

A Renewable Energy Powered Trustless Value Transfer Network

A Solar Powered SolarCoin Generator Node and a Process to Generate SolarCoin from the Sun Automatically



White Paper

2015/11/09

Authors:

Luke P. Johnson, Solcrypto

Co-Authors:

Ahmed Isam, Solargenix

Nick Gogerty¹, Joseph Zitoli¹

¹SolarCoin Foundation

Document Created According to the Open Standards Principles¹
To the extent possible under law, Solcrypto has waived all copyright and related or
neighboring rights to this document.
This work is published from: Japan.

¹ <https://open-stand.org/about-us/principles/>



Table of Contents

(1) Abstract.....	2
(2) Rationale.....	3
(3) What is The SolarCoin Network?	4
(4) Proof-of-Work (PoW) Phase	5
4.1 Structure	5
4.2 Process.....	6
(5) Proof-of-stake-Time (PoST) Phase.....	6
5.1 Structure	6
5.2 Process and need for a low carbon blockchain alternative	7
5.3 The proof of stake-time protocol	8
(6) Actual Solar Powered SolarCoin Node Construction.....	10
6.1 Introduction	10
6.2 Component List.....	11
6.3 Construction.....	13
6.4 Communication Protocol of the Node	13
(7) API Overview	14
7.1 Definition of requirements and standardization	14
7.2 Further development	15
(8) Further Developments to SolarCoin Ecosystem.....	15
(9) References:	15

(1) Abstract

The purpose of this work is to show how low carbon value can flow across a network and how SolarCoin can operate. The article aims to explain the added value that SolarCoin creates and further to show how a solar powered node on the SolarCoin blockchain actually operates. A test SolarCoin node was also created.

The aim of this document is to disseminate valuable information that crosses over between solar engineering, network engineering and finally blockchain development and fintech.

The work starts by introducing how to get SolarCoin- either generating it from solar energy, or by trading it. Then the work goes on to explain a general overview regarding how blockchains operate for people who are new to the blockchain technology.

And finally the document details plans for a solar powered SolarCoin node that generates SolarCoin and simultaneously protects the transparent consensus ledger.

A solar powered SolarCoin node was constructed and tested for an 11-month period and still ongoing at our research labs in Tokyo. The details of the



construction and operation of this setup were documented. This document was written in the intent of freely distributing information so that further innovation can occur in the future. In the future, it is hoped that the process of creating an open source SolarCoin blockchain node will be streamlined and simpler, so that SolarCoin nodes can proliferate. This will enable more people to benefit from the added value that SolarCoin has for planet Earth, and its people.

(2) Rationale

A more distributed financial system that is secured and generated by renewable energy would help society with transparency, ease-of-use, access, entrepreneurial and innovation flow and more efficient allocation of scarcity to individuals willing to participate. These are beneficial because they don't rely on centralized strict or hierarchical social systems to secure the process of the allocation of scarcity. Additionally as base inputs these systems are not inherently powered by fossil energy. A centralized system that is powered by fossil energy is a risk to the future of human civilization because (1) it promotes centralization of power, corruption, cronyism and decision making processes that are not dependent on distributed data flow (2) it is inherently less robust in its design as it is vulnerable to a single point of attack and (3) it introduces more carbon into the Earth's atmosphere which has been shown to accelerate the affects of human induced climate change.

Conversely, a distributed open consensus system that is powered by renewable energy is (1) non-centralized (2) robust to attack on a single point as the network size increases (3) able to verify consensus efficiently, will not inherently promote power waste and can be available to anyone in the world who owns a solar panel and some off-the-shelf networking technology and open-source software, (4) possibly powered by solar energy and (5) can disseminate information across the whole network efficiently that can gather accurate and distributed data about interest rate and other quantifiable variables.

