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

Gridcoin Development Team
teamgridcoin.slack.com

December 1, 2017

Abstract

Gridcoin [6] is a decentralized, open source cryptocurrency which performs transactions without the need for a central issuing authority. Gridcoin securely rewards volunteer distributed computing performed on the BOINC [5] platform. BOINC is a volunteer computing grid which combines the processing power of individual users for the purposes of scientific research. The platform is already home to numerous independent projects with such diverse goals as curing diseases like cancer, AIDS, Ebola and Zika, assessing climate change, perfecting orbits of potential hazardeous asteroids and many others [11-20]. Since its creation in the early 2000s, the BOINC network has maintained an active userbase consisting of hundreds of thousands of participants from around the globe. Gridcoin was created in part to incentivize and further grow the BOINC userbase by rewarding calculations performed on the network.

Though heavily based on Bitcoin, Gridcoin distinguishes itself in its "environmentally friendly" method of securing the network. Instead of using Proof of Work, which hinges on the wasteful task of inverting a hash function, Gridcoin implements the novel approach of Proof of Stake [2] linked to Distributed Proof of Research [3], developed specifically for Gridcoin. In particular, Proof of Research replaces hash function inversion, which has no value outside of the network which it secures, with useful scientific computation on the BOINC network. Consistent with Gridcoin's decentralized structure, selection of which scientific projects to include in Proof of Research is carried out using a voting mechanism embedded in the blockchain. Additionally, we propose to reserve a small percentage of the minted Gridcoins in a special fund to sponsor scientific projects outside of mainstream and with no direct immediate reward like neglected diseases in poor countries. This new funding mechanism ushers in the new and exciting prospect of scientific research directed by the goals and interests of a decentralized international community.

Contents

Figure 1: *Gridcoin Art Medal depicting research in the fields of biology, electronics and astrophysics*

1 Introduction

Since the advent of the Information Age, data collection and analysis have become more and more essential to modern life. The need for fast processing of enormous volumes of data has stimulated exciting innovations in information technology infrastructure. In particular, distributed processing, also known as grid computing, has emerged as an efficient means of processing large scale data by distribution of the workload over a large network of individual processing units.

On the other hand, procuration of such a large number of processing units requires funds and infrastructure typically available only to governments, corporations, and universities. In a competitive funding environment, organizations and individuals with valuable data to process may nevertheless end up excluded from traditional funding channels. Even projects of significant and fundamental interest to humanity may fall under this category, due to their inability to satisfy government and corporate interests or secure short-term monetary returns.

Perhaps surprisingly, however, the means to circumvent this barrier are already on hand, sitting on our desks at home or lodged in our pockets: The combined Idle Processing Potential (IPP) of consumer electronic devices overshadows even the most robust decentralized super-computer, Bitcoin. Nevertheless, IPP is severely underutilized. To tap into this potential, Gridcoin seeks to create a decentralized and sustainable distributed processing network which prioritizes both the utilization of IPP and the creation of a free host ecosystem for researchers and individuals with data to process. Towards this end, Gridcoin has created a blockchain-based digital asset which rewards individuals and entities which volunteer their IPP to the grid computing network, BOINC. A single Gridcoin 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 means to process computational data for free. In operation since 2002, BOINC has maintained an active community consisting of hundreds of thousands of users. This vast userbase reliably contributes the computational muscle to support a wide range of independent projects, such as mapping the Milky Way galaxy, finding record prime numbers, folding proteins, testing disease cures and vaccines, and searching for extraterrestrial life.

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 in which they find intrinsic value. This eliminates the bias towards the researchers and organizations who happen to have the most funding.

A typical node on the Gridcoin network runs two clients: 1) the BOINC client, which manages the downloading and processing of data, and 2) the Gridcoin client, which interfaces with other nodes on the Gridcoin network. Like a Bitcoin wallet, the Gridcoin client allows users to transfer money to and from different addresses. Moreover, it contributes to the overall health of the network by verifying each new block and, depending on the configuration, itself staking new blocks. The coinstake in the new blocks proposed by any given wallet corresponds to an associated amount of work done on BOINC, expressed in Gridcoins.

1.1 BOINC

BOINC users run a client which downloads and manages the processing of work units (WU) for specific projects. A work unit consists of executable code and specific parameters for which the code is run. After the work unit is completed the BOINC client returns the results to the BOINC servers.

An example BOINC project is the World Community Grid [11], which is composed of various research initiatives with a humanitarian focus, for instance fighting cancer or curing Ebola. SETI@home [20], which scans radio waves from space for signs of alien life, is another well-known project. In total there are over 40 BOINC projects, but only the BOINC projects on the Whitelist help users earn Gridcoins. The complete Whitelist is available in the appendix. Each Gridcoin wallet can vote in polls concerning which projects enter or exit the Whitelist. New projects with interesting computational tasks have a high chance of getting on the Whitelist, while projects which do not have a constant supply of work units tend to be dropped.

The computational output of a given Gridcoin user is measured and stored on the BOINC server. The unit of work is a cobblestone, which on a project-by-project basis is converted into a certain number of "credits". While credits accumulate over time, computational *power* is measured by the Recent Average Credit (RAC), defined as a weighted time-average of credits earned per unit time. These units of measure are discussed later on in this whitepaper.

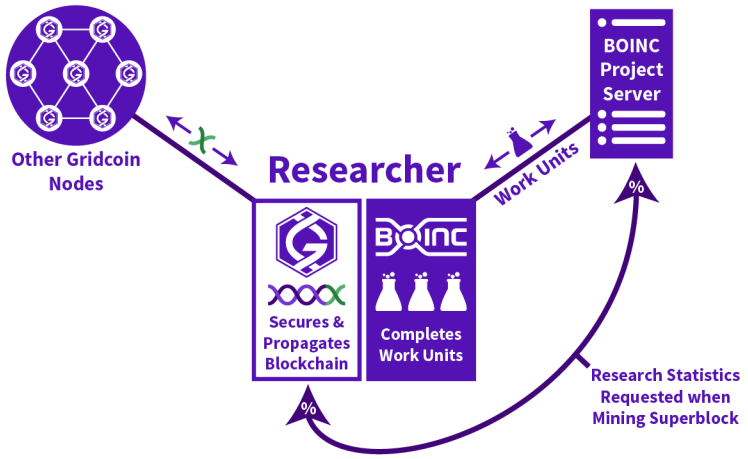

Figure 2: *Gridcoin and BOINC Architecture* [5]

A CPID (Cross Project Identifier) is a unique identifier on the BOINC network that links the contributions of a single user to different projects. Knowledge of a user's CPID allows anyone to view the contributions of that user to BOINC projects.

