Gridcoin - Performing Meaningful Scientific Computations Instead of Inverting Hashes with Proof of Work

Gridcoin Development Team
Technical Whitepaper
teamgridcoin.slack.com

August 22, 2017

Abstract

This whitepaper describes how Gridcoin makes it possible to reward running scientific simulations with cryptocurrency in a completely decentralized way. Gridcoin is heavily based on Bitcoin [1] with the outstanding exception that Proof of Work where energy is wasted in inverting a hash function is replaced with the novel approach of Proof of Stake [2] linked to Distributed Proof of Research [3], developed on purpose for gridcoin. The voting mechanism embedded in the blockchain which allows to choose which scientific projects to include in Proof of Research is outlined. In conclusion, an outlook is given on how Gridcoin could complement the way science is funded, sparking competition between traditionally funded science and gridcoin funded science.

1 Introduction

Gridcoin [6] is a decentralized, open source math-based digital asset (cryptocurrency) which performs transactions peer-to-peer cryptographically without the need for a central issuing authority. Gridcoin securely rewards volunteer distributed computing performed upon the BOINC [5] platform in a decentralized manner. Available projects in BOINC in 2017 range from attempting to cure

diseases like cancer [11,12,13], ebola [11], AIDS [11] and virus Zika [11], through orbit analysis and reconstruction of asteroids [14], through simulating earth in different ages to assess climate change [15], through mathematical research [16,17], through identification of subatomic particles [18] to scanning the sky for gravitational waves [19] and extraterrestrial intelligence [20].

Although there are other configurations, a typical node runs both the BOINC client to download, execute and report results of scientific computations and the Gridcoin client. The gridcoin client performs several functions: like a bitcoin wallet it allows to transfer money from different addresses, it keeps the blockchain with transactions up to date talking to other nodes and verifying each new block for validity and tries to stake other blocks on the blockchain by collecting new transactions. The coinstake in the proposed new blocks for the own wallet corresponds to the amount of work done on BOINC expressed in gridcoins.

TODO: do nice figure about single node with Gridcoin/BOINC.
TODO: do nice figure about network of nodes running Gridcoin/BOINC.

1.1 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.

TODO: update project list One example for a BOINC project is the World Community Grid [11], which consists of various other projects, for example to solve cancer or beat Ebola. SETI@home [20], 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.

1.2 Gridcoin Client

TODO:

1.3 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 The steps involved are:

- Install BOINC
- Add projects to BOINC
- Install and configure Gridcoin wallet so that it is linked to BOINC
- Acquire gridcoins and move them to your wallet
- Send a beacon so that the wallet CPID is persisted in the blockchain
- Wait until client manages to stake first block with PoS and DPoR reward for your wallet.

2 Neural Network

TODO: explain that the name is misleading.

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 [21] 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, seminal concept invented by Satoshi in 2009 [1], 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 [2]), 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, as in any other consensus based cryptocurrency. The actual reward the node gets then depends on the RAC (Recently Averaged Credit [22]) for each project for this user as stored in the superblock.

To understand RAC, we first look at the *cobblestone* [22]. The *cobblestone* is a unit of measure defined as follows: it is 1/200 day (=7 minutes and 12 seconds, 432 seconds) of CPU time on a reference computer that does 1 Gigaflop (= 1 billion floating point operations per second) based on the Whetstone benchmark. A *cobblestone* in other words correspond to 432 seconds * 1 Gigaflop = 432 billion floating point operations.

Recently Averaged Credit is computed as follows: the daily average of cobblestones in last week plus half of the daily average of cobblestones during two weeks ago plus fourth of the daily average during three weeks ago and so on.

We hereby define:

γ : this is the average RAC done by a user on a particular BOINC project p since last payment to user u identified by *CPID*.

Γ : this is the average RAC done by all users partecipating in Gridcoin on a particular BOINC project p since last payment to user u.

τ : this is the time expressed in days since last payment to user u.

Θ : this is the available gridcoin supply per day assigned to BOINC project p

G : this is the constant number of gridcoins created per day on the gridcoin network.

n : this is the number of BOINC projects in the whitelist. Partecipants in whitelisted projects do receive a reward in gridcoins for their computational effort.

The ratio

$$\gamma/\Gamma$$

is the percentage of work done by user u on BOINC project p in respect to all other gridcoin users working on project p.