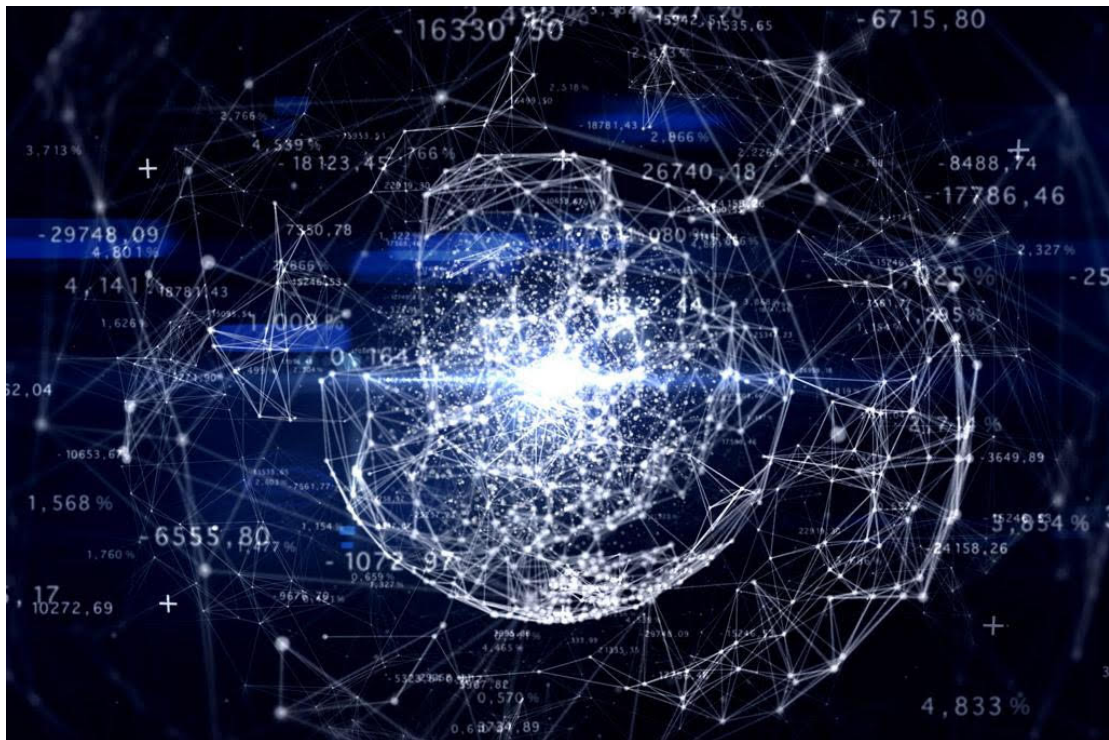
An individual or organisation on the planet participating in the renewable powered open network consensus system will be able to access a (1) sophisticated and distributed financial system (i.e. like Bitcoin and corresponding eco-system) (2) possible smart contract systems that could verify land-ownership, contracts and other trustless lending and financial innovations, (3) micro-payment systems (4) fast money transfer systems. This opens the system in order to improve the financial access and reduce costs for another potential 2 billion people in the world that currently do not have access to power, let alone a financial system. In addition, existing systems can be redesigned to increase efficiency and ease of use.

Since the first proposal of the Bitcoin protocol in 2008 by Satoshi Nakamoto [1] and the subsequent growth of the Bitcoin system globally a number of newer systems have been developed. These newer systems are relying less on the



computationally intensive Proof-of-Work System or (mining) and moving to other distributed Consensus systems like the Ripple protocol [2] or Vericoin's [3] Proof-of Stake Systems in order to secure the blockchain. The blockchain is a continuously updating open ledger that can be accessed by any individual or machine to verify the existence of a currency or contract very easily.

A low carbon mechanism that does not promote the waste of electrical power in order to secure the blockchain system is desirable. This is where Proof-of-Stake-Time (PoST) is added to the SolarCoin blockchain. PoST blockchain securitization has been demonstrated to reduce electricity usage by 97-99% when compared to POW blockchain securitization.



(3) What is The SolarCoin Network?

An electricity backed currency was first conceived in 2011 by Nick Gogerty and Joseph Zitoli in their original published paper “DeKo: An Electricity-Baked Currency Proposal” [2]. In 2013 the Gogerty and Zitoli formalized the implementation by creating the SolarCoin blockchain and subsequently launching it in early 2014.

The SolarCoin network is an open transparent public ledger (blockchain) that has been running since January 2014-August 2015 on a Proof-of-Work consensus and from August 2015 onwards with a Proof-of-Stake-Time consensus.

The value of SolarCoin is connected to something tangible, the Sun, and people's desire to help planet Earth. The Sun has been powering planet Earth for over 4



billion years. In just 1 hour, the Sun provides enough energy for the entire human civilization to power itself for a whole year.

SolarCoin is a digital currency connected directly to a renewable energy source. It transfers value from **people to people** that want to use Solar Energy. This in turn promotes more people to make and use solar energy.

