terraCoin:
Cryptocurrency for the plant

6.S898 Final project

Jennifer Switzer

December 12, 2019

1 Introduction

Blockchain-based cryptocurrencies such as Bitcoin provide secure, decentralized currencies free from the control of governments or banks. However, they do so at a steep environmental cost; the proof of work consensus algorithms that form the backbone of many such currencies are, by their very design, highly energy-intensive. A recent report found that, thanks to its high energy usage, Bitcoin alone could be responsible for 2 °C of warming within the next three decades [1].

For my 6.S898 final project, I decided to explore whether it would be possible to create a cryptocurrency with the same security properties as Bitcoin but significantly less impact. The outcome of this work is terraCoin, a proposed alternate cryptocurrency backed by the training of machine learning models that solve climate-related problems.

In this work, I contribute the following: (1) a theoretical design overview for terraCoin, including a problem submission platform; (2) a proof-of-concept implementation and preliminary evaluation of terraCoin's proof of useful work for the climate; and (3) a discussion of the implications of these findings for the future of a greener blockchain, including a roadmap for deploying terraCoin.

2 Background on blockchain

At the core of Bitcoin is a public record called a blockchain. A blockchain is an append-only list of records that are cryptographically linked and resilient to tampering. Blockchain was first developed for Bitcoin [2] and forms the basis of most cryptocurrencies today. However, the technology itself has a myriad of applications, including electronic document certification, secure voting, and even the optimization of energy grids [3]. This section provides an overview of blockchain technology.

Blocks. A blockchain is merely a public ledger consisting of sequential units called blocks. Each block can be thought of as a record that verifies a certain set of transactions. These transactions are not necessarily monetary; they may be records of any sort of activity, including votes, or the transfer of copyrights.

Miners. The blockchain grows thanks to the activity of entities called miners. In order to append a block to the blockchain, a miner takes in the previous block and the transactions it wishes to verify, and completes some expensive computation called a *proof of work*, which generates the next block. Once a block has been generated, it is published to the blockchain network, and other miners validate that the generated block is legitimate.

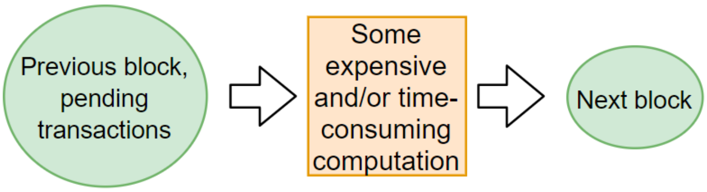
Previous block, pending transactions
Some expensive and/or time-consuming computation
Next block

Figure 1: Proofs of work require computationally-intensive calculations by design

Proof of work. The proof of work takes in the numerical representation of the previous block in the chain, as well as the set of transactions to be verified, and generates a numerical representation of the next block. This process is summarized in Figure 1. There are several formal requirements on the proof of work:

1. It must be expensive by design, so that miners cannot simply fake transactions.
2. It must be relatively simple to verify, so that generated blocks can be easily validated.
3. It must take a hash of the previous block as input, in order to ensure the integrity of the blockchain and prevent the pre-computation of blocks. It must be impossible to generate a block without first knowing the previous one.

It's important to note that, since the proof of work must be computationally intensive by design, it is not possible to reduce the energy usage of blockchain-based technologies simply by increasing efficiency.

Bitcoin. Blockchain technology has been the basis of multiple cryptocurrencies, of which the most notable and widespread is Bitcoin. Bitcoin's proof of work scheme involves breaking cryptographic hashes. Miners are given the result of a SHA-256 hash, and must determine the input value that generated it. The only way to do so is through brute-force trial and error; however, once a solution is found, it is relatively simple to verify. Successful miners are rewarded in bitcoins.

3 Motivation

This project was motivated by two observations: first, that blockchain consensus algorithms based on proofs of work, by their very design, require the expenditure of large amounts of computational power; and second, that climate modeling involves performing computationally-intensive tasks. This raised the question: Is it possible to design a proof of work that involves performing some useful computation for climate science?

This section explores, first, the environmental cost of Bitcoin's power-hungry consensus algorithm, and second, what existing alternative consensus algorithms have been developed, including proofs of useful work that have the potential to be applied to climate science.