The amount of coins σ for project p the user u gets if he was only running project p is computed:

$$\sigma = (\gamma/\Gamma) \cdot \tau \cdot \Theta$$

As of now the Θ is the same for each project, so

$$\Theta = G/n$$

γ and Γ are calculated so that in case there were several superblocks since the last payment the average RAC of all those superblocks is used.

The *researchreward* for user u is then the sum of the rewards for each whitelisted project:

$$researchreward = \sum_{p=1}^{n} \sigma(p)$$

The *totalreward* for user u is then the reward for the research done by this node plus the reward that any node gets for staking a block, called $inflationreward$ in the next formula:

$$totalreward = inflationreward + researchreward$$

The $inflationreward$ 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

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

4.1 Coin Supply and security measures

With a fixed daily research coin supply per project ($\Theta = G/n$) 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 p. 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.

$$G = MaxDailyEmissions - AvgDailyPaymentsPaidInLast14Days$$

There are also a few security rules. For example time since last payment in days (τ) 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 gridcoins, which at the current coin supply means an research driven inflation of around 5

5 Voting Mechanism

6 Transaction Speed

TODO: Bitcoin [1] transaction speed is 7 TPS. Visa/Mastercard is 30 TPS.

6.1 Segregated Witness

possible implementation in gridcoin? block size for sure, but compressing step? TODO: ask developers

6.2 Proximity of neighbours

describe proposal about having nodes connecting to geographical neighbours and still have some random connections. discuss mathematically some implications...

7 Outlook

7.1 Commercial Projects

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.

7.2 Mining Pool

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

7.3 Gridcoin Funded Science

TODO: gridcoin funded research

8 Conclusion

One gridcoin a day takes diseases away (TODO: just joking here)

9 References

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* , 2009, available from `https://bitcoin.org/bitcoin.pdf`.

[2] Sunny King, Scott Nadal, *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake* , 19.08.2012, available from `https://peercoin.net/assets/paper/peercoin-paper.pdf`.

[3] Rob Halfoerd, *Crypto-Currency using Berkeley Open Infrastructure Network Computing Grid as a Proof Of Work* , 23.05.2014, available from `https://www.gridcoin.us/images/gridcoin-white-paper.pdf`.

[4] *Gridcoin*, Rewarding Volunteer Distributed Computing 2014-2017, available from `http://www.gridcoin.us`.

[5] *BOINC, Open-source software for volunteer computing* , 2002, available from `http://boinc.berkeley.edu`.

[6] *Gridcoin Entry on Wikipedia* , 30.08.2016, available from `http://en.wikipedia.org/wiki/Gridcoin`.

[7] Andreas M. Antonopoulos, *Mastering Bitcoin* , O'Reilly, 01.06.2017.

[8] Aleksander Berentsen, Fabian Schr, *Bitcoin, Blockchain und Kryptoassets* , Universitt Basel, 2017.

[9] Roger Wattenhofer, *The Science of the Blockchain* , Inverted Forest Publishing, 2016.

[10] Devin Williams, *Cryptocurrency Compendium: A Reference for Digital Currencies* , Darknetreferences llc, 22.06.2017.

[11] *World Community Grid* , available from `http://www.worldcommunitygrid.org`.

[12] *GPUGRID.net* , available from `http://www.gpugrid.net`.

[13] *Rosetta@home* , available from `https://boinc.bakerlab.org/`.

[14] *Asteroids@home* , available from `http://asteroidsathome.net/boinc/`.

[15] *Climate Prediction.net* , available from `http://www.climateprediction.net`.

[16] *yoyo@home* , available from `www.rechenkraft.net/yoyo/`.

[17] *Collatz Conjecture* , available from `http://boinc.thesonntags.com/collatz/` .

[18] *LHC@home Classic* , CERN, Geneva, available from `http://lhcathome.cern.ch`.

[19] *Einstein@home* , available from `http://einsteinathome.org`.

[20] *Seti@home* , Berkeley, University of California, since 1998, available from `http://setiathome.berkeley.edu`.

[21] *Google Filesystem* , entry on Wikipedia, available from `http://en.wikipedia.org/wiki/Google_File_System`.

[22] *Cobblestone, Recently Averaged Credit* , entry on BOINC wiki, available from `http://boinc.berkeley.edu/wiki/Computation_credit#Recent_Average_Credit`.

10 Credits

The authors are hereby introducing how Gridcoin works and submit this paper as entry for a bounty for a technical whitepaper issued by the Gridcoin community. The authors credit entirely Rob Halfoerd [2] and the Gridcoin community for the ideas and technical work expressed in this paper.