Finally, BOINC also allows the creation of teams. When a user joins a team, the work done by that member is added to the total work done by the team. To earn Gridcoin, a user must join team *Gridcoin*, which on some projects is listed as *gridcoin*, lowercase.

1.2 Gridcoin Client

The Gridcoin Client is very similar to a Bitcoin client, inheriting substantial portions of source code from it. It is sometimes called a wallet, because it stores the Gridcoins owned by a user. The client allows users to receive and send Gridcoins to other clients. If it is attached to BOINC, it is able to mine blocks which reward the user for work done on BOINC. The client also occasionally stakes Gridcoins so that they earn interest.

1.3 Setting Up a Network Node to Earn Gridcoins

Tutorials for setting up BOINC and the Gridcoin client are available on www.gridcoin.us. Briefly, the steps to become a solo miner are as follows:

1. Install BOINC.
2. Add projects to BOINC that belong to the Whitelist [42].
3. Install and configure the Gridcoin wallet so that it is linked to BOINC.

4. Acquire Gridcoins by buying them on exchanges and transferring them to your wallet.

5. Send a beacon so that the wallet CPID is present in the blockchain.

With proper setup, the client can begin staking blocks and rewarding the miner with Gridcoin. The odds of staking a block are proportional to the number of coins owned; the expected time until the next block is staked can be estimated from within the client. Note, however, that this is only an estimate of the average: the actual time to stake a block may be smaller or larger.

On the aforementioned website there are also instructions about mining in a common pool, which in contrast with solo mining has the advantage of consistent and predictable payouts. There is also the possibility to be an *investor* simply by owning Gridcoins and running the Gridcoin client (without needing to be a BOINC researcher). In the latter case, the investor earns interest on the Gridcoins they own, simply by running the wallet.

1.4 Mining Pool

If users do not manage to get some starter coins, available from faucets, or if they lack the experience to buy them from exchanges, they have the possibility to join the Gridcoin Mining Pool [55]. Steps to become a pool miner are as follows:

1. Register with GRCpool.com and select projects in which to participate.

2. Install BOINC.

3. Add GRCpool as account manager in BOINC. BOINC will download the selected projects in step 1. BOINC will submit computed results under the CPID of GRCpool. Thus, GRCpool will credit the user's balance on the website depending on how much work was performed.

4. Install the Gridcoin wallet in investor mode, without linking it to BOINC. Create a new Gridcoin address.

5. Login into GRCpool.com and move the credited Gridcoins to the local wallet by using the newly created Gridcoin address

Mining with the pool is easier to setup, but has two main drawbacks. First, the user does not inherit his/her own BOINC statistics. Instead, these are formally credited to the mining pool. Second, the user is not able to vote in polls issued by the network (see chapter 9).

1.5 Mining on Several Devices

Independent of whether the user mines solo or in the pool, it suffices to set up a single Gridcoin wallet linked to the same BOINC credentials. All devices used for mining will install BOINC and use the same credentials. Currently it is possible to mine Gridcoin using cell phones, tablets, PCs (even Raspberry Pi and its clones), playstations, high end servers, and advanced mining equipment. Both CPU and GPU mining are available, depending on the project.

In the foreseeable future, this list may expand further. With the growth of the Internet of Things, mining may even become possible on devices such as smart watches and house appliances!

1.6 Integrating Gridcoin in Existing Exchanges

For exchanges that wish to integrate Gridcoin in their infrastructure, the client can be run entirely in textual mode out of a Linux bash shell. The daemon named *gridcoinresearchd* implements the same commands with the same syntax as *bitcoind*, making the integration of Gridcoin in any existing cryptocurrency exchange infrastructure quick and easy [56].

2 Neural Network

This chapter starts with a disclaimer as the Gridcoin Neural Network [61] does not share anything with neural networks as commonly defined in the field of Artificial Intelligence. The Gridcoin Neural Network is charged with assigning Gridcoins to BOINC researchers. It is a kind of proportional calculation as we will see in the following chapters.

Gridcoin uses a distributed system to come to a consensus how much work was done by each user. For this purpose each node of the network, each Gridcoin client in other words, asks each BOINC project server, what the current Recent Average Credit of each member of team Gridcoin is. This information is mined in a special block called a Superblock. This information is hashed, so each node does not see the exact information from other nodes, 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 (a special network packet) 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. The probability to be chosen depends on the amount of Gridcoins the node has. A block contains all transactions that have taken place in the network since the last block stored on the blockchain. The node adding this block adds a transaction sending newly minted Gridcoins to their personal wallet in proportion to the BOINC work they did. Other nodes accept the new block only if the transactions are all valid and if the newly minted Gridcoins claimed by the creator node correspond to the amount of BOINC work did by the creator node as written in a previously minted superblock.

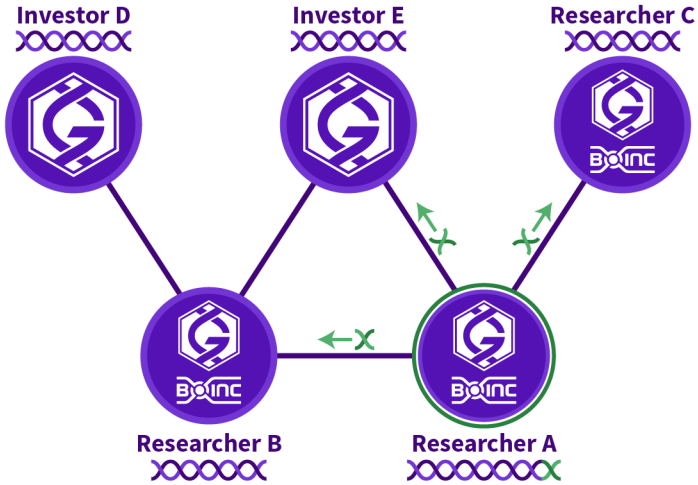

Figure 3: *A researcher mines a new block and sends it to other node's blockchains, so that they verify it and incorporate it*

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

Each participant helps performing research by computations in Gridcoin's network. The network average is similar to difficulty in Proof of Work mining. As the network average rises it becomes harder to get the same magnitude. If a user wants to keep getting the same reward, they would have to add more compute power if there is 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 [43] and Blackcoin's [44] 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 the user acquires the higher the probability

that they will mint a block.

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 with a transaction that moves the 50 Gridcoins away from Bob, the coin age for Bob is consumed.

Novacoin enabled Proof of Work as a stand alone function next to Proof of Stake. 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% increase of total supply per year. This target is therefore adjusted continuously and not every 2 weeks like Bitcoin's difficulty. In Gridcoin the rate listed in the APR schedule is annualized, the rate applied to the coin balance with an APR of 1% on coins held one day is therefore 1%/365. When transferring the coins to a new address, a lock time of 16 hours takes effect, before age is accumulated again.