3.1 The environmental cost of Bitcoin

Bitcoin has been widely criticized for its disproportionately huge energy use. Estimates of its annual consumption range from 20 to 70 TWh of energy each year– roughly equivalent to the energy consumption of the entire countries of Ireland or Austria, respectively. [4] [5]. These numbers are especially huge considering that Bitcoin transactions account for only 0.03% of non-cash transactions. Furthermore, Bitcoin's energy usage is liable to increase, as the currency becomes more widely adopted and its proof of work problems more difficult [6]. It may not be surprising then that a recent study estimated that Bitcoin alone could be responsible for 2°C of warming within the next three decades [1].

Some Bitcoin proponents have argued that Bitcoin is in fact environmentally friendly since a large proportion of its mining makes use of renewable energy sources such as geothermal and hydropower [7]. However, there are a few major issues with this claim. The first is that there is nothing intrinsic to Bitcoin (or any other cryptocurrency) that necessitates the use of renewable energy; mining companies are highly incentivized to make use of the cheapest energy sources they can find, which oftentimes happens to be remote sources of hydro or thermal power. However, if the energy landscape were to change or if mining companies were to somehow lose access to these sources, they might again turn to fossil fuels. Second, in many cases Bitcoin's use of these renewable resources merely displaces the use of fossil fuels; if there is only so much wind energy available in a region, for instance, then the presence of a wind-based Bitcoin mining farm will decrease the amount of renewable energy available to other actors. Thirdly, hydropower, a major source of renewable energy for Bitcoin mining facilities, has a huge local environmental impact [8].

3.2 Existing solutions

Reducing the energy cost of Bitcoin's proof of work would be the best way to curb its environmental impact. However, as mentioned previously, this is difficult to accomplish given the nature of the proof of work; it must, by design, be expensive.

There are many proposed solutions for overcoming this limitation. These proposed solutions typically fall into one of two categories: (1) Consensus algorithms that do not rely on a proof of work [9], and (2) Proof of useful work algorithms, which perform some useful computation as a side-effect of their proof of work [10].

Alternative consensus algorithms to proof of work include proof of stake (where miners have to risk forfeiting their existing coins if they falsify a transaction), proof of capacity (which is based on disk space), and proof of burn (which is based on burning existing coins). Although all of these alternative consensus algorithms have flaws that have prevented their wider adoption, with time and future development they may become viable as an alternative to proof of work [11].

Proof of useful work algorithms are proofs of work that perform some externally useful computation. For instance, Primecoin is a cryptocurrency with a proof of useful work scheme based on finding large prime numbers [12]. Although this proof of work still involves expending large amounts of energy, the amortized cost of maintaining the currency is reduced, since the energy expended also results in the calculation of useful results. Designing a truly useful proof of work is difficult, however, due to the requirements on the proof of work, which must be: computationally intensive; relatively easy to verify; and provably inseparable from the block it verifies. Failure to meet these criteria would compromise the security of the blockchain. Academic research into proofs of useful work has described some general classes of problems that may fit these requirements [10].

A proof of useful work with particularly wide applicability is described in Coin.AI [13]. Coin.AI is based on training machine learning models until a certain performance threshold is met. I chose the Coin.AI algorithm as the basis for terraCoin's consensus algorithm.

I made the decision to go with a proof of useful work, and Coin.AI specifically, for multiple reasons. First, although alternative non-proof-of-work consensus algorithms are promising, they have seen relatively little widespread adoption. For instance, the cryptocurrency Ethereum has been attempting to shift to a proof of stake system since 2014, so far without success. They have reported several large barriers to adoption, including the fact that the security properties of proof of stake are as of yet unproven [14]. While the technology is certainly promising, it is not yet mature. Additionally, the majority of popular cryptocurrencies today remain based on proofs of work, so a proof of useful work may have a better chance of adoption. Second, the Coin.AI scheme provides a proof of useful work that, if feasible, could be applied to solve a wide variety of problems. Anything that can be specified as a machine learning problem can be solved using Coin.AI. There are many areas of research within climate science to which machine learning can be applied, including the parameterization of moist convection [15], which has been identified as a crucial area of research for reducing uncertainty in climate modeling.

