Gridcoin - Rewarding research instead of mining

This whitepaper describes how Gridcoin makes it possible to reward running scientific simulations with cryptocurrency in a completely decentralized way.

1. BOINC

BOINC is a system for distributing the workload of scientific simulations. Users of BOINC have a client running that solves work units (WU) for the specific projects. A work unit consists of code and specific parameters for which the code is run. After the work unit is completed the BOINC client sends back the results to the BOINC servers, where the results are analyzed.

One example for a BOINC project is the World Community Grid **[WCG]**, which consists of various other projects, for example to solve cancer [**Cancer**] or beat Ebola [**Ebola**] . SETI@home [**SETI**], which looks for signs of alien life by monitoring electromagnetic radiation from space for patterns, is another well-known project. In total there are about 40 BOINC projects, but only the BOINC projects on the [**Whitelist**] help users earn Gridcoins.

The information which researcher has computed how many work units is stored on the BOINC server. The unit of work done is a **credit** (cobblestone), which is 1,000 double-precision MFLOPS based on the Whetstone benchmark [**Whetstone**]. The **RAC** is the average amount of credits earned per day.

A **CPID** (Cross Project Identifier) is a number that links together the participation of a single user in all the different projects with a single common identifier, with a CPID one can see the research done by one user over all different projects this user participates in.

There are also teams in BOINC, users can join teams and the work done by each member of the team is added to get the work done by the team. It is necessary for a Gridcoin-researcher to be a part of team “Gridcoin”, which on some projects is listed as “gridcoin”, lowercase. .

2. Neural Network

Gridcoin uses a distributed system to come to a consensus how much work was done by each user. For this each node (Gridcoin client) asks each BOINC project server, what the current RAC of each member of team Gridcoin is. Using the Google Distributed File System (GDFS) the nodes exchange the information regarding which user has done how much work. This information is hashed, so each node does not see the exact information from each other node, but the hash can be compared and it can be found out, if the hash of this node is the same as the majority hash of all nodes.

To become a part of the Neural Network, a researcher's Gridcoin client has to send a "**beacon**" containing the CPID and the wallet's address. This is a transaction with a very small amount of Gridcoins, that links the CPID and wallet-address of this researcher in its meta-information, so that this information is now forever stored in the blockchain.

3. The blockchain

A blockchain stores all information about all transactions that have taken place. When one knows all transactions, one also knows the current balance of each address. In **Proof of Stake [POS]** a node is randomly chosen among all nodes to add the next block to the blockchain. A block contains all transactions that have taken place in the network since the last block. The node adding this block is rewarded with Gridcoins. When the node adds a block, it also chooses the next node randomly among all nodes. However, this is not done completely at random, but weighted by the amount of Gridcoins each node holds.

When the probability is weighted by the current amount of Gridcoins, the reward that one gets on average for adding blocks is directly proportional to the amount of Gridcoins in possession (as this is the probability to be chosen to add the next block and get the reward) and thus can be seen as an interest for the user.

4. Rewarding Researchers

Gridcoin does not only want to reward holders of the coin (as in pure proof-of-stake coins such as Peercoin), but wants to reward researchers. Because of this there is an additional reward depending on the amount of research done. This information is read from a superblock. In some blocks, so called superblocks, the majority opinion from the distributed Neural Network, which user has done how much

work is also saved as a hash. These blocks are generated once a day. The current amount of research done by each CPID stored in the last superblock can be viewed on **[SUPER]**. If a node gets chosen and the hash this node contains about the amount of work done by each user is the same as the majority hash stored in the Neural Network, then this node gets to stake the next block and everything starts again. If the hash is not the same as the majority hash, the node gets "punished" for trying to cheat the system and does not stake, but chooses the next node that gets a chance to stake. The actual reward the node gets then depends on the RAC for each project for this user as stored in the superblock.

At first the amount of coins per project this user would get if he was only running this project is computed:
coinsPerProject = (averageUserProjectRACsincelastPayment / averageTeamGridcoin ProjectRACsinclelastPayment) * Time since last payment in days * coinSupplyPerProjectPerDay

As of now the **dailyCoinSupplyPerProject** is the same for each project, so
coinResearchSupplyPerProjectPerDay = dailyResearchyCoinSupply/#Projects

averageUserProjectRACsincelastPayment and **averageTeamGridcoinProjectRACsinclelastPayment** means that in case there were several superblocks since the last payment the average RAC of all those superblocks is used.

The research reward is then the sum of the rewards for each whitelisted project:

researchRewardForNode = sum of coinsPerProject over all whitelisted projects

The **totalRewardPerNode** is then the reward for the research done by this node plus the reward that any node gets for staking a block:
totalRewardPerNode = inflationRewardForNode + researchRewardForNode

The **inflationRewardForNode** depends on the time that passed since the last stake is chosen in a way that it leads to an interest rate of 1.5% per year.

The rewards that contain only **inflationRewardForNode** and no **researchRewardForNode** are often called PoS (Proof of Stake) rewards, whereas the rewards containing **inflationRewardForNode** plus **researchRewardForNode** are called Proof of Research rewards.

4. Coin Supply and security measures

With a fixed **dailyResearchCoinSupplyPerProject** it would not be ensured that the inflation rate is always the same; it could vary depending on how many new researchers join the project. Because of this, the amount of average payouts over the last 14 days is used as a lagging indicator of how much was paid out recently - if very little was paid out in the last 14 days more is paid out now and the other way round.

dailyResearchCoinSupply = MaxDailyEmissions - AvgDailyPaymentsPaidInLast14Days

There are also a few security rules. For example Time since last payment in days can not be greater than 6 months, otherwise there is no payment and the coins paid out per user does have a very high upper limit (~20000) per stake.
The **MaxDailyEmissions** is set to 50000, which at the current coin supply means an research-inflation of around 5%. This rate however will grow smaller, as the coin supply grows but the amount of coins produced per day stays the same. Additionally the **inflationRewardForNode** is chosen, so that the interest inflation is around 1.5% per year.

5.Setting it up

For setting up BOINC and the Gridcoin client to earn Gridcoins by running scientific simulations on your computer follow the tutorial on gridcoin.us

6.Outlook

Commercial Projects: If it is possible to reward users for running specific code on their computers with cryptocurrency, they could also run commercial simulations on their computers basically for free as they are already rewarded by the newly generated cryptocurrency. This would make it possible to offer computing-intensive services much cheaper than is possible now.

Pool mining: Making it possible for users to earn Gridcoins by only pointing their BOINC client at the email address of a pool

7. Links

[WCG] https://secure.worldcommunitygrid.org/

[Cancer] http://www.worldcommunitygrid.org/research/hdc/overview.do

[Ebola http://www.worldcommunitygrid.org/research/oet1/overview.do

[SETI] http://setiathome.ssl.berkeley.edu/

[Whitelist] http://www.gridcoin.us/Guides/whitelist.htm

[Whetstone] https://en.wikipedia.org/wiki/Whetstone_(benchmark)

[POS] https://peercoin.net/assets/paper/peercoin-paper.pdf , specifically this implementation: http://bravenewcoin.com/assets/Whitepapers/blackcoin-pos-protocol-v2-whitepaper.pdf

[SUPER] http://www.gridresearchcorp.com/gridcoin/?result&t=CPID_Leaderboard