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

Gridcoin Development Team
Technical Whitepaper
teamgridcoin.slack.com

August 30, 2017

Abstract

TODO: rework abstract

Gridcoin [6] is a decentralized, open source math-based cryptocurrency which performs transactions 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].

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

An increased quality of living in a society often coincides with an increase in that societys ability to freely gather and process data. Distributed processing, also known as grid computing, offers a tool by which massive quantities of data can be processed at speeds tens of thousands of times faster than any centralized super computer. This speed is directly proportional to the advancement of processing technology, currently progressing in accordance with Moores law.

At the same time, the Idle Processing Potential (IPP) which already exists in digital societies is severely underutilized. From cell phones to personal computers to office workstations, the combined IPP of the world overshadows even the most robust decentralized super-computer, Bitcoin. Gridcoin seeks to create a decentralized and sustainable distributed processing network which prioritizes both the utilization of IPP and the creation of a free to host ecosystem for researchers and individuals with data to process. To accomplish this goal, Gridcoin has created a block-chain based digital asset which rewards individuals and entities which volunteer their IPP to the grid computing network, BOINC. A single GRC represents the value prescribed to a volunteered unit of IPP on the BOINC network. The Gridcoin blockchain is secured through Proof of Stake. Rewards are distributed through a protocol developed by Gridcoin called Distributed Proof of Research, or DPoR.

BOINC, The Berkeley Open Infrastructure for Network Computing, is an open-source distributed processing network which provides scientists and enthusiasts with a means to host data for free. BOINC has been operating since 2002 and has and continues to process data that helps map the Milky Way, detect near earth asteroids, find prime numbers, fold proteins, test cures and vaccines, test chemical and molecular combinations, Search for Extraterrestrial Life (SETI), and more.

By directly rewarding those who volunteer their idle processing power to BOINC, Gridcoin creates an ecosystem in which valuable data, or a worthwhile project, is defined by an open market of science instead of a market of pay-to-play. In other words, volunteers will move their IPP to projects which they deem of value with no need to consider the reward they will receive.

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.
TODO: do nice figure about BOINC architecture, maybe take it from some

BOINC paper...

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 up a network node to earn gridcoins

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   Distributed Proof of Research

Editor's note: this chapter is sourced from reference [23].

Each participant helps performing research by computations in Gridcoin's network. The network average is similar to difficulty in PoW mining. As the network average rises it becomes harder to get the same magnitude so if you want to keep getting the same reward you would have to add more compute power if we have an environment of a rising network average. If the price rose significantly more compute power would come on board, raising the network

average, making it harder to get the same reward, just like difficulty in Proof of Work.

4.1 Proof of Stake

Proof-of-Research (PoR) is an algorithm, which combines a scheme to reward Miners for their work with an extremely secure block finding mechanism. This mechanism uses Peercoin's [2] Proof of Stake in Novacoin's [TODOref] and Blackcoin's [TODOref] improvement of it. In Proof-of-Stake, currency is not mined, but minted as yearly compound interest. For this the Researcher needs a Wallet with Gridcoins already inside it. As a mint mechanism Proof-of-Stake uses the stake of the holder itself. The more stake he acquires the higher is the probability that he will mint a block to himself.

To calculate the interest reward, coin-age is used. Coin-age is the stake of the investor times the days he held it for. If the investor Bob holds 50 Gridcoins for 3 days, he has acquired 150 coin-age. The higher the coin age, the larger will be the reward compared to the target reward. Once a block is found, the coin age is consumed and starts over again.

Novacoin enabled Proof-of-Work as a stand alone function next to Proof-of-Stake [TODOref]. This means work can be calculated separately from interest and allows for separate hash targets.

Blocks are generated to meet a certain set yearly hash target for the whole network, for example a 1

Gridcoin has eliminated the possibility of a 51

These improvements were already made by Blackcoin, which Gridcoin, in an effort to keep up with current technology has implemented. Blackcoin also included the [Zerocash] protocol, a process enabling anonymous transactions. For now this feature has been disabled from the wallet. Potentially this could be used in Gridcoin to guarantee that BOINC accounts cannot be tracked and as a result hijacked.