The Coin.AI algorithm, and how it was adapted for terraCoin, is described further in the following section.

4 PWC: Proof of Work for the Climate

This section describes the core of terraCoin: a blockchain proof of work that performs useful computations for climate science. This Proof of Work for the Climate (PWC) is heavily based on the mechanism described by Coin.AI [13], a proof of useful work based on the training of machine learning models.

This section provides a description of the formal requirements that must be met by a blockchain proof of work; an overview of the Coin.AI mechanism, and how it was adapted to terraCoin; and a discussion of some climate-related problems that can be solved using this mechanism.

4.1 Formal requirements on the proof of work

In order to maintain the integrity and security of the blockchain, the proof of work must satisfy the following requirements:

1. The problem must require significant computational effort, in order to ensure that some work was actually performed by miners.
2. The problem must be dependent on the hash of the previous block as an input variable. It must be impossible to generate the next block without the previous one.
3. Solutions must be relatively easy to verify, so that they can be validated.
4. The mining scheme must have a well-defined method of selecting a winner.
5. Once a block has been mined, all other potential blocks under mining must be discarded.

These requirements must be met in order to secure the blockchain. A proof of work that does not meet all of these requirements may provide weak or non-existent security guarantees.

4.2 Coin.AI

Coin.AI's proposed proof of useful work requires training deep learning models until a certain performance threshold is met. Training a deep learning model is generally

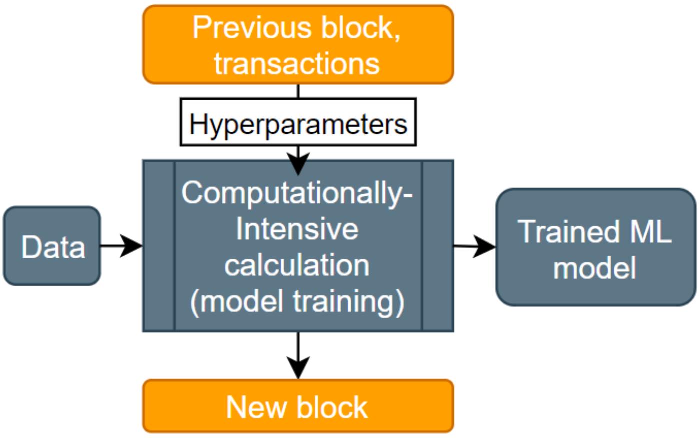
Previous block, transactions
Hyperparameters
Data
Computationally-Intensive calculation (model training)
Trained ML model
New block

Figure 2: The Coin.AI proof-of-work scheme is based on training machine learning models.

considered a computationally expensive process, so this problem meets Requirement 1.

The process of mining a new block is as follows: The miner fetches the hash of the previous block, and selects a set of N transactions that it wishes to verify. These form the input to the proof of work.

The inputs to the proof of work are used to specify the deep learning model to be trained. This specification is performed as follows: The hash of the previous block and the transactions to be generated are concatenated, and the digest of this concatenation is computed using a crytographically secure hash. The obtained hash is then used to specify the hyperparameters of the model to be solved. These hyperparameters include the number of convolutional layers in the model, the number of filters at each layer, and the activation function of each layer.

The mapping from the hash to the hyperparameters of the model is left to be specified by the implementation. However, it's essential that the range of possible models is large. In order to meet Requirement 2, it must be functionally impossible for a miner to compute a block without the hash of the previous one. If the problem space were too small, a miner could simply solve all possible problems ahead of time, thus precomputing all possible blocks.

Once the topology of the machine learning model is specified, the miner trains the model on the current active problem. The active problem consists of a training data set, a test data set, and a minimum performance threshold that the trained model must meet. It is publicly available and accessible to all miners and validators.

When the miner reaches the specified performance threshold, it submits the completed problem for validation. Validation has two steps: First, the validator verifies that the topology of the trained model was calculated properly from the inputs; and, second, they ensure that the performance of the trained model does indeed meet the performance threshold. Checking that a trained model meets a certain threshold of performance is a relatively cheap operation, especially when compared to training the model itself, so Requirement 3 is met.

