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

Gridcoin Development Team
Technical Whitepaper
teamgridcoin.slack.com

October 23, 2017

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.

Contents

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.

5.1 Cobblestone

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.

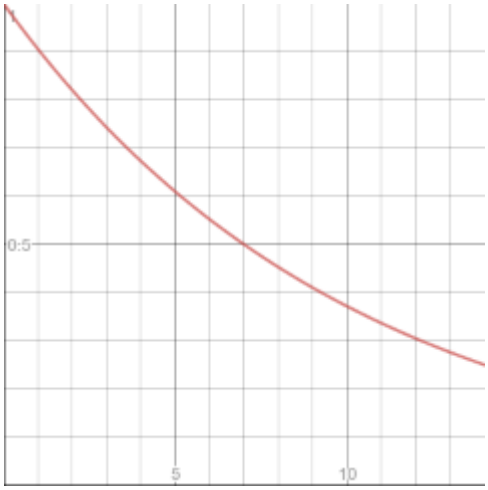
5.2 Recently Averaged Credit (RAC)

Recently Averaged Credit is calculated every time a user is granted new credit in form of cobblestones. Credits are exponentially averaged with a given half life of one week. Following explanation and figures are taken from [31]:

First, we define a decay function over seven days (t is given in days):

$$d(t) = \mathrm{e}^{-t \cdot ln(2)/7} \tag{1}$$

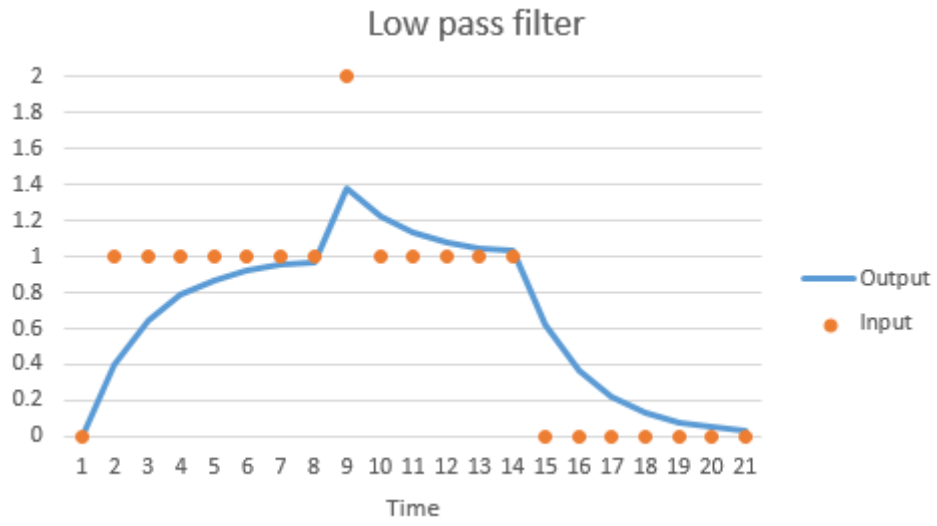
As you can see in the graph below after one week the value is exactly halve, a week later it is again halved. Also note that after a half day the value has dropped to 0.95. It is a continuous mechanism. 7 is said to be the half life of the function. [31]



We now take an infinite impulse response low-pass filter with α as smoothing factor:

$$new\_value = \alpha \cdot old\_value + (1 - \alpha) * new\_input \tag{2}$$

The following graph gives an impression on how the above function behaves. As the input jumps to 1 the output slowly follows and wants to go to 1 as time passes. When the input changes this just repeats. This is called low pass because the output will only follow slow changes, at relevantly low frequencies. The inputs fast short jump to 2 didnt really make it to the output. [31]



To get the formula for Recent Average Credit, we use the decay function $d(t)$ as smoothing facgtor in the infinite impulse response low pass filter:

$$RAC(new) = RAC(old) \cdot d(t) + (1 - d(t)) \cdot credit(new) \tag{3}$$

where $credit(new)$ is the credit in cobblestones for a calculated workunit issued in instant t.