Gridcoin has increased the difficulty of a 51% attack, an attack on a standard Proof of Work coin, which involves a single entity owning a minimum of 51% of the total network hash rate. To attack Gridcoin in a similar way, the attacker would have to make a 51% buy-out, meaning he needs to own 51% of all the coins. In addition to the 51%, the attacker would have to buy and hold the cumulative stake weight of all nodes with fewer than 30 blocks staked. Since interest is being paid to those who let their nodes run for the network, transaction fees are not needed in theory. However they are still enforced to prevent transaction spam on a single node.

These improvements were already made by Blackcoin [44], which Gridcoin, in an effort to keep up with current technology has implemented. Blackcoin also included the Zerocash [45] protocol, a process enabling anonymous transactions. For now this feature has been disabled from the Gridcoin 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 Proof of Stake payment. A wallet that is not associated with a BOINC account is called an Investor wallet.

4.1.1 Block Kernel Target

$$X_{i+1} = X_i \cdot \frac{\left(\frac{16 \cdot 60}{90} - 1\right) \cdot 90 + (t_i - t_{i-1}) + (t_i - t_{i-1})}{\left(\frac{16 \cdot 60}{90} + 1\right) \cdot 90} \tag{1}$$

$$X_{i+1} = X_i \cdot \frac{810 + 2 * (t_i - t_{i-1})}{990} \tag{2}$$

Field	Description
txPrev.block.nTime	block time of referenced tx
txPrev.nTime	timestamp of referenced tx
txPrev.vout.hash	hash of referenced tx output
txPrev.vout.n	index of referenced tx output
txPrev.vout.n	index of referenced tx output
Stake Modifier	a number composed of enthropy gathered from past blocks
nTime	current UNIX timestamp

Figure 4: *Gridcoin Kernel Parameters*

$$X_{i+1} = X_i \cdot \frac{405 + (t_i - t_{i-1})}{495} \tag{3}$$

Legend: t_i is time when a block i was created (CBlock.nTime). X_i is the block kernel target like in Bitcoin [63]. In equation (3) we see that the more time passes since creation of the last block X_i the higher the block kernel target gets. The higher kernel target makes easier for miners to satisfy the Proof of Stake Inequality.

4.1.2 Proof of Stake Inequality

To create a new valid block for the Gridcoin blockchain the following inequality has to be satisfied:[1]:

$$SHA256(SHA256(kernel)) < X_i \cdot UTXO \tag{4}$$

First a data string (called *kernel*) is formed from the kernel components (see table), then the kernel is hashed to obtain a proof hash, and then this proof hash is compared to the current block kernel target. Both proof hash and target are (big) numbers. The kernel forms a valid proof only if the proof hash is less than the block kernel target. [60]

The idea of PoS is that you can't just iterate over some nonce trying endlessly, burning your CPU/GPU/ASIC power, until you find a valid kernel. In PoS, you can only try using different coins you have and the current time. [60]

The referenced unspent transaction output ($UTXO$) must be at least 16 hours old.

4.2 Proof of Research

To tie BOINC and Gridcoin 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

[1] This paragraph is sourced from [59] but it includes security fixes done in [60].

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 [46]. A Monte Carlo simulation was run to test the fairness of the network.

4.3 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 users' owed balance increases and when enough is owed and the user's wallet is connected to the network and unlocked to stake they will receive their reward. What a researcher is owed is commonly referred to as their Research Savings Account or RSA.

4.4 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% per year, as the coin base increases the number of coins created increases but always at a rate of 1.5% per year. Proof of Stake is in every block, when a Proof of Research block is staked the Proof of Stake reward is also included.

4.5 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 0.117416

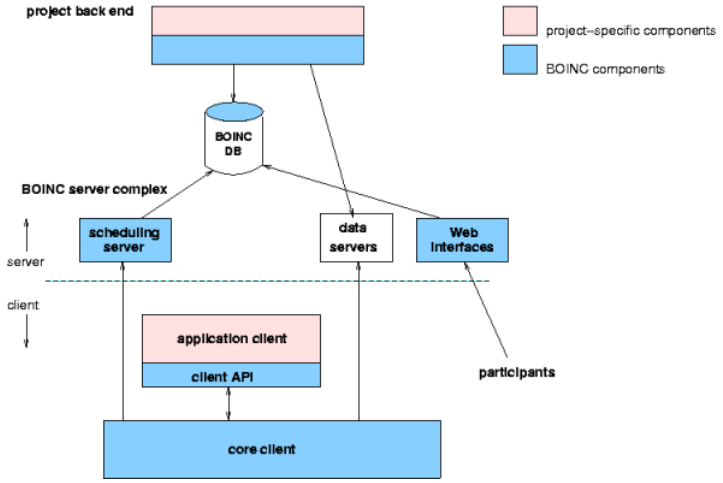

Figure 5: *BOINC Client/Server Architecture* [5]

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. A user must stake one block after the beacon is sent before they 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 a user 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 one begins with the faster the first block will be minted. The initial age coins must be before they are able to stake is 16 hours.

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

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, called superblocks, the majority consensus 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 `www.gridcoinstats.eu`. If a node gets chosen and the hash this node contains about the amount of work done by this 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. The actual reward the node gets then depends on the *RAC* (Recent Average 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 or 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 Recent Average Credit (RAC)

Cobblestones are converted into a certain number of "credits" on a project-by-project basis. The unit of conversion is not monitored by BOINC, and hence some projects grant more credits per cobblestone than others. However, this discrepancy does not affect Gridcoin payouts, since a researcher's output for a given project is normalized by the overall output of Gridcoin researchers *within the same project* (see section 5.3).

Besides tracking the *total* computational output of a researcher (measured in total credits), BOINC also calculates a quantity called the Recent Average Credit (RAC), which is a time-averaged measure of computational *power* (credits per unit time). More precisely, RAC is an exponentially weighted moving average over computational power, thus granting more weight to recently earned credits. The details of its calculation are as follows.