The first miner to produce a trained model that meets the specified performance is considered the "winner" and receives a reward in terraCoins. When a winning model is chosen, it replaces the previous "most recent" block in the blockchain; all models specified using this previous block therefore become invalid. Thus Requirements 4 and 5 are met.

4.3 The Proof of Work for the Climate

terraCoin employs a Coin.AI-based proof of work that solves climate-related machine learning problems. Quite simply, the Coin.AI algorithm is applied to solve climate related machine learning parameterizations. For implementation details, see Section 7.

There are many climate-related problems on both the science and mitigation size that can be addressed by machine learning, including modeling solar fuels, controlling smart homes, and predicting sea level rise[16].

One particularly interesting application is using machine learning to parameterize moist convection (cloud formation) [15] [17]. Cloud formation is the largest source of uncertainty in climate modeling [16]. The science of cloud formation is so complicated that physical models of these processes are typically too computationally expensive to include in climate models. However, trained machine learning models have been shown to provide similar performance to physical models at a fraction of the computational cost [15]. I propose that terraCoin first be used to tackle this category of problems.

5 System overview

terraCoin consists of four major components, as shown in Figure 3: the problem generator; the terraCoin engine; miners and validators; and users of the currency. This section describes the interactions between these components, and how they accomplish terraCoin's two core functionalities: Validating terraCoin transactions, and solving climate-related machine learning problems.

The problem generator, described in more detail in the following section, generates the problems to be solved by the miners. At any given time, there is one

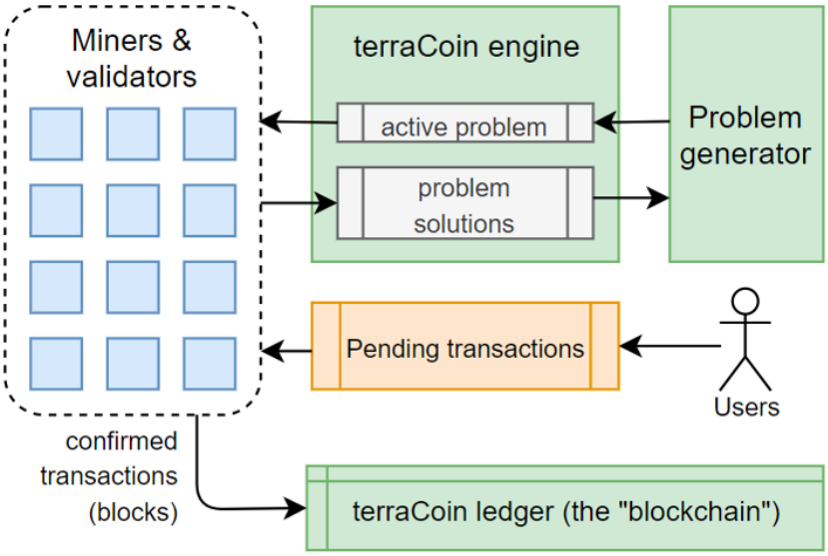

Figure 3: An overview of terraCoin

active problem, the problem to be solved in order to mine the next block. The current active problem is broadcast publicly and maintained by the terraCoin engine.

The terraCoin engine maintains a record of pertinent information, including the active problem and the solutions to previous active problems. For the most part, it acts as a relay between the problem generator and the miners. Note that the inclusion of the problem generator and the engine mean that terraCoin, unlike Bitcoin, is not fully decentralized. This is an unavoidable limitation, since the problems to be solved must be chosen carefully in order to further terraCoin's mission of completing useful problems for climate science.

Miners and validators form the core of terraCoin. They are independent entities, either individuals or professional mining companies, who mine new blocks in exchange for terraCoins. Miners read in pending transactions from a public database, and the active problem from the terraCoin engine. They then calculate the model to be trained according to the algorithm described in Section 4.2, and train the model until they reach the threshold performance. The first miner to reach the threshold is considered the "winner", and their solution passes to the validation stage. Once the solution has been validated, it is appended to the terraCoin blockchain. The solved problem is passed back to the terraCoin engine.

terraCoin users are those who perform transactions with the coin. They may be individuals or businesses. These transactions are pending until they are encoded in a block that is appended to the blockchain. Similar to Bitcoin, this means that terraCoin transactions would likely have a significantly longer delay than traditional means of monetary exchange such as Visa.