5.3 Gridcoin Payout to a user running multiple projects

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.

5.4 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 $inflationreward$ is chosen, so that the interest inflation is around 1.5% per year.

5.5 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 2'565'561 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 terahashes/s 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!

5.6 Gridcoin Power Consumption estimate

We start to calculate the consumption of Gridcoin closest relative, Bitcoin. We use first the approach explained in [29], where it is assumed that an ASIC miner (a dedicated hash processor) calculates with 1 Watt of power one Gigahash/s. TODO: For example, we look at a common bitcoin ASIC hardware like the Antminer S9. This device computes 14 THash/s using 1350 W of power, so 14'000 GHash/s/1350W = 10.37 GHash/Wm this makes our assumption 10 times smaller. END TODO. According to [26], bitcoin speed on August 26, 2017 was 6'354'668.57 terahash/s or 6'354'668'570 gigahash/s or 6'354'668'570 W. These are 6.354 GW of power. They are equivalent to the power produced by 6 large nuclear power plants. Over one year, which has 365 * 24 hours (=8760 hours), we get 6.354 GW * 8760h = 55'661 GWh or 55.661 TWh/year.

By comparison, the Swiss Federal Railways consume about 3 TWh/year, and CERN in Geneva 1TWh/year.

Another approach outlined in [27] for the Bitcoin Energy Consumption Index, they get 16.2 TWh/year as consumption estimate for last year.

- 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]

Ethereum, another common cryptocurrency consumes with the above method 5.5 TWh of power in one year [28].

To calculate power consumption of BOINC on September 2, 2017, we look first at the daily cobblestones added in this day: 3'300'282'122 cobblestones. The subset of Gridcoin users did 489'559'755. These numbers roughly compare to the numbers used in the previous chapter to estimate BOINC and gridcoin speed, taken on August, 22, 2017. We now take following assumption: half of the cobblestones are computed with a standard CPU like an Intel Core i5 and half with an average GPU like Nvidia GTX 1060. The Intel Core i5 features 4

cores times 4.57 GFlops = 18.28 GFlops with 77W and the 1060 graphic card does 3'850 GFlops with 120W of power. By diving by 200 we get first the speed in GFlops on September 2, 2017: 16'501'410 GFlops for BOINC and 2'447'799 GFlops for Gridcoin. Power calculation of Boinc becomes:

$$16501410/2 \times 77/18.28 + 16501410/2 \times 120/3850 = 35011228W = 35.011MW$$

$$35.011MW \times 24h \times 365days = 306696MWh = 0.307TWh$$

35 MW can be compared to the power produced by a middle sized power plant in the Alps.
In one year, BOINC consumes about 0.307 TWh. Similarly, Gridcoin power calculation gets:

$$2447799/2 \times 77/18.28 + 2447799/2 \times 120/3850 = 5193522W = 5.193MW$$

$$5.193MW \times 24h \times 365days = 45491MWh = 0.045TWh$$

This calculation assumes that most power to run Gridcoin is in Proof of Work and that running the client is almost negligible compared to the PoW part.
If we assume that one household roughly consumes 5 kW, then Gridcoin power consumption corresponds to 1000 households. It is like a medium village of 4'000 people in the mountains.

5.7 CO2 impact

We calculate emissions from electricity generation based off figures from the EPAs eGRID emission factors based on 2012 data published in 2015. On average, electricity sources emit 0.554 kg CO2 per kWh (0.5925 metric tons CO2 per MWh). State CO2 emissions per kWh may vary greatly in accordance with the amount of clean energy in the energy supply (Vermont: 0.002495 kg/kWh ; North Dakota: 0.938255 kg/kWh). [30]

Using the above mentioned averaged factor and the calculations done in the previous subsection, we calculate the CO2 impact for the following frameworks regardless of their size and purpose:

- Bitcoin: 55.661 TWh/year = 32.94 millions metric tons CO2 per year
- Ethereum: 5.5 TWh/year = 3.26 millions metric tons CO2 per year
- BOINC: 0.307 TWh/year = 0.18 millions metric tons CO2 per year
- Gridcoin: 0.045 TWh/year = 0.027 millions metric tons CO2 per year

//TODO: find some things to compare which also produce 32 millions metric tons per year. It has to be something ugly.