Generally speaking, an exponential moving average S_i of a fixed-interval time series X_i is a moving average which assigns exponentially less weight to data points in the past. More precisely,

$$S_i = (1-\alpha)^i X_0 + \alpha \sum_{j=1}^{i} (1-\alpha)^{j-1} X_{i-j+1} \tag{5}$$

where $0 < \alpha < 1$ is a constant weighting factor. A large α, corresponding to smaller $1-\alpha$, assigns smaller weight to data points in the past. S_i can also be computed recursively for $i > 1$:

$$S_i = \alpha X_i + (1-\alpha) S_{i-1}. \tag{6}$$

with $S_0 \equiv X_0$. This moving average can be understood intuitively using figure 6. The output is S_i, and the input is X_i. As the input jumps to 1 the output slowly follows and approaches a value of 1. When the input changes this process just repeats. The inputs rapid jump to 2 did not substantially contribute to the output. Thus, S_i has a smoothing effect on the relatively noisy series X_i [31]. We want to implement something similar for computational power. On the other hand, generally BOINC updates its statistics at uneven time intervals $\ldots < t_{i-2} < t_{i-1} < t_i$, and hence a time-dependent weight α must be defined. BOINC has found it convenient to use the exponential weighting factor:

$$\alpha_i = 1 - \mathrm{e}^{-(t_i - t_{i-1}) \cdot \ln(2)/th} \tag{7}$$

where t is given in days. The BOINC source code works equivalently in terms of the weight function

$$w(t_i - t_{i-1}) \equiv \mathrm{e}^{-(t_i - t_{i-1}) \cdot \ln(2)/th}. \tag{8}$$

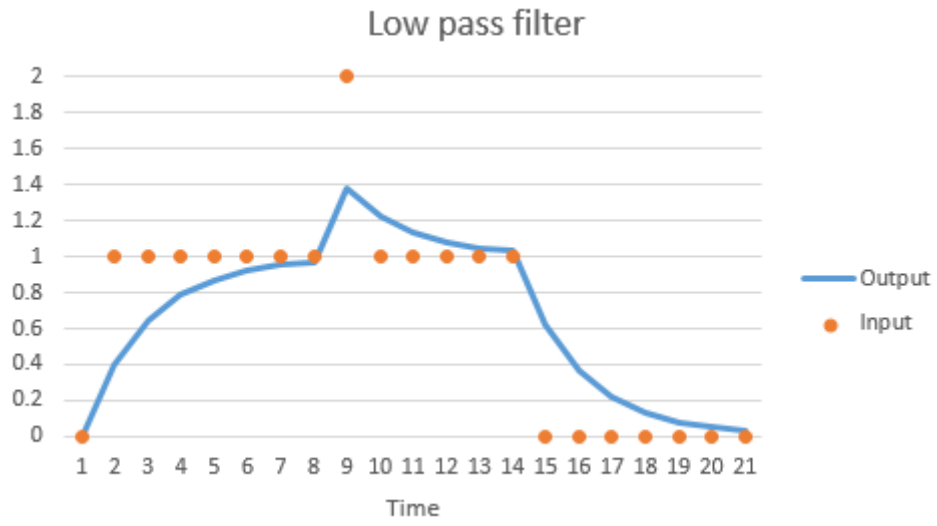

Figure 6: *A low pass filter in action smooths spikes and dips*

The quantity th is called the halving parameter, since

$$w(t_i - t_{i-1}) = \left(\mathrm{e}^{-\ln(2)}\right)^{(t_i - t_{i-1})/th} = \left(\frac{1}{2}\right)^{(t_i - t_{i-1})/th} \tag{9}$$

using elementary properties of logarithms. BOINC has found it convenient to set th equal to 7 days. Note that when $t_i - t_{i-1}$ is large, α_i is close to 1, thus indeed granting exponentially less weight to older computations. In fact, if RAC is updated weekly, credit from 1 week ago is granted half the weight, credit from 2 weeks ago is granted one-quarter the weight, etc. Roughly speaking, credit from more than 2 months ago will not contribute significantly.
Let's put all of this together. Suppose the computational power at time t_i is R_i. Having defined $RAC(t_i)$ in the above as the weighted moving average of the previous R_i, we have:

$$RAC(t_i) = [1 - w(t_i - t_{i-1})]\, R_i + w(t_i - t_{i-1}) \cdot RAC(t_{i-1}). \tag{10}$$

Of particular interest is the *long time limit* of this equation. If we crunch at a constant rate R for several months, what value will RAC level out to? If we assume RAC is updated at constant time intervals $t_i - t_{i-1} = \Delta t$, then it is not hard to find at least *one* time-invariant solution to the above equation: $RAC = R$. To be careful, one should prove that there are no other solutions. This turns out to be in fact the case, as one can show using equation (5).

Thus, if one crunches at a constant rate R *credits per day*, and RAC is updated in constant time intervals, then RAC levels out to R. If $t_i - t_{i-1}$ is not constant but depends on i, there will be some variations, although these are expected to be small compared to the average value R.

5.3 Gridcoin Payout to User Running Multiple Projects

We hereby define:

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

Γ : this is the *RAC* done by all users participating 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 [42]. Participants 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 around.

$$G = MaxDailyEmissions - AvgDailyPaymentsPaidInLast14Days$$

There are also a few security rules. For example time since last payment in days (τ) cannot be greater than 6 months, otherwise there is no payment and the coins paid out per user does have a very high upper limit ($\tilde{5}000$) per stake. The $MaxDailyEmissions$ is set to 50'000 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.

6 Enviromental Sustainability

6.1 Gridcoin as TOP 500 Supercomputer

TOP 500 at `www.top500.org` is a worldwide list of existing supercomputers ranked by their computational speed. In this chapter, we calculate the position of BOINC, Gridcoin and Bitcoin.

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 users produced 3'034'366'125 cobblestones. Gridcoin users produced a subset of that amount: 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 show 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 (it halves every 4 years, last halving event was in 2016).

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 fastest supercomputer in the world and outperform the first ranked supercomputer by factor 643'391!

6.2 Gridcoin Power Consumption Estimate

We start to calculate the consumption of Gridcoin's 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 0.5 Watt of power one Gigahash/s. According to [58], Bitcoin speed on August 26, 2017 was 6'354'668.57 terahash/s or 6'354'668'570 gigahash/s or 3'177'334'285 W. These are 3.177 GW of power. They are equivalent to the power produced by 3 large nuclear power plants. Over one year, which has $365 \cdot 24$ hours (=8760 hours), we get 3.177 GW $\cdot$ 8760h = 27'831 GWh or 27.831 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 gives 16.2 TWh/year as consumption estimate for last year. Steps to calculate the mentioned index are:

- 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 choose the approach outlined in [21]. 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: the BOINC average user owns a standard CPU like an Intel Core i5 with an average GPU like Nvidia GTX 1060. The Intel Core i5 features 4 cores times 4.57 GFlops = 18.28 GFlops with 77W consumption and the 1060 graphic card does 3'850 GFlops with 120W of power. This system totally features 3868.8 GFlops: 0.47

By diving the cobblestones 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:

$$16'501'410 \cdot 0.0047 \cdot 77/18.28 + 16'501'410\ cdot 0.9953 \cdot 120/3850 = 838'601W = 0.839MW$$

$$0.838MW \cdot 24h \cdot 365days = 7'350MWh = 7.350GWh$$

0.838 MW can be compared to the power produced by a little hydro power plant in the Alps.
In one year, BOINC consumes about 7.350 GWh. Similarly, Gridcoin power calculation gets:

$$2'447'799 \cdot 0.0047 \cdot 77/18.28 + 2'447'799\ cdot 0.9953 \cdot 120/3850 = 124'397W = 0.124MW$$

$$0.124MW \cdot 24h \cdot 365days = 1'086MWh = 1.086GWh$$

This calculation assumes that most power to run Gridcoin is in Proof of Research and that running the client is almost negligible compared to the PoR part.
If we assume that one household roughly consumes 1 kW, then Gridcoin power consumption corresponds to 124 households.