Eventually it is intended to build a basis for the world's solar energy value transfer protocol. This will be done using a network of solar powered nodes around the whole world. These directly interact with the SolarCoin blockchain stabilizing, supporting and maintaining it. The nodes don't even need an existing electrical grid. The SolarCoin nodes are powered by themselves as solar Photovoltaic systems. Some could be even on Wi-Fi and transportable, on your smartphone, for example.

This is ground-breaking, because until the nodes are actually installed in a lot of the world (about 2 billion people) may never have been granted access to electricity let alone a sophisticated financial system. SolarCoin actually provides a base for both. As the network grows, more users are added, more people use solar energy. More people are rewarded for choosing a low carbon electricity source and blockchain consensus mechanism. The system grows this positive cycle continues. The Earth can be placed on a path to escape the worst affects of human induced climate change possibly limiting the temperature increases.

(4) Proof-of-Work (PoW) Phase

4.1 Structure

Traditional Proof-of-Work [5] mining of the block reward in the continually updating blockchain has been the method initially proposed by Sakamoto [1] in 2008. Proof-of-work protocol is a way of solving a challenge-string or mathematical puzzle. A person or prover of the work will need to come up with their corresponding response string (proof) to the challenge string of the representing mathematical puzzle. Which in this case is a hash function. The only known way to find a proof string is to try many combinations in the corresponding proof string. This could mean if you have a hash function that has for example 40-bits, about 2^{40} steps or different strings are on average required to find the proof string. This largely comes out to requiring large computational force (computing power) to solve the proof string. Once the proof is solved, it is very easy and fast to validate the solved result.

Bitcoin, Litecoin and many other crypto currency variants employed this strategy to issue consensus across the network.

The PoW method uses brute computing force to find the block reward and has been noted to promote electricity wastage and an arms race for “miners” to



increasingly deploy more powerful processors to locate the block reward (solve the mathematical proof) and unlock coins. As the Bitcoin ecosystem developed, more mining power became concentrated to mining or centralized server mining farms. This actually decreased the stability of the blockchain because it increased the risk of a 51% attack on the consensus network.

4.2 Process

For SolarCoin, about the first 34 million SolarCoins were mined from January 2014 to September 2015 using the PoW consensus [5]. The original blockchain was designed on a Litecoin fork. Additionally before the PoW phase was launched publically the SolarCoin Foundation (SCF) pre-mined about the additional 98 billion SolarCoin and are keeping them in cold storage. These coins are earmarked for future solar energy generation claims for approximately the next 40-years. This creates a secondary mechanism whereby the solar energy generator can apply to the SolarCoin foundation directly or via a localized network of authorized SolarCoin foundation affiliate websites to ask for SolarCoins to be sent to their wallet once they prove that they have generated solar energy via documentation or authorized electricity metering. After this first phase, the network hard-forked to a Proof of Stake Time (PoST) blockchain on September 25th 2015 at Block 835,213.

(5) Proof-of-stake-Time (PoST) Phase

5.1 Structure

Proof-of-Stake has been proposed to originate in comments about Bitcoin by Nick Szabo in May 2011 in discussing alternative proof systems. [3] In November 2011 Sunny King made the first commits on github and the development and implementation of the new proof system had begun.

The proof-of-stake process to reach consensus can be explained by the analogy of “staking” a claim. In the former wild-west frontier society of the early United States settlers who first reached new lands needed to “stake their claims” to new land and therefore took ownership of land to cultivate and manage under their ownership rights. In the analogy, Coins are staked or claimed via an open and transparent consensus ledger (The Blockchain). These staked coins are earmarked to the wallet address that is staking the coins at a certain point in time. Therefore each wallet that is generated is a node of the consensus network and will tell the other nodes how many coins are staked in that wallet at that time. This is a continual and ongoing process that is propagated through the blockchain over time. Therefore as the network grows, more crosschecks and confirmations of the amount of staked coins in each wallet happen.