6 Voting Mechanism

7 Transaction Speed

TODO: Bitcoin [1] transaction speed is 7 TPS. Ethereum is 14 TPS. Visa/Mastercard is 30'000 TPS. Bitshares claims it is 100'000 TPS.

7.1 Segregated Witness

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

7.2 Proximity of neighbours

Most blockchain algorithms are built over a random network. Each node connects randomly to other nodes regardless of their network position. To improve transaction speed it would be advisable to choose neighbours which are in proximity of the node seeking new connections. The node could traverse periodically existing connections and establish with a metric how far the node is. It could prune the connections which are farthest and substitute them with other random connections.

There are several metrics which could be used:

- Using geographical position as approximation for network proximity: there are geolocation services that can extract an approximate geographical position starting from an IP number.
- Using network hop count and latency: the node could ping each existing connection and retrieve how many nodes are in between (network hop count) and how much time a packet needs to reach the other node (network latency).

The above mentioned algorithm should be tailored so that the network keeps connected to avoid islands with their own fork of the blockchain.

8 Gridcoin Security

9 Outlook

9.1 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.

9.2 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

9.3 Gridcoin Funded Science

Although the scientific method is the cornerstone of modern society, it has also some dark sides or at least it can be futher ameliorated.

The advent of Internet did a lot to increase communication between scientists. It also introduced the problem of plagiarism [TODO]. For the increasing amount of papers, there is not enough and competent people to guarantee an indipendent and competent peer review [TODO]. Sometimes, papers are not available for free but only through expensive subscribtions (remember Aaron Schwartz [TODO]). It is possible to read a paper, but seldomly the source code of software in the paper is made available to the public. So, it is very difficult to test and indipendently what it is written in the paper, unless a considerable amount of work is invested to replicate the software. Datasets are often kept secret to discourage competitors, although most of the time they are put togheter with many from the taxpayer. The significance problem [TODO] points to another problem: it is easy to collect money for mastodontic projects inline with the mainstream of science thinking, but it is very difficult to get even little funding to test an idea which is outside of mainstream. As a personal opinion: huge amounts of money are spent in search of dark matter, while the electrodynamic theories of Universe are disregarded. (TODO: maybe remove this sentence)

If gridcoin would introduce a fix amount in the coinbase of each block with empty input and output a special gridcoin address named 'Gridcoin Funding', the network would collect gridcoins to that special address for each block added to the blockchain. People with an idea who would like to get funded, they would first submit their proposal in form of a whitepaper to the gridcoin community plus a gridcoin address to receive fundings plus the amount of gridcoins needed to fullfill the project. If the proposal fits some basic prerequisites, a special Gridcoin poll will be created on the blockchain asking the community to get funds for the project. In this special poll the gridcoin address of the project and the requested sum of gridcoins will be hardcoded. If the community approves the poll, funds will be automatically sent to that gridcoin address.

Getting all fundings in the beginning are normally a bad motivator. So there will be a mechanism which will pay out the amount to the gridcoin address split in fixed intervals, for example monthly. There will be a mechanism to issue a second poll to ask to stop of fundings, in case the project is not performing as expected.

On September 10, 2017, the market capitalization of Bitcoin was 67'641'887'163 $composed by a circulating supply of 16'556'575 of bitcoins at a price of 4'085.50$. If one percent of that bitcoins would have been spent to a similar fund described above, the fund would have about 676 million dollars available for projects.