6 Problem selection

This section describes how terraCoin selects the problems to be solved by the engine. In the context of this project, a problem consists of the following: a training data set, a validation data set, any constraints on the system, and a quality metric for the system. In order to ensure that the problems being solved are truly climate related, there must always be some central authority that determines which problems to solve.

6.1 Problem collection

terraCoin's problem collection system consists of two major components: (1) an accreditation system that allows researchers to register themselves as climate scientists and thus gain access to the terraCoin system; and (2), a submission portal for those accredited researchers to submit their problems.

Accreditation. Accreditation ensures that the problems accepted by terraCoin are legitimately relevant to climate science. Any researcher wishing to submit problems to terraCoin must first apply for accreditation. As part of this application, they must provide a description of the problems they intend to submit, and how they will advance climate science research. As mentioned in Section 4.3, a preference will be given (in the short term) to problems related to cloud formation.

Accepted researchers will receive terraCoin accreditation for the year. This accreditation will allow the researcher to submit a predefined number of problems. They will also be able to specify a priority level for each problem submitted, so that particularly important research can be fast-tracked. The exact number of problems a researcher is allowed at each priority level for any given time period would be determined by the number of accredited researchers and the availability of terraCoin miners. Accreditation must be renewed each year in order to keep problem submission rates in line with the rate of problems solved by the terraCoin engine.

Problem submission. Once a researcher is accredited, they gain access to the terraCoin submission system and are able to submit their problems. Each problem submission consists of the following information:

1. The problem itself (training and validation data, constraints, and quality metric)

2. The problem's priority level

3. A qualitative description of the data specific enough for other researchers to understand

Submitted problems will be validated to ensure that the problem is well-defined, and that the researcher submitting the problem has not exceeded their submission limit. Once a problem is validated, it is passed into the problem management system, described in the following section.

6.2 Problem management

Validated problems must be stored before being passed into the terraCoin engine. There are two stages to this storage: the waiting problem pool, and the active problem pool.

Waiting problem pool. Newly validated problems are placed directly into the waiting problem pool. The waiting problem pool can hold an unlimited number of problems; however, in practice the number of waiting problems should remain relatively small if the submission and solve rates are kept relatively equivalent.

Problems in the waiting problem pool are ranked according to their assigned priorities. These ranks determine the probability that a given problem will be chosen for the active problem pool.

Active problem pool. The active problem pool contains a defined number (2^{16}) of problems that are available to be pulled in to the terraCoin engine. Each problem in the active problem pool is assigned a unique 16-bit identification number. This identification number allows the terraCoin engine to specify the problem to be selected for the engine.

All problems in the active problem pool have an equal chance of being selected by the terraCoin engine. This prevents miners from predicting the next problem to be chosen.

Problem selection. When the terraCoin engine requires a new problem, it sends a request to the active problem pool. This request will include the identification number of the problem to be passed to terraCoin.

In response to this request, the specified problem is passed to terraCoin. The problem is removed from the active problem pool, and a request for a replacement is sent to the waiting problem pool. The waiting problem pool selects the replacement problem based on the rankings of problem importance. The replacement problem will be given the same identification as the problem it is replacing.

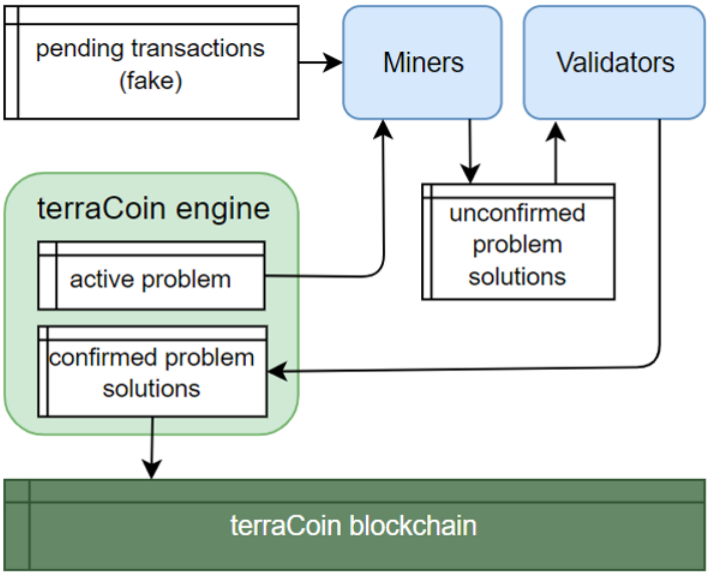
pending transactions (fake)
Miners
Validators
terraCoin engine
active problem
unconfirmed problem solutions
confirmed problem solutions
terraCoin blockchain

Figure 4: My proof of concept implementation includes miners, validators, and a simple terraCoin engine.