Inherently the PoS system is more efficient than the PoW at reaching a consensus, it is lower cost in terms of resource usage (computing power) and also electricity usage. A number of variants on the PoS system are already in existence and operational on their own separate blockchains. These include the Vericoin



“proof-of-stake-time” or POST protocol [4]. Early Versions of the PoS protocol use the “Coin age” as the method for the proofhash in the block reward-solving scheme. For example, this first occurred in the Peercoin case. Other cases were Nxt and Blackcoin. Nxt currency was the first exclusively Proof-of-Stake currency. The Nxt developers did not use “Coin age” as a factor in reaching consensus in order to mitigate the risks of excessive coin age. Blackcoin made a custom new method of reaching stake consensus and Nxt use the Blackcoin protocol. Vericoin forked from Blackcoin prior to their custom protocol being implemented and used the code base from NovaCoin which is a modified version of PeerCoin. Finally the SolarCoin POST hard fork was based on the Vericoin fork.

5.2 Process and need for a low carbon blockchain alternative

The SolarCoin hard fork from the PoW phase to the Vericoin based SolarCoin POST phase occurred in September 25th 2015 at block number 835,213.

The main difference to previous PoS protocols is the proof hash criterion for consensus in the PoST case. This uses “Stake time” as an alternative to “Coin-Age” to solve the proof of hash criterion.

There has been a lot of criticism since the creation of Bitcoin and it’s associated PoW blockchain about the amount of electricity needed to sustain the consensus mechanism.

How much energy does Bitcoin use? Some estimates converge on about 10 Watts per GH/s (10 watts per Giga-hash per second). Anecdotal evidence cites somewhere between 10 and 0.5 Watts per GH/s. It depends if you are mining the Bitcoin using a Raspberry Pi or a more efficient ASIC miner. [6] At current rates of the amount of GH/year for Bitcoin, this calculates to about 452,625,810 GH/s or $10W * 452,625,810 \text{ GH/s} = 4,526,258,100W$ or 4.53 GW. To convert power to energy we need to multiply by the number of hours in a year including leap years ($24 * 365.25 = 8766$ hours) This means possibly around $3.96 \times 10^{13} \text{ Wh/year}$ or 39.6TWh/year. Other estimates range from 2-40TWh/year. Values for GH/s are taken from Bitcoinwisdom.com.

This means at the current user count of about 1.5 million Bitcoin users, about 4.53 GW of instantaneous energy is necessary just to maintain the blockchains consensus mechanism. This is about 3017 W/user (3kW/user) in instantaneous power or $3017 * 8766 \text{ hours} = 26,447,022 \text{ Wh/year/user}$ or 26.4 MWh/ year/user.

SolarCoin uses a Proof-of-stake time protocol. This means that the user needs to run a web-based wallet to maintain the network stability and users don’t need to participate in using increasingly energy intensive computer processors to search for coins. Assuming that the user is running a PC that approximately uses 100W to maintain the network (using a web based wallet), and the current number of network participants in the Solarcoin blockchain and assuming that everyone is staking 100% of the time, then the amount of energy needed to maintain consensus is approximately $100W * 300 \text{ users} * 8766 \text{ hours} = 262,980,000 \text{ Wh}$ for the whole blockchain, or 876,600 Wh/user/year or 0.88 MWh/ user/year.



Currently this is about 1-3% of the total energy necessary to support the consensus.

Now, if we create Solar-powered SolarCoin nodes, then this energy per user needs to be user less, because the computers that are used will be chosen to be low powered machines of about 5-8W instantaneous power.

Therefore the Solarcoin blockchain per user uses 1-3% of the BitCoin blockchains input energy to maintain consensus. With the potential to improve depending on how many low-power DC solar powered Solarcoin nodes are a percentage of the total network.

5.3 The proof of stake-time protocol

The main premise of proof-of-stake time is to use “Stake-time” as an alternative to “Coin-Age”. It is a non-linear proof function that defines a fraction of time for a wallet node that is active and idle at any given block.

The equation for the proof hash consensus degrades the ability of the wallets stake (consensus power) for wallets that are idle for longer times. [7].

The resultant effect of the proof-of-stake implemented consensus function is that it requires a network activity level that is proportional to the number of coins held, and relative to the network strength. Actively staking a wallet is incentivized to maximize the likelihood to signing a block, and to earn all the matured interest in reward for doing this.

In the Vericoin version of the PoST protocol this was the case that the new 'stake-time window' mechanism progressively rewards more consecutive staking and decreases maximum matured interest of the less active nodes. Additionally, the previous Network Stake Dependent Interest (NSDI) is now a variable inflation rate that the new interest rate targets. A combination of these two factors results in a significantly greater individual interest rate for those who actively stake. The end result is a more active, secure network, which has proven to be virtually impervious to weighted 51% attacks on internal tests.