Malaria is a diffuse disease in Africa but pharmaceutical companies are not investing in medecines for it, not because they are bad as in any good conspiracy theory, but simply because they can not afford to pay the research and development bill with the money they would collect from poor people with that disease. Imagine for a moment a pharmaceutical company asking for a 100 million dollars from the gridcoin fund to start research on malaria cures. Although utopic,

the scenario is not completely unthinkable, viewed the numbers of bitcoin in the previous paragraph.

Or imagine a hypothetical researcher in Electrodynamics using gridcoin funds unifying electromagnetism and gravitation and wiping out some phantastillion tons of dark matter from the Universe.

Or imagine Elon Musk funding the settlement of humans on Mars with gridcoins.

Having traditionally funded science compete against gridcoin funded science could spark the next scientific revolution since the Age of Enlightenment.

10 Competitors

10.1 Golem Network

Golem grand vision is about a global, open sourced, decentralized supercomputer that anyone can access. It's made up of the combined power of user's machines, from personal laptops to entire datacenters. Anyone will be able to use Golem to compute (almost) any program, from rendering to research to running websites, in a completely decentralized and inexpensive way. The Golem Network would like to achieve a decentralized sharing economy of computing power, where anyone can make money 'renting' out their computing power or developing and selling software. [35]

Golem rewards are done through Ethereum tokens. Developers are required to develop computational tasks following a certain API, so that tasks can be distributed to users willing to compute them. Developers purchase Golem tokens and give them to users who are calculating for them.

At time of writing, Golem implements a distributed CGI rendering prototype as showcase of Golem abilities. However, Distributed Rendering is not something difficult to implement. BURP is a BOINC project that implements it [36]. The Global Processing Unit project also implements a distributed rendering mechanism among other functionalities [37].

10.2 Science Power and Research Coin (SPARC)

SPARC is an Ethereum token which will soon experience its own Initial Coin Offering (ICO).

Like Gridcoin, SPARC is initially leveraging existing demand and infrastructure. The alpha version of SPARC network connects to the BOINC network and rewards participant nodes with SPARC coins for computational work performed. Researchers and developers requiring computing power purchase

SPARC tokens from an exchange and attach them to their projects. These tokens are distributed to the participant nodes in proportion to work performed. SPARC tokens can then be exchanged directly for computing power from the network or traded for conventional currency on an exchange. [34]

In short at time of writing, SPARC is rewarding BOINC work with premined tokens through a centralized website. By contrast, Gridcoin is rewarding researches on a dedicated blockchain in decentralized manner.

10.3 Einsteinium

Einsteinium (shorted with EMC2) is a Bitcoin-like currency with a philanthropic side goal of funding scientific research. It lets community members vote on which worthwhile scientific research projects the proceeds should be awarded. The coin was launched on March 1st 2017. [33]

EMC2 automatically donates 2% of every block mined to the Foundation Fund to be used for donations. The mining of Einsteinium is divided into Epochs: each Epoch mines 36000 blocks of coins and is targeted to last approximately 25 days. Every 25 days, at the end of each Epoch, a new ground breaking scientific cause is selected to receive Einsteinium Foundation funding. [33]

Like Bitcoin, Einsteinium is a distributed peer-2-peer digital currency released without any premine. EMC2 implements the primary innovation of Wormhole Mechanics. To reward long term miners each Wormhole Event occurs randomly during each epoch and is 180 blocks long; with a reward of 2970 EMC2 per block. [33]

Einsteinium coin uses a Proof of Work scrypt algorithm and will have a total of 299 million coins . 2.5% of each block will go to the Einsteinium Foundation with 2% to be given to science projects and .5% going towards faucets, give-aways. and marketing. Einsteinium had a good launch and there was no premine. [33]

Einsteinium is therefore already implementing what it is described in the chapter about Gridcoin funded science but does not reward users for performing BOINC computations.

11 Rationale about investing in Gridcoin

The current Bitcoin price surge (October 2017) has similarities to the dotcom bubble in the beginning of the millenium. The dotcom bubble created as side effect all Internet services we are using today.

