc users wish to remain anonymous, Gridcoin requires no permanent unique identifier per user. Gridcoin does not transmit any sensitive unique identifier through the network. Instead, it transmits the Project CPID, a public identifier that only reveals the user credit per project. Gridcoin maintains a Skein hash algorithm to determine the origination of the owner of the CPID in a non-deterministic way. When a boinc account is stolen, the user merely needs to change the master e-mail address to regain control. The system will automatically recover. Previously mined CPID-blocks are non-deterministic and cannot be stolen from the chain to receive new credits.

Efficiency

Since Gridcoin is biased towards providing energy efficiency, a built in Skein-Groestl-Cubehash miner is provided that may solve PoB blocks up to one half of the saturation level of the daily block quantity with a prerequisite of a GPU mined Scrypt-Groestl-Cubehash block. This raises the power efficiency of the Gridcoin network by 50%.

Innovative Security Features - Advanced Encryption Standard

Gridcoin innovates with a new feature to require Skein-Groestl-Cubehash results to be encrypted with AES and tested before block solutions can be submitted. This minimizes the chance of porting the integrated miner into GPUs.

Dynamic Reward Subsidy

To prevent faulty project abuse and equalize GPU Boinc projects vs. CPU, Gridcoin calculates real time network 14 day moving average for Boinc for the entire network. Subsidies are based on average performance.

The dynamic subsidy calculation, promoting BOINC competition is:

```
(Currency)Subsidy =
(VerifiedMinerRecentAverageCredit/[ProjectType]NetworkRecentAverageCredit)*150
(With a ceiling of 150, and a minimum of 5 GRC).
```

Innovative Extensions to Bitcoin

Gridcoin extends the Block storage specification to store the CPID, project name, RAC, PoB Difficulty. Gridcoin adds many new commands to the RPC console: execute, allows commands to be added without modifying the RPC protocol.

For example, execute backupwallet, will backup the private keys.

Listitem network will produce a list of average Boinc RAC for the entire network.

Dynamic Proof Of Boinc Difficulty Algorithm

The Proof Of Boinc Difficulty is designed to increase as the number of participants with valid CPID:Projects increase.

PoBDiff = (TotalNetworkProjectCPID(count):(per)Project(within T-14 days))/576

SQL Queries

Gridcoin allows full SQL queries against the block chain. In the future, Gridcoin will allow the user to audit and track sent coins providing confirmation by transaction in real time.

Conclusion

Gridcoin is the first cryptocurrency that successfully diverts wasted energy towards useful scientific research, operating as a distributed peer to peer network with no central authority, and provides greater efficiency using normal consumer grade hardware.

References

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)

Berkeley Open Infrastructure Network Computing Grid: BOINC:
An open source middleware system for volunteer and grid computing.
(http://boinc.berkeley.edu/)

Waste heat and power dissipation: Inefficient Heat Generation:
(http://en.wikipedia.org/wiki/CPU_power_dissipation)

Globally Unique Identifier: GUID
(http://en.wikipedia.org/wiki/Globally_unique_identifier)