The following equations are defined to explain the Vericoin PoST protocol: Consensus-power (p), defined as the fraction of coin age (g) of the average network wide stake-time weight (n) over 60 blocks (1hour). (This assumes that the network can run at 60 blocks per hour.

Eqn1. Consensus-power (p):

$$p = g/n$$

Eqn 2. Time-active fraction (f):

$$f = \cos^2(\pi p) \{if(p > 0.45), f = m\}$$



Where m = minimum stake time of 8 hours. If the consensus-power (p) is greater than 0.45 all age is lost and the Time-active fraction is equal to the minimum stake time.

Vericoin decided that inflation targeted interest rates could be calculated for Vericoin, however for SolarCoin n is too small compared to the initial pre-mined supply (34 million).

This is shown in the original equations stated by the Vericoin paper:

Eqn.3 Interest reward (r):

$$r = gi * 33 / (365 * 33 + 8)$$

Where the interest reward rate (r) is the product of coin-age (g) and the interest rate (i), and an approximation of the number of days in a year. Interest rate is then calculated in the form:

Eqn.4 Interest rate (i):

$$i = (17 * (\log n / 20)) / 100$$

Where the interest rate (i) is logarithmically proportional to the network stake weight (n).

However for the SolarCoin version of the PoST protocol, there was a large number of pre-mined SolarCoin that was on the blockchain at the beginning of the release when the version 2.0.1 wallets were released. This meant that because there was no cap of the interest rate and a targeted change in the interest rate meant that the maximum interest that could be earned was a huge and undefined number (likely approaching infinity). Many community participants reported this immediately and a new version of the wallet was released at ver2.0.3. A new interest rate cap was implemented at 10%. Then quickly after this and a few days of PoST occurring it was calculated that because n is so small compared to the initial coin supply and because it is logarithmically proportional, the targeted interest rate would be stuck at 10% for years.

It was therefore recommended to reduce CPU usage (in line with the SolarCoin foundation goals of lowering CO₂), the calculation of n would be not calculated in the ver2.08 release. A set interest rate of 2% p.a. would then be capped.

On this date of writing, the network is stable on protocol version 2.08 and running at 1-2 blocks per minute. Currently it is at block 883,376. The SolarCoin PoST protocol has a set 2% interest rate and the nodes that are running are reporting this interest being delivered over the blockchain and then maturing after 500 confirmations.





(6) Actual Solar Powered SolarCoin Node Construction

6.1 Introduction

As an experimental test an off-grid stand-alone photovoltaic system was constructed from July to October 2014 and tested from November 2014-November 2015. The system is still generating on average 40Wh per day or 40/1000000 or 0.00004 SolarCoin (SLR)/day.

From October 2014-until the 31st of December 2014 the system was originally located on the 7th floor of an inner city Tokyo small office complex building and the PV system was facing East. A significant shading of the sun occurred both due to the fact that the system was placed on a building balcony and a large building was blocking morning light from the East. Still the 250W panel and corresponding system was able to generate 40-60Wh per day.

From the 1st of January 2015 until November 2015 the system was moved to the 3rd floor of another office build and that buildings balcony about 3km away from the first location. This balcony had significant shading (an even higher amount) than the first location and the system was only generating 15-20Wh per day or about 0.00002 SolarCoin (SLR)/day.

The off-grid power system was comprised of a 250W quasi-mono crystalline ReneSolar module, a maximum power-point tracker (Etracer) a DC-AC 12V inverter, about 5m of solar cabling running on a 12V system voltage and a 100Ah 12V lead-acid battery.

We chose the new quasi-mono cell structure for our module because of the module manufacturers very low temperature coefficient. Solar modules are semiconductors placed in the sun, therefore they output their highest efficiency at the lowest temperatures. The temperature coefficient of the Vitrus II cell technology is -0.4%/ °C. This is a few percent better than the industry standard. Although this would need to be independently verified by reading a third-party test report for these modules.

Additionally the system had a solar monitoring system comprised of a pyranometer, a two PT100 temperature sensors for ambient temperature and one PT100 temperature sensor for the battery, an Elseta WCC200 gateway for Modbus communication protocols and an Accuenergy AcuDC 240 series DC Power energy meter and associated shunt resistor for analogue DC energy logging and conversion to digital signals using the RS485 channel and the Modbus communication protocol.