6.3 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: 27.831 TWh/year = 16.47 millions metric tons CO2 per year
- Ethereum: 5.5 TWh/year = 3.26 millions metric tons CO2 per year
- BOINC: 7.35 GWh/year = 4'354 metric tons CO2 per year
- Gridcoin: 1.086 GWh/year = 643 metric tons CO2 per year

According to the Carbon Footprint Calculator [54] a car which runs for 200'000 km produces 50 metric tons CO2. If we assume that the car has an average life of 12 years, we get 4.17 metric tons per year. Using these numbers, Bitcoin produces CO2 comparable to a park vehicle composed by 3'950'000 cars.

7 Other Functionalities

7.1 Voting Mechanism

The gridcoin wallet embeds a voting mechanism that allows polls to be created and answered by users. How many votes a user has depends on user's coin and research age.

A list of current and past polls is mantained on Gridcoin Stats [57]. To vote on a poll a user issues the command `gridcoinresearchd execute vote [pollname] [pollanswer]` [56].

Polls can be of any kind, the most important ones related about projects to be included or excluded from the Gridcoin Whitelist [42].

7.2 Transaction Speed

These are empirical transaction speeds as often encountered in literature:

- *Bitcoin* : Bitcoin transaction speed is around 7 transactions per seconds.
- *Ethereum* : Current implementation of Ethereum (October 2017) reaches 14 transactions per second.
- *Gridcoin* : Gridcoin is heavily based on Bitcoin and also reaches a speed of 7 transactions per second.

- *Bitshares* : Bitshares based on Graphene toolkit claims 100'000 transactions per second on a testnet. However a testnet is a quite simplified environment that could not match the harsh reality of a crowded Internet.
- *Credit Card* : The worldwide credit card system processes about 300'000 transactions per second.

From this figures it is visible that at time of writing the state of the art blockchain technology is able to transfer value between people, but not at speed sufficient to substitute the existing credit card infrastructure. Therefore Bitcoin and the existing cryptocurrencies are seen more as value storage like gold rather than a digital currency able to enact day to day transactions between people.

7.3 Transaction Efficiency

In [58] it is compared how much energy is needed for a transaction in Bitcoin versus a credit card transaction. By taking our Bitcoin power consumption estimate of 27.831 TWh/year and dividing by 365 day · 24 hours · 3600 we get 27'831'000'000 kWh/(365 · 24 · 3600) = 882.515 kWh/s. In this second Bitcoin does 7 transactions, so each transaction costs 882.515 kWh/7 = 126 kWh. If one household needs 24 kWh per day, one Bitcoin transaction can power 5.25 households for one day.

By analogy, the Gridcoin network consumes with the current number of miners 1.086 GWh in one year. These are 0.035 kWh/s. Gridcoin does 7 transactions per second as well, therefore the transaction cost is 0.035 kWh / 7 = 0.005 kWh per transaction. Of course, this might change if the Gridcoin price should soar and attract more miners who will have to share the same amount of minted Gridcoins per day. At least, the power consumed in Gridcoin advances scientific research and is not wasted inverting a hash function.

In the estimate in reference [27], it is assumed that the datacenter infrastructure to power VISA credit card system in 2016 is equivalent to 50'000 households. If we take for one household roughly 1 kW of power consumption, we get 50 MW to power VISA. We also now VISA processed 82.3 billion transactions in 2016. 50MWh/3600s = 13.89 kWh/s. 82.3 billion transactions per year correspond to 2'603 transactions per second. The power consumed in one transaction is 13.89 kWh/s / 3600 = 0.005 kWh per transaction like Gridcoin in these days.

To get an idea 0.005 kWh are 5W for one hour: one VISA or Gridcoin transaction can power a Raspberry Pi Model 3 for one hour.

7.4 Proximity of Neighbours

Following functionality is not implemented in Gridcoin yet, but could help improving its transaction speed. The main idea is to disentangle the existing random network to a network which is closer to the underlying geographical topology.

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.

7.5 Gridcoin Security

Gridcoin security relies on the fact that Gridcoin is an Open Source derivate of Bitcoin: it inherits Bitcoin's security which is unbroken since creation of Bitcoin. Gridcoin Proof of Stake is the hardened Blackcoin version [44], more secure than Peercoin [2].

If a BOINC account is hacked and its owner is unaware of Gridcoin, so that its email, password and CPID are known to the attacker, the attacker can receive gains of the unaware BOINC user by sending a beacon with the compromised CPID linked to the attacker's wallet, collecting gridcoins for work done by a BOINC user unaware of gridcoin existence.

However, although unfortunate, the previous event will never disrupt the inherently secure transactional mechanism of Gridcoin's blockchain ensuring that people holding and transactions stay secure. Gridcoin blockchain is operating smoothless since 2014 and there were never events which disrupted the way Gridcoin operates. As any other cryptocurrency, Gridcoin remains vulnerable to a 51% attack though it made it more difficult to exploit, but a vibrant community around Gridcoin stays vigilant and will make sure this will never happen.

In [59] a group of security researchers found two attacks which could be exploited on Gridcoin client version 3.5.8. Gridcoin clients with version 3.6.0 and above implement the new Gridcoin PoS Kernel v8 [60] which prevents both exploits described in [59].

Additionally, in Gridcoin there will never be an ASIC race as in Bitcoin, because of the scientific nature of the computations which is not easily replicated in FPGA or ASIC machinery. This will ensure Gridcoin will distribute

rewards among miners in a more democratic manner than Bitcoin and will avoid tendency to centralization as seen in Bitcoin.

8 Outlook

8.1 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.