The reason why there is high demand of Bitcoin is threefold:

- The Bitcoin supply is limited. The embedded mining algorithm of Bitcoin halves the bitcoin reward for any new block in the blockchain every 4 years and stops creating Bitcoins when 20.67 million bitcoins are created. By 2021 most existing bitcoins in circulation will be minted.
- Bitcoin is currently used by many players, including big investors, to buy other minor cryptocurrencies and to fund new companies that use cryptocurrencies as crowdfunding mechanism.
- Bitcoin is seen by many as digitalized gold and many put their money into bitcoin as long term investment.

Bitcoin has two main drawbacks: we saw in the previous chapter that Bitcoin can not be used as mean to exchange goods between people as its transaction speed is too low. We also saw that Bitcoin is not enviromentally susteinable: the algorithm which protects and verifies transactions and creates new blocks is consuming too much power.

It is reasonable to think that soon or later the regulator will prohibit Bitcoin due to enviromental concerns or at least that the mindset of people will turn to other more eco-friendly cryptocurrencies, especially as the consequences of climate change will be the more visible.

Gridcoin finds a way to consume the energy wasted in Bitcoin to the benefit of mankind: the energy used to secure the blockchain of Gridcoin is also used to advance scientific research in fields where a great amount of computation is needed.

For the sake of completeness we mention here another ecofriendly cryptocurrency with a bright future: Solarcoin [38]. Solarcoin is a Proof of Stake cryptocurrency where little energy is needed to secure the blockchain. Additionally, people running solar installations on their roofs are awarded one solarcoin for each megawatthour their solar installation produce. Awards are retroactive, but need to be proved by documents verified by the grid responsibles and by a non password protected website showing the current production of the solar installation.

12 Conclusion

In this technical whitepaper we first introduced BOINC software to perform scientific computations and the gridcoin wallet. We gave a brief overview of the underlying blockchain technology and explained how Proof of Stake in combination with Proof of Research is used to reward BOINC researches with gridcoin. We gave an estimation of gridcoin and bitcoin power consumption and we saw that gridcoin is way more power efficient because in gridcoin the consumed energy is used to advance scientific reseach for the benefit of mankind, while in bitcoin it is all invested in inverting a meaningless hash function. Finally, in the outlook section, we explored the concept of gridcoin funded science, an improvement to gridcoin which could fuel the next scientific revolution since the

enlightment age.

13 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.

[29] *How Much Power Does the Bitcoin Network Use*, estimation of Bitcoin power consumption, availabe from https://www.thebalance.com/how-much-power-does-the-bitcoin-network-use-391280.

[30] *How we calculate CO2 impact*, Conversion rate for kWh to CO2 metric tons, October 2017, available from https://carbonfund.org/how-we-calculate/

[31] *The math behind BOINC RAC*, jefpatat, September 2017, available from https://steemit.com/gridcoin/@jefpatat/the-math-behind-boinc-rac/

[32] *RAC and Gridcoin rewards for dummies*, hotbit, September 2017, available from https://steemit.com/gridcoin/@hotbit/rac-and-grc-rewards-for-dummies-calculate-you-maximum-rac-in-5-seconds

[33] *Idea behind Einsteinium*, Einsteinium foundation, October 2017, available from https://www.emc2.foundation/more-about-foundation

[34] *Science Power and Research Coin (SPARC) Whitepaper*, October 2017, http://sparc.network/sparc-whitepaper-4.pdf

[35] *Golem Network*, October 2017, http://golem.network/

[36] *BURP the Big and Ugly Rendering Project*, 2004-2017, http://burp.renderfarming.net/

[37] *GPU - a Global Processing Unit*, 2004-2014, http://gpu.sourceforge.net

[38] *Solarcoin - A global rewards program for solar electricity generation* , http://solarcoin.org

14 Appendix

14.1 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

14.2 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 [3] and the Gridcoin community for the ideas and technical work expressed in this paper.