BOINC participation is not required to receive a PoS payment. A wallet that is not associated with a BOINC account is called an Investor.

4.2 Proof of BOINC

To prove his contribution of BOINC work a Researcher installs the BOINC software on his PC. He chooses a Project from the Current BOINC Whitelist [TODOref]. Only projects from the Current BOINC Whitelist will yield a reward. The whitelist is update regularly. The Researcher registers at the project with his email and is granted a CPID (cross project identifier), which keeps track of his unique credits. If the system is now conscious of the email, it automatically knows its pairing CPID. At the moment this is done through Netsoft-online, which will not remain a permanent solution. Netsoft also acts as a credit checking farm, next to BOINC stats [TODOref], ensuring that the credits claimed by the owner of a CPID, have the same value as what is stored in the project and later the block chain. The Researcher then starts downloading

his work from the server. When he is finished with computing this work container, he sends it back to the server together with a recommendation of credits to be granted for this workload. The server compares this recommendation with another one and then grants the lower credit to both Researchers.

To standardize this unit the Researcher calculates his Recent Average Credit (RAC). RAC consists of a daily acquired credits average.

TODO: adjust this formula

This means that Credits older than a week are only weighted half as much. When t=0 (during the first acquistion of credits) RAC=Credits . It is difficult to calculate an accurate prognosis for RAC, since Credits tend to be payed out sporadic.

With this RAC a recent savings account (RSA) is created. It keeps track of a potential overflow of magnitude. The magnitude for a single project is calculated with:

TODO: adjust this formula

NRAC is the Average of RAC included in the blocks that have so far been mined with RAC from a single project. If no block has been found so far for this Project, a reward of 30 will be granted for every block. If the calculated reward is is greater than the current maximum block subsidy, the overflow is stored in the RSA. The payout is delivered as soon as a Proof-of-Stake Block has been found by a researcher. The factor 100 ensures that the Researcher's RAC is greater than 100 before he receives any additional subsidy on top of his Proof of Stake interest for every found block. Gridcoin uses a lookback period of 6 months, to check if the credit has been gathered later than 6 months ago. Credit older than 6 months is therefore disregarded. A single Researcher can accrue rewards in a Research Savings Account across multiple devices for up to 6 months. The payments are subject to caps in the Maximum Block Subsidy. The Maximum Block Subsidy is the maximum reward that can be accrued per block from the Research Savings Account, and also serves as the daily limit of how much credit can be added to the Research Savings Account.

4.3 Proof of Research

To tie these two systems together and create a protocol that is both Proof-of-Work and Proof-of-Stake, but not wasteful of its resources in doing so, values from both algorithms are stored in the block header to provide a point of reference and cryptographic proof. Next to the normal Proof hash of Blackcoin, Gridcoin introduces the hash of the BOINC email together with the distributed client public key, which is used to calculate the CPID. This is called the CPID hashing algorithm. While the CPID is public, it cannot be used, or even stolen by another user, since he also needs the email for that, which only has its hashed value stored. Any invalid CPID is rejected, meaning that the CPID needs to be genuine, and the user has signed up with team gridcoin. The user's magnitude

is verified by parsing the XML as a 3rd party. This is described as Accuracy.

The verification through Netsoft and other credit checking farms will only be done during the first 6 confirms of a block. Once it is verified, no further evidence is needed. Both rewards are calculated together. As shown in the above reward calculation coin-age is already a part of the function. If somebody with no BOINC work to account for, an investor, finds a block, the values are simply left blank. "Difficulty" is adjusted dynamically similar to Kimoto's Gravity Well [TODOref]. A Monte Carlo simulation has been run to test the fairness of the network, the output [TODOref] and the source code [TODOref] can be reviewed. There is also a google docs [TODOref], to assist in understanding the variables.