The off-grid power system was designed to generate enough power to run the monitoring system off-grid over the whole year. However, in this case due to the severe shading limitations on the balcony's of both locations we had to use auxiliary power to run the monitoring system. That said, if this system was in full sun at the correct tilt angle of the latitude and increased to 500W continuous input, that will be able to cover all of the auxiliary power needs that the monitoring system requires. An initial PVSyst simulation was completed in PVSyst 6.3 to determine the energy yield of the off-grid system design and this showed that the system at 500W was more than enough to cover the power needs. The current system is severely shaded on a balcony and therefore is generating at maximum 5-8W in the middle of the day.

For a SolarCoin generation node, the monitoring system is actually not required (unless SolarCoin futures trading is required), only the communication gateway (WCC200) is necessary so that the analogue signal from the electricity meter can be fed and converted to a digital signal and a Modbus protocol so that the WCC200 can then send this to a communication server and the associated API that will graph energy output over time (kWh vs. time).

Probably the most important part of the system is converting the correct and accurate information from the DC side energy output and logging to the gateway. We chose the Accuenergy (AcuDC 240) meter because these have only recently been released for DC monitoring and have a high accuracy of $\pm 0.2\%$ on the output signal.

6.2 Component List

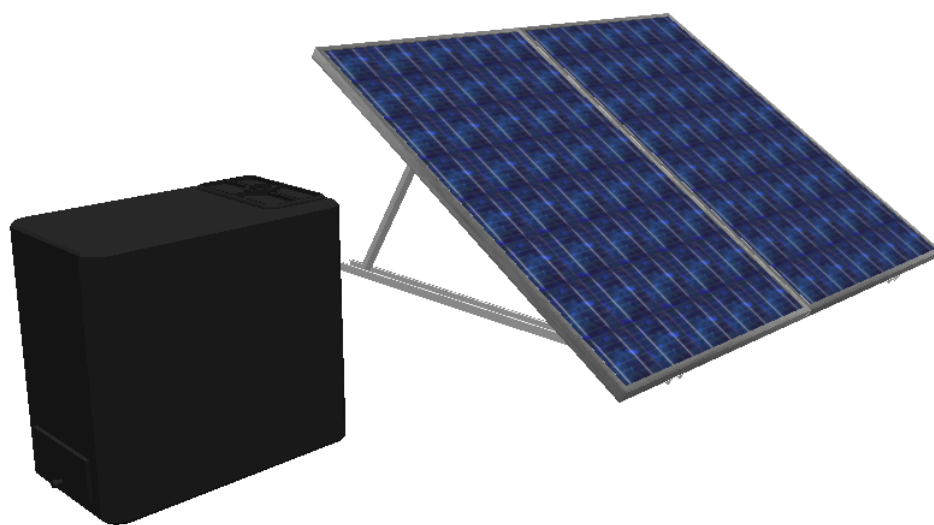


Figure 1- Black Box (SolarCoin Node includes a 100Ah battery, Maximum Power Point Tracking, analogue to digital converter for energy logging over RS485 and Modbus TCP/IP, Connection gateway to API), Solar Array's 2x 250W ReneSola Vitrus II arrays delivering 500W continuous peak power.



Component Type	Part
Solar Module x 2 (250W)	JC250M-24/Bb
Maximum Power Point Tracker	Etracer ET2415N
Lead Acid Battery	12V 100Ah
Inverter	12V HLS-500W
Solar Cables (5m)	Positive and Negative Cables for oversizing of solar module current
AcuDC 240	DC kWh meter
WCC200	Cloud Industries Gateway
AD Converter	DNA485
Pyranometer	LPPyra02
Associated active cooling fans	USB Powered cooling fans
Communications cables	Misc. communications cables

Table 1.0- Components for stand-alone SolarCoin Node.

Outputs include radiation (insolation measurements) updated every few seconds; kWh readings updated every few seconds and temperature readings. An example of 1 month's solar radiation output in the cloud industries login is found here in Figure 2.