If a particular commercial project should struggle to get users on board because it is boring or too much ressource intensive requiring special hardware setups, following could be thinkable:

1. The commercial project buys a given set of Gridcoins on exchanges
2. The project registers CPIDs of users interested in joining along with a user's gridcoin address for payouts
3. Registered users do work for the commercial project and submit results to the BOINC server of the project
4. Registered users receive the usual Proof of Research payout issued by the Gridcoin network
5. Registered users receive an additional payout done by the commercial project as incentive to enhance and mantain their ressource intensive setup. The payout is done using Gridcoins bought in step 1. to the previously collected users's gridcoin addresses.

8.2 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 further ameliorated.

The advent of Internet did a lot to increase communication between scientists. However, it also introduced the problem of plagiarism and amplified the problem of falsified data [48]. For the increasing amount of papers, there is not enough incentive and competent people to guarantee an independent and competent peer review process [49,50,51]. Sometimes, papers are not available for free but only through expensive subscriptions (remember Aaron Swartz [52]). It is possible to read a paper, but seldomly the source code of software in the paper is made available to the public. Therefore it is very difficult to independently test 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 together with money from taxpayers. The significance problem [53] hiddenly points to another big scientific issue: it is quite 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.

If Gridcoin would introduce a fixed 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.

Imagine Elon Musk funding the settlement of humans on Mars with Gridcoins or an X-Wing spaceship lurking in your garage bought second hand and developed with Gridcoin funding.

Having traditionally funded science compete against Gridcoin funded science could spark the next scientific revolution since the age of enlightenment.

9 Competitors

9.1 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 many other functionalities [37].

9.2 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 researchers on a dedicated blockchain in a decentralized manner.

9.3 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.

10 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 cannot be used as mean to exchange goods between people as its transaction speed is too low. We also saw that Bitcoin is not environmentally sustainable: the algorithm which protects and verifies transactions and creates new blocks is consuming too much power.

It is reasonable to think that sooner or later the regulators 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.

11 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 researchers 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. Because of Gridcoin's nature computations will stay on CPUs and GPUs and there will never be an ASIC race as seen in Bitcoin.

Finally, in the outlook section, we explored the concept of Gridcoin funded science, an improvement to Gridcoin which could spark the next big scientific revolution since enlightenment age.

12 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://coss.io/documents/white-papers/Gridcoin.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 Schuer, *Bitcoin, Blockchain und Kryptoassets* , Universitaet 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] *On gridcoin mining, profitability, value and other random thoughts.* , hotbit, September 2017, available from https://steemit.com/gridcoin/@hotbit/on-gridcoin-mining-profitability-value-and-other-random-thoughts.

[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

[39] *21 Terms to Understand Cryptocurrency* , Max Middelmann, October 2017, https://medium.com/the-mission/21-terms-to-understand-cryptocurrency-8bee30aa8dfc

[40] *Transaction*, Bitcoin Wiki, http://en.bitcoin.it/wiki/Transaction

[41] *Google Definitions*, www.google.com

[42] *Gridcoin Project Whitelist*, http://www.Gridcoin.us/Guides/whitelist.htm

[43] *Novacoin*, http://coinwiki.info/en/Novacoin

[44] *Blackcoin Proof of Stake Protocol v2*, Pavel Vasin, https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf

[45] *Zerocash: Decentralized Anonymous Payments from Bitcoin (extended version)*, Eli Ben-Sasson et. al, May 18 2014, http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf

[46] *Kimotos Gravity Well*, Cryptorials, http://cryptorials.io/glossary/kimotos-gravity-well/

[47] *Gridcoin - Rewarding research instead of mining*, Anonymous User, https://docs.google.com/document/d/1PUmLpL3jb-Dhf9-60MPpCYpCvBukUIWeKO8Pww0bhII/edit#heading=h.1gqiga6cbzja

[48] *Plagiarism and falsified data slip into the scientific literature: a report*, John Timmer, Ars Technica, 08.08.2007, https://arstechnica.com/features/2007/08/plagiarism-and-falsified-data-slip-into-the-scientific-literature/

[49] *Can we trust peer review? New study highlights some problems*, Cathleen O'Grady, Ars Technica, 20.07.2016, https://arstechnica.com/science/2016/07/can-we-trust-peer-review-new-study-highlights-some-problems/

[50] *Mindless Eating or how to send an entire life of research into question*, Cathleen O'Grady, Ars Technica, 24.04.2017, https://arstechnica.com/science/2017/04/the-peer-reviewed-saga-of-mindless-eating-mindless-research-is-bad-too/

[51] *Do we need an alternative to peer-reviewed journals?*, Jonathan M. Gitlin, Ars Technica, 18.07.2011 https://arstechnica.com/science/2011/07/do-we-need-an-alternative-to-peer-reviewed-journals/

[52] *Open access: All human knowledge is there, why can not everybody access it?*, Glyn Moody, Ars Technica, 06.07.2016, https://arstechnica.co.uk/science/2016/06/what-is-open-access-free-sharing-of-all-human-knowledge/

[53] *There is a debate raging in science about what should count as significant*, Cathleen O'Grady, Ars Technica, 04.08.2017, https://arstechnica.com/science/2017/08/theres-a-debate-raging-in-science-about-what-should-count-as-significant/

[54] *Carbon Footprint Calculator*, Carbon Footprint Ltd, Hampshire UK, October 2017 https://calculator.carbonfootprint.com/calculator.aspx?tab=4

[55] *grcpool - Gridcoin Mining Pool*, www.grcpool.com

[56] *gridcoinresearchd - RPC commands*, http://wiki.gridcoin.us/RPC_commands

[57] *Gridcoin Stats Polls - Active and Past Pools*, http://www.gridcoinstats.eu/poll

[58] *A Single Bitcoin Transaction Takes Thousands of Times More Energy Than a Credit Card Swipe* , Christopher Malmo, 07.05.2017, https://motherboard.vice.com/en_us/article/ypkp3y/bitcoin-is-still-unsustainable

[59] *Breaking and Fixing Gridcoin*, Martin Grothe, Tobias Niemann, Juraj Somorovsky, Joerg Schwenk, Horst Goertz Institute for IT Security, Ruhr University Bochum, 16.09.2016, https://www.usenix.org/system/files/conference/woot17/woot17-paper-grothe.pdf

[60] *Gridcoin PoS kernel v8*, TomasBrod, 12.09.2017, https://github.com/gridcoin/Gridcoin-Research/wiki/Stake-V8

[61] *DEV Neural Network*, TomasBrod, 31.07.2017, https://github.com/gridcoin/

Gridcoin-Research/wiki/DEV-Neural-Network

[62] *Gridcoin V8 difficulty and what it tells you*, skcin, September 2017, https://steemit.com/gridcoin/@skcin/gridcoin-v8-difficulty-and-what-it-tells-you

[63] *Bitcoin Kernel Target*, Bitcoin Development Team, https://en.bitcoin.it/wiki/Target

[64] *Decentralised Currencies Are Probably Impossible But Lets At Least Make Them Efficient*, Ben Laurie, 05.07.2011, http://www.links.org/files/decentralised-currencies.pdf

[65] *On Bitcoin and Red Balloons*, Barbaioff M. et al., 2011, https://arxiv.org/pdf/1111.2626.pdf

13 Appendix

13.1 Terminology

- *51% attack* : A 51% attack is a situation where more than half of the computing power on a network is operated by a single individual or concentrated group, which gives them complete and total control over a network. Things that an entity with 51% of the computing power can do include, but are not limited to: [39]

  - Halting all mining.
  - Halting and manipulating all interpersonal transactions.
  - Using singular coins over and over.