6.3 Posting solutions

When a problem is solved by the engine, the researchers who submitted the problem are notified and the resulting solution is posted to an online forum. This forum is open to the general public, and maintains a record of all of the solutions generated by the terraCoin engine. This ensures that the resulting insights are available to the community at large.

The solution to a problem consists of the following information: (1) the problem itself, and the qualitative description of the data originally provided; (2) the trained model; (3) the hyperparameters of the trained model.

7 Implementation

I created a basic proof of concept for terraCoin that includes miners, validators, and a basic terraCoin engine. The proof of concept, though simple, provides an opportunity to reason about the feasibility and potential security properties of such an implementation.

7.1 Overview

The terraCoin proof of concept consists of 400 lines of Python, organized as follows: 50 for the transaction generator, 100 for the terraCoin engine, 150 for mining, and 100 for validation.

The system, shown in Figure 4 is organized into the following interacting software components: A transaction generator, a basic terraCoin engine, and multiple mining & validating entities. It also contains several public databases, including pending transactions, unconfirmed problem solutions, confirmed problem solutions, and the terraCoin blockchain itself.

The transaction generator generates fake transactions that mimic real terraCoin transactions. The generated transactions are placed into a database that is readable by the miners and validators.

The terraCoin engine maintains the active problem–a set of training data, testing data, and performance threshold–and a database of confirmed problem solutions. In my basic implementation, there is no problem generator, and the active problem does not change.

Mining entities read in pending transactions and the current active problem, and generate unconfirmed solutions. These unconfirmed solutions are then written to a database that is readable by validators.

Validators read in unconfirmed solutions and check if they're legitimate. Once more than 50% of validators have confirmed a problem solution, the solution is passed to the terraCoin engine, which publishes the trained model and writes the generated block to the blockchain.

My code is available at https://github.com/jfswitzer/898-terracoin.

8 Informal evaluation

This section provides an informal argument for the security properties of terraCoin as implemented. Specifically, I evaluate whether terraCoin meets the three major requirements for a blockchain proof of work: (1) it must be computationally intensive to solve; (2) it must be relatively cheap to verify; and (3) it must be impossible to pre-compute blocks.

8.1 Complexity of mining and validation

As a proxy for computational complexity, the time elapsed for both mining and validation was measured. Results are summarized in Figures 5 and 6. The latency