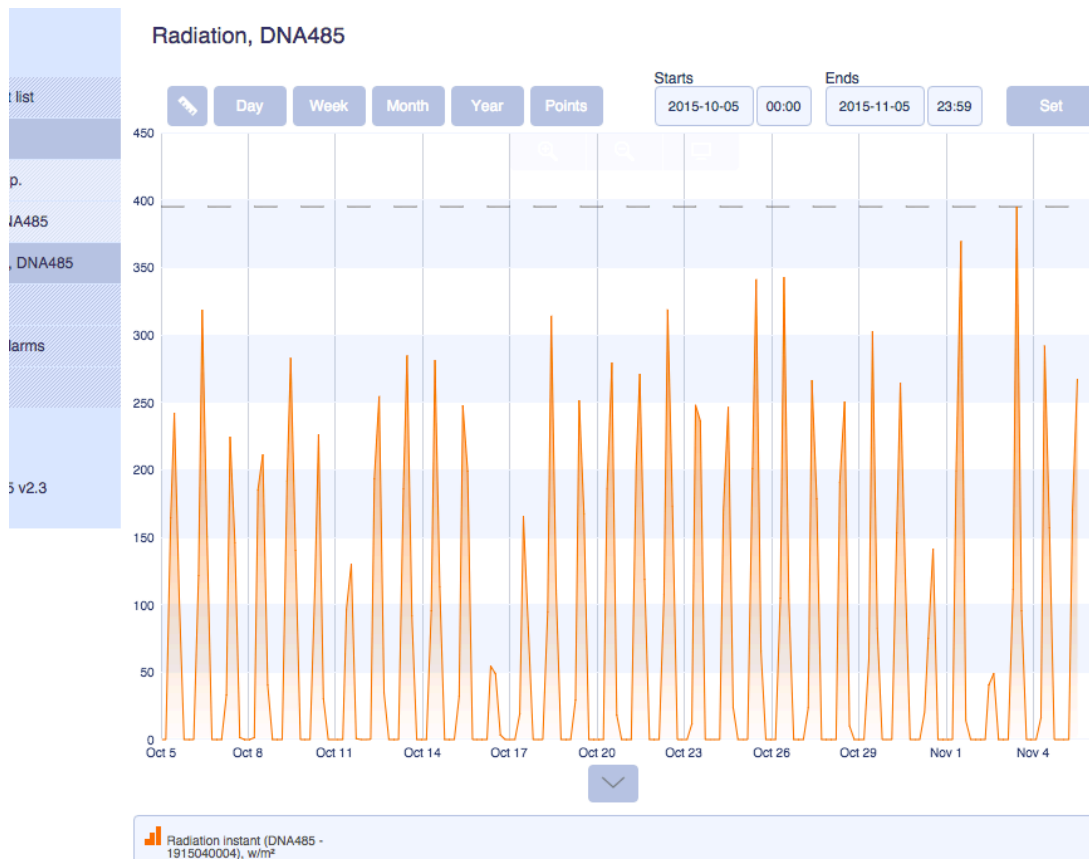


Figure 2- Solar Insolation for the balcony over a 1-month period. Remember this balcony is severely shaded showing that the maximum input solar insolation is <math><400 \text{ W/m}^2</math>, where in open fields this can routinely peak at above

6.3 Construction

The node took about 4 days to construct. It is made out of anodized aluminum and perspex covering all of the electronics for weatherproofing. Additionally all of the communication equipment is housed in an IP67 weatherproof electronics box. Including the WCC200 router and gateway. The node has been operational for about 1 year now from November 2014 until November 2015.

6.4 Communication Protocol of the Node

The communication process can be best outlined in a flow chart for understanding in Figure 3. It is assumed that all communication is secure and although the API is open, standard security practices are met to protect user privacy under existing governments privacy laws.

Essentially the analogue DC electricity is measured and then converted to a digital signal inside the ACU unit. The ACU unit then transmits this signal to a database structure on the Modbus TCP/IP protocol. In many cases many different types of protocols could be used like Profibus, AnyBus. The main point was to collect the structured database information on the servers and then



allowing the SolarCoin Foundation’s API to fetch the correct data. In this case a Cloud Industries Platform was used to collect, store and display the data. The affiliate websites own API needs to collect the Cloud Industries database information in the structured arrays and then send it to the receiving API that was written by the SolarCoin Foundation.

(7) API Overview

7.1 Definition of requirements and standardization

The SolarCoin foundation has expressed interest at making a standardized and lightweight API for the securitization of SolarCoin grants to the network. Affiliate websites like Solcrypto will participate by placing API calls and asking for verification in the SolarCoin granting procedure algorithmically.