- *address* : A wallet address, or simply address, is an identifier of alphanumeric characters, that represents a possible destination for a cryptocurrency payment. Addresses can be generated at no cost by the wallet's user.

- *ASIC* : Application Specific Integrated Circuit: a dedicated chip optimized to perform only one kind of computation. In case of Bitcoin it is inverting the hash function that makes possible to attach new blocks to the blockchain.

- *Bitcoin* : The first digital currency able to decentralize the account's ledger by means of a blockchain.

- *beacon* : A beacon is a particular network transaction containing the CPID of a user to signal the network that this user is starting to calculate valid scientific research.

- *block* : Blocks are essentially pages in a ledger or record keeping book. Blocks are the blockchain's components where unalterable data related to the network is permanently stored.

- *blockchain* : A blockchain is a data system that allows for the creation of a digital ledger of transactions on a non-centralized network. Cryptography is the main operator that allows for users to engage with the ledger without the need for any central figurehead. In laymans terms, this means that people and computers all over work together to create a network instead of a network being made by one single person or company. This network is enabled and protected through cryptography! We have seen this used in currency, data transfer and on. The blockchain is comprised of "blocks" and is constantly growing as each new record, datum, or block is added onto the chain for everyone to see. [39]

- *BOINC* : Berkeley Open Infrastructure for Network Computing is a software which allows users to donate computational time to scientific research. It is possible to participate in several projects, each run by different and recognized scientific institutions. It utilizes a client/server architecture. Clients calculate tasks in the form of work units and report them to servers running the BOINC project software.

- *BOINC client* : A BOINC client runs on a users's computer, mini-PC (e.g. Raspberry Pi), cellphone, tablet, or any other device with a CPU (watches might come in the future). It downloads work units from a BOINC server and processes them. When results are available, it reports them back to the BOINC server.
- *BOINC server* : A BOINC server runs a particular BOINC project. It distributes work units to BOINC clients and collects the submitted results, once the workunits are calcuated by the client.
- *BOINC project* : A BOINC project is an umbrella for several tasks which are distributed by a recognized scientific institution. A BOINC project publishes scientific results from time to time after enough work units are processed.
- *cobblestone* : A cobblestone or BOINC credit corresponds to 432 billion floating point operations, 432 gigaflops or 0.432 teraflops.
- *consensus* : Consensus is agreement achieved over a peer to peer network when all network nodes agree on something, for example a transaction of a digital currency between two users or a reward given to a particular user. It is achieved by cryptographical means. A 51% attack can break it.
- *CPID* : A Cross Project Identifier is assigned to each node running BOINC and it is used to uniquely identify the node both in the Gridcoin network and in the BOINC infrastructure.
- *CPU* : Central Processing Unit: a multipurpose computing device. This is the heart of computers and most smart electronic devices. It is suitable for serial computations.
- *cryptocurrency* : A digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank. [41]
- *Ethereum* : The first digital currency to introduce a flexible blockchain by means of a Turing complete virtual machine. Infinite loops are avoided by having the program to pay a little amount of money in each loop.
- *FPGA* : Field Programmable Gate Array: these chips can be reprogrammed to perform dedicated tasks. Once programmed, they do these tasks at faster speed than CPUs. They were used in the early days of Bitcoin mining. They might experience a revive with the coming revolution in Artificial Intelligence as they are suitable to simulate neural networks.
- *Gridcoin* : The first digital currency that rewards users for performing meaningful scientific research.
- *GPU* : Graphics Processing Unit: the heart of any graphic card. The ability to render pictures and animations evolved into the ability to execute general purpose parallel computations. They are suitable to run at high speed some scientific computations.

- *Kimoto's Gravity Well* : It is a common method for difficulty readjustment in cryptocurrency mining. It was first implemented by Megacoin and named after that coins lead developer. It was designed to solve problems caused by multipool mining.
  Multipools are mining collectives which automatically switch to mining whichever cryptocurrency is the most profitable. The problem with this is that when a multipool targets a coin the increase in hashing power makes the difficulty soar, which in turn makes profitability of mining crash. The multipool then moves on to the next target and the network is left struggling to find miners to keep maintaining the network with the new high rate of difficult. Kimotos Gravity Well algorithm allows difficulty to be readjusted every block, meaning that it can respond to both increases and decreases in hashing power immediately and keep the difficulty level at an appropriate level. [46]

- *magnitude*: The magnitude in the BOINC network is the ratio between the recent work done by a single node against the work done by the entire BOINC network done on a particular project.

- *"Neural network"* : The Gridcoin neural network is a consensus computation validated by the nodes on the network that decides how many Gridcoins each node receives in exchange for the scientific research performed. It is not to be confused with a neural network in the artificial intelligence context.

- *Peercoin* : The first digital currency which introduced Proof of Stake to avert the huge energy consumption of Proof of Work.

- *Proof of Work (PoW)* : Proof of work was a concept originally designed to sieve spam emails and prevent DDOS attacks. A Proof of Work is essentially a datum that is very costly to produce in terms of time and resources, but can be very simply verified by another party. The proof of work for Bitcoin is referred to as a nonce, or number used only once. This has been considered an energy intensive alternative to proof of stake as the computers unfortunately have to be on and running, which also drives the market towards centralization of hashing power which is what the blockchain aims to defeat! [39]

- *Proof of Stake (PoS)* : Proof of stake has been considered the greener alternative to PoW. Where PoW requires the prover to perform a certain amount of computational work, a proof of stake system requires the prover to show ownership of a certain amount of money, or stake. [39]

- *Proof of Research (PoR)* : Proof of Research is the novel approach introduced by the Gridcoin network to reward users performing scientific calculations for the benefit of mankind.