4.4   Research Age

Research Age was created as a way to eliminate the cap on how many coins a single CPID could earn in a single day. The cap was initially created as a security measure but lead to reduced competition and CPID splitting. Research Age works much like Coin Age. As time passes and as more credits are earned your owed balance increases and when enough is owed if your wallet is connected to the network and unlocked to stake you will receive your reward. What a researcher is owed is commonly referred to as their Research Savings Account or RSA. A video explaining proof of research is [TODOref].

4.5   How Gridcoin is created

Gridcoin is created daily from two activities, Proof-of-Stake and Proof-of-Research. Proof of Research is produced at a targeted rate of about 50'000 coins per 1000 blocks. A factor is used to adjust rewards to achieve this target and is called a Magnitude Unit and is stored in the blockchain. If the number of coins generated is too low the Magnitude Unit increases, this increases the number of coins paid for a certain magnitude, if the number of coins generated is too high the Magnitude Unit decreases, this decreases the number of coins paid for a certain magnitude. This has the effect of balancing Proof-of-Research payments with Proof-of-Stake payments. Effectively, if fewer researchers are helping to secure the network, the incentive is increased. The second activity is Proof-of-Stake, and it is produced at an target rate of 1.5

4.6   Proof of Research Beacons

A beacon must be sent to the network to advertise a new CPID. This is performed automatically from the wallet if it is unlocked. The cost is .00011 Gridcoin and must be done once every six months. This beacon allows the Neural Network to know that it must look for that CPID's research credits in whitelisted project credit reporting files. You must stake one block after the beacon is sent before you begin to accrue research owed, the lookback period is 6 months for what a researcher is owed but it looks back to the last staked block, not from when the beacon was sent. To stake a block you must start with some coins, these can be purchased from an exchange or acquired from one of many faucets, or through the IRC channel faucet and tipping system. The more coins you

begin with the faster you will stake your first block, however, to help new researchers with low coin balances stake their first block a stake weight bonus is added, a balance of 100 coins should have no problem staking it's first block in less than 5 days provided that the wallet is online and unlocked for staking all the time. The initial age coins must be before they are able to stake is 16 hours.

5   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% per year.

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.

5.1 Gridcoin as TOP 500 Supercomputer

We saw in the previous chapter that one cobblestone (or one BOINC credit) corresponds to 432 billion floating point operations. We try now to extrapolate the current speed of general BOINC users and the subset of BOINC users who run also the gridcoin client.

On *boincstats.com*[24] for August 26, 2017 we read following numbers: on this day BOINC useres produced 3'034'366'125 cobblestones. Gridcoin users produced a subset of that amout: 513'112'244 cobblestones. To convert the cobblestones in billion operations per second, we multiply them first by 432, to get the floating points operations done in one day. We then divide by the number of seconds in one day which is 24 hours at 3600 seconds = 86400 seconds.

$$gigaflops = (cobblestones \cdot 432)/(24 \cdot 3600) = (cobblestones \cdot 432/86400) = cobblestones/200$$

Following formula above, we convert the cobblestones for BOINC users and Gridcoin users into billion operations per second:

- BOINC users did 3'034'366'125 cobblestones, this is converted to the speed of 15'171'800 gigaflops or 15'171 teraflops or 15.171 petaflops.

- The subset of BOINC users who run also gridcoin client did 513'112'244 cobblestones, this is converted to the speed of 2'565'560 gigaflops or 2'565 teraflops or 2.565 petaflops.

- The number above teach us that gridcoin users on August 26, 2017 are 2.565/15.171 = 16.9% of BOINC users

We now look at the TOP 500 supercomputer statistics, that it is adjusted every six month. We take for reference the list of June 2017 [25].

- BOINC users with 15'171 teraflops are ranked 6th between supercomputers *Sequoia* and *Cori*.

- gridcoin users with 2'565 teraflops are ranked 49th between supercomputers *Tianhe-1A* and *cascade*.

If we forget for one moment that Bitcoin does not allow flexible computations, but consistently attempts to invert only and always the same hash function. What would be bitcoin ranking in TOP 500 supercomputer list on August 26, 2017? According to [26], bitcoin speed on this day was 6'354'668.57 terahash 80'704'290.84 petaflops or 80'704'290'840 teraflops. From this numbers we understand that calculating one hash costs 12'700 floating point operations.