So far a majority of API calls need to be implemented from the SolarCoin Foundation API in the software on GitHub called “Project Demeter” and associated project called “SolarCoin-Data-Extract”. [8]

Once this API is operational, then any SolarCoin affiliate website can send an API call and then get their SolarCoins processed by Project Demeter.

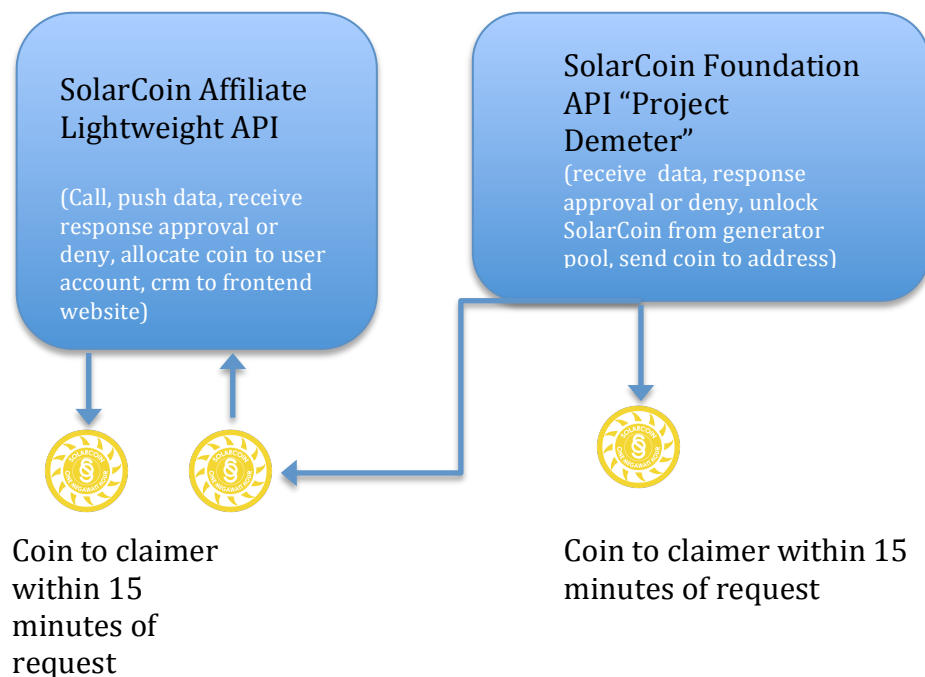


Figure 3- High level overview of claimant process.

7.2 Further development

It is also possible that affiliate websites deploy their own blockchains to administer their own users efficiently and transparently. For example using the ERIS industries stack could be a good example. This would only be investigated if it efficiently allocates coin flow to each user in the network and grows the network participants.

(8) Further Developments to SolarCoin Ecosystem

These are some further investigation points in order to grow network participants:

- Ethereum
- Cryptographically securing the generator pool with internal sidechains, multisig. Establishing a more liquid claimant market.
- Colour Coins
- Futures trading of SolarCoins by future simulation guessing of the SolarCoin generation amount on certain nodes and node cluster regions and then trading SolarCoin.
- POST Interest rate targeting and actual simulation according to geographic distribution and clustering of solar-powered SolarCoin nodes.
- Matlab simulations and projections of SolarCoin node clusters on a POST blockchain.

(9) References:

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org, 2008.

[2] Gogerty, Nick and Zitoli, Joseph, “DeKo: An Electricity-Backed Currency Proposal “ (January 4, 2011). Available at SSRN: <http://ssrn.com/abstract=1802166>

[3] David Schwartz *et al* “The Ripple Protocol Consensus Algorithm”, Ripple Labs, 2014.

[4] Vericoin POST White Paper

<http://www.vericoin.info/downloads/VeriCoinPoSTWhitePaper10May2015.pdf>

[5] Proof-of-work explained by the Khan Academy at URL:

<https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-proof-of-work>



[6] How Much Electricity Does Bitcoin Use? <https://medium.com/@interdome/how-much-electricity-does-bitcoin-use-c350bd84c64e>

[7] SolarCoin (SLR) market capitalization at URL:
<http://coinmarketcap.com/currencies/SolarCoin/>

[8] Project Demeter and Project SolarCoin Data Extract: <https://github.com/ahmed-isam/Project-Demeter/tree/4f7f0cc1b12f61f8ac194bba25a7f78a60cb0380/test>

<https://github.com/ahmed-isam/SolarCoin-Data-Extract>