- *Recent Average Credit (RAC)* : Recent Average Credit is a function that calculates the amount of scientific work performed starting from the work units reported by a user to a BOINC project server.

- *Research Savings Account (RSA)* : this term denotes research performed by a user which was not rewarded with Gridcoins yet.

- *Superblock* : A superblock is a specificity of the Gridcoin network. It is a special blockchain block that contains how much work was done by each single user. It is generated about once a day.

- *transaction* : A transaction is a transfer of a cryptocurrency value that is broadcasted to the network and collected into blocks. A transaction typically references previous transaction outputs as new transaction inputs and dedicates all input coin values to new outputs. Transactions are not encrypted, so it is possible to browse and view every transaction ever collected into a block. Once transactions are buried under enough confirmations they can be considered irreversible.
  Standard transaction outputs nominate addresses, and the redemption of any future inputs requires a relevant signature.
  All transactions are visible in the block chain, and can be viewed with a hex editor. A block chain browser is a site where every transaction included within the block chain can be viewed in human-readable terms. This is useful for seeing the technical details of transactions in action and for verifying payments. [40]

- *wallet* : any software able to send and receive payments using the underlying blockchain technology. A wallet is typically a client that connects several other network nodes to mantain its blockchain uptodate.

- *workunit* : A single scientific calculation performed on a BOINC client. A work unit can last from minutes (typically if it is run on a modern graphic card, a GPU) to entire months (some climate simulation can last several weeks).

13.2 Gridcoin Whitelist

The Gridcoin Whitelist [42] includes all BOINC projects which give a reward in Gridcoin. It is compiled by people's vote persisted on the blockchain. At time of writing (October 2017) the following project are whitelisted:

- *Amicable Numbers* : Amicable Numbers is an independent research project that uses Internet-connected computers to find new amicable pairs. Currently searching the 10^{20} range. Private

- *Asteroids@home* : Asteroid research - it uses photometric measurements of asteroids observed by professional big all-sky surveys as well as 'backyard' astronomers. The data is processed using the lightcurve inversion method and a 3D shape model of an asteroid together with the rotation period and the direction of the spin axis are derived. Charles University in Prague [14]

- *Citizen Science Grid* : Umbrella project for DNA@Home, SubsSet Sum@Home, and Wildlife@Home. University of North Dakota

- *ClimatePrediction.net* : Run computer models to simulate the climate for the next century, producing predictions of temperature, rainfall and the probability of extreme weather events. University of Oxford. [15]

Additional note: due to delays in reporting user's statistics, this project is not in the whitelist, but will be as soon as the issue is solved.

- *Collatz Conjecture* : Attempting to disprove the Collatz Conjecture. Private [17]
- *Cosmology@Home* : Darkmatter/Universe Model Research Department of Astronomy at the University of Illinois at Urbana-Champaign
- *DrugDiscovery@Home* : Discovery of new drugs for the most dangerous and widespread diseases. Digital BioPharm Ltd
- *Einstein@home* : Search for spinning neutron (pulsars) stars using data from the LIGO gravitational-wave detectors, the Arecibo radio telescope, and the Fermi gamma-ray satellite. University of Wisconsin - Milwaukee, Max Planck Institute [19]
- *Enigma@Home* : this project is an effort to break 3 original Enigma messages with the help of distributed computing. The signals were intercepted in the North Atlantic in 1942 and are believed to be unbroken. Private
- *GPUgrid* : Full-atom molecular simulations of proteins Private Sponsors [12]
- *LHC@Home* : Accelerator Physics. CERN in Geneva, Switzerland [18]
- *Milkyway@home* : Creation of a 3D map of the Milky Way galaxy using data gathered by the Sloan Digital Sky Survey. This project enables research in both astroinformatics and computer science. Rensselaer Polytechnic Institute
- *Moo! Wrapper* : Moo! Wrapper brings together BOINC volunteer computing network resources and the Distributed.net projects. It allows a BOINC Client to participate in the RC5-72 challenge. Distributed.Net
- *NFS@Home* : Lattice sieving step in Number Field Sieve factorization of large integers. Many public key algorithms, including the RSA algorithm, rely on the fact that the publicly available modulus cannot be factored. If it is factored, the private key can be easily calculated. California State University Fullerton
- *NumberFields@home* : Research in number theory. Number theorists can mine the data for interesting patterns to help them formulate conjectures about number fields. Arizona State University, School of Mathematics
- *PrimeGrid* : Search for prime numbers. Primes play a central role in the cryptographic systems which are used for computer security. Through the study of prime numbers it can be shown whether current security schemes are sufficiently secure. Private, supported by Rackspace
- *Rosetta@Home* : Protein structure prediction that may ultimately lead to finding cures for some major human diseases. University of Washington [13]

- *SETI@home* : Search for Extraterrestrial Intelligence (SETI). University of California, Berkeley [20]
- *SRBase* : Attempting to solve Sierpinski/Riesel bases up to 1030. The project is in collaboration with the Mersenne CRUS project.
- *theSkyNet POGS* : Astronomy Research. Combine the spectral coverage of GALEX, Pan-STARRS1, and WISE to generate a multi-wavelength UV-optical-NIR galaxy atlas for the nearby Universe. Calculate physical parameters such as: star formation rate, stellar mass of the galaxy, dust attenuation, and total dust mass of a galaxy; on a pixel-by-pixel basis using spectral energy distribution fitting techniques. International Centre for Radio Astronomy Research (ICRAR), a joint venture of Curtin University and The University of Western Australia
- *TN-Grid* : The gene@home project is an implementation of the PC-IM algorithm, whose purpose is to expand Gene Regulatory Networks (GRN). Each network is a graph that specifies the causal relationships inside this set of genes, and helps in studying the gene expression phenomenon: the process through which the DNA is transcribed into RNA and the RNA translated into proteins. National Research Council of Italy (CNR)
- *VGTU* : Distributed computing platform for scientists of Vilnius Gediminas Technical University (VGTU). Vilnius Gediminas Technical University
- *Universe@home* : Physics and Astronomy. University of Warsaw
- *YAFU* : Factorize numbers of 70-130 digit length which are needed to bring Aliquot Sequences to a size of 130. Private
- *yoyo@home* : Brings existing distributed computing projects to the BOINC world using the BOINC Wrapper technology. Supported by Rechenkraft.net [16]
- *World Community Grid* : FightAIDS@home, Smash Childhood Cancer, fight Tuberculosis, research better materials for solar panels. Sponsored by the IBM responsibility initiative [11]

13.3 Credits

The authors credit Rob Halfoerd [3] and the Gridcoin community for the ideas and technical work expressed in this paper. The paper structure and some sections are sourced from an anonymous Google document [47].