The stated Bitcoin difficulty of 923'233'068'449 (August 26, 2017) which is a number of 40 binary digits (1101011011110100111110101010010110100001) tells us that a hash needs to have the first 40 bits set at zero in order to get the coinbase reward for the block. To date, the coinbase reward is 12.5 bitcoins (TODO: check if difficulty is explained correctly).

The fastest supercomputer in TOP 500 list is Sunway TaihuLight of National Supercomputing Center in Wuxi, China with a speed of 125'435.9 teraflops. Bitcoin would be by far the fastet supercomputer in the world and outperform by factor 643'391!

5.2   Gridcoin Power Consumption estimate

We start to calculate the consumption of Gridcoin closest relative, Bitcoin. We follow the approach outlined in [27] for the Bitcoin Energy Consumption Index.

- Calculate total mining revenues

- Estimate what part is spent in electricity

- Find out how much miners pay per kWh

- Convert costs to consumption

The Bitcoin Energy Consumption Index assumes that miners will ultimately spend 60% of their revenues on operational costs on average. For every 5 cents that were spent on operational costs it is assumed that 1 kilowatt-hour (kWh) was consumed. [27]

Price movements can be small or large, but new energy-hungry machines won't all appear overnight. Realistic behaviour is introduced by linking price dynamics to the expected time required for producers to fully respond to a changing situation. [27]
//TODO: add what BECI estimates on August 2017
//TODO: add the same for Ethereum
//TODO: give examples for Federal Swiss Railway Consumption
//TODO: give example for CERN

//TODO: add estimate for BOINC users
//TODO: add estimate for gridcoin users

//TODO: Calculate CO2 impact.

5.3 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%. This rate however will grow smaller, as the coin supply grows but the amount of coins produced per day stays the same. Additionally the $inflation reward$ is chosen, so that the interest inflation is around 1.5% per year.

6 Voting Mechanism

7 Transaction Speed

TODO: Bitcoin [1] transaction speed is 7 TPS. Visa/Mastercard is 30'000 TPS.

7.1 Segregated Witness

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

7.2 Proximity of neighbours

8 Outlook

8.1 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.

8.2 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

8.3 Gridcoin Funded Science

TODO: gridcoin funded research

9 Conclusion

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

10 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`.

[23] *Proof-of-Research* , entry on Gridcoin wiki, available from `http://wiki.gridcoin.us/Proof-of-Research`.

[24] *boincstats.com* , BAM! account manager and BOINC statistics, available from `http://www.boincstats.com`.

[25] *TOP 500 Supercomputers list* , June 2017, available from `https://www.top500.org/lists/2017/06/7`.

[26] *Bitcoin Charts* , estimation of Bitcoin speed , available from `https://bitcoincharts.com/bitcoin/`.

[27] *Bitcoin Energy Consumption Index*, estimation of Bitcoin power consumption, availabe from `http://digiconomist.net/bitcoin-energy-consumption`.

[28] *Ethereum Energy Consumption Index*, estimation of Ethereum power consumption, availabe from `https://digiconomist.net/ethereum-energy-consumption`.

11   Appendix

11.1   Terminology

- *bitcoin* : TODO

- *peercoin* : TODO

- *gridcoin* : TODO

- *ethereum* : TODO

- *golem* : TODO

- *cryptocurrency* : TODO

- *BOINC* : TODO

- *CPID* : TODO

- *beacon* : TODO

- *BOINC server* : TODO

- *BOINC project* : TODO

- *BOINC client* : TODO

- *cobblestone* : TODO

- *RAC* : TODO

- *superblock* : TODO

- *Proof of Work* : TODO

- *Proof of Stake* : TODO

- *Proof of Research* : TODO

- *transaction* : TODO

- *block* : TODO

- *blockchain* : TODO

- *consensus* : TODO

- *51% attack* : TODO

11.2   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.