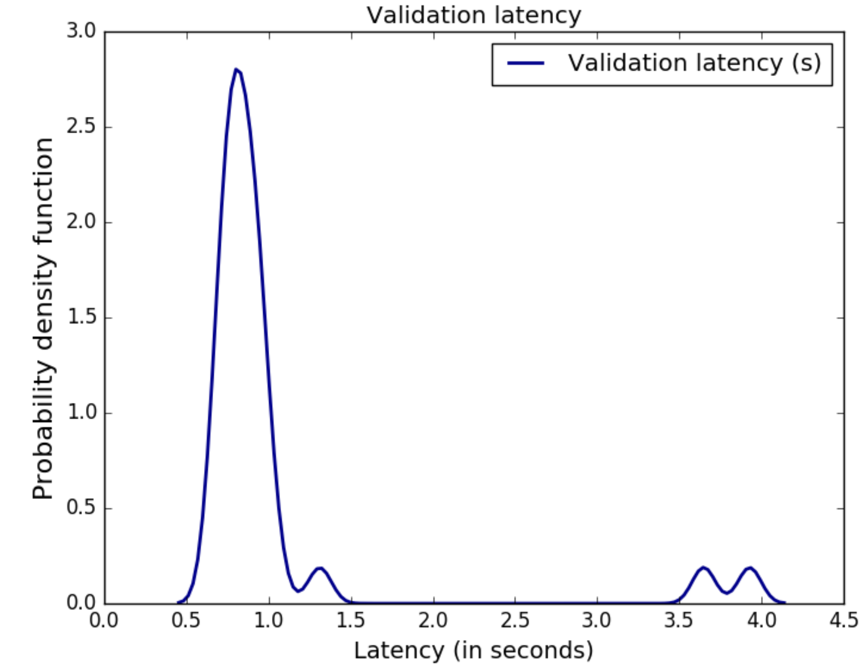

Figure 5: Latency of validation

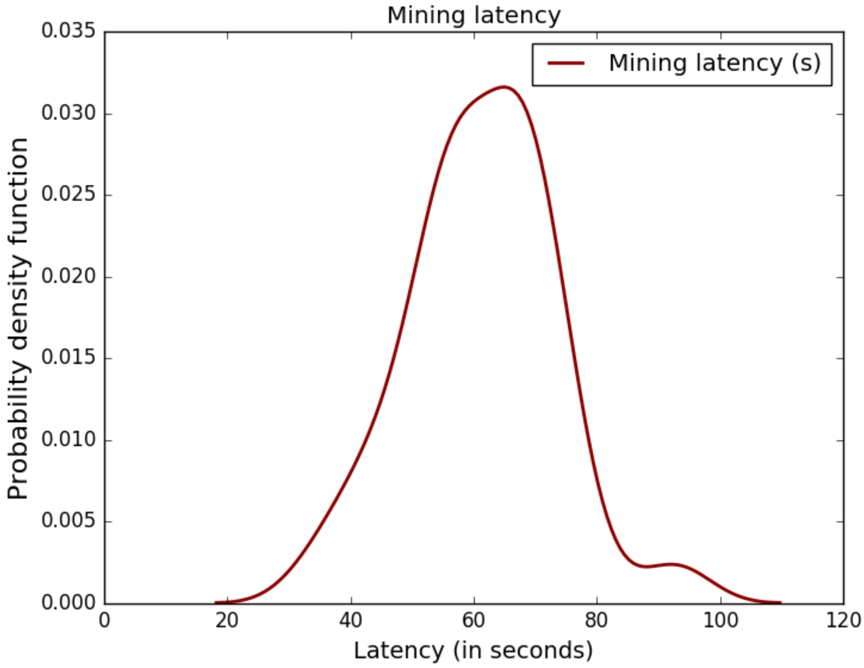

Figure 6: Latency of mining

	Fully correct solution	Doesn't meet performance threshold	Trained on incorrect training/test set	Incorrectly computed hyper-parameters
Confirmed?	*Y*	*N*	*N*	*N*

Table 1: terraCoin validators only confirm correct solutions

of mining was on average 60*x* that of the latency of validation. Although this ratio is promising, it is nowhere close to Bitcoin's ratio of 10 minutes for computing a solution, and near-instantaneous verification.

However, this ratio could be significantly increased in a production-level implementation by tuning the complexity of the model to be trained, and increasing the efficiency of validation. These preliminary results indicate that terraCoin does meet (or at least has the potential to meet) Requirements 1 and 2.

8.2 Success of validation

In order to ensure that blocks cannot be pre-computed (Requirement 3) it's imperative that validators properly catch invalid solutions. I created a small test suite of correct and incorrect solutions in order to test the functionality of the validators. Table 1 summarizes the results of this evaluation.

There are three ways that a solution (i.e. a trained model) can be found invalid. The trained model might be correctly specified but not meet the specified performance threshold. It could also have been trained on the wrong data, in which case it might meet the performance threshold for that data but not for the correct data. Finally, it may have hyper-parameters that were not correctly computed from the input hash. As shown in Table 8.2, the terraCoin validators catch each category of invalid solutions, and only confirm the valid solutions. Requirement 3 is therefore met.

9 Discussion

This work has explored the possibility of a proof of useful work for climate science, and has proposed terraCoin as one potential means of accomplishing such a proof of work. This section discusses the implication of these findings for the future of proofs of useful work, and greener blockchain technology in general.

9.1 Implication for proofs of useful work

As far as I am aware, my proof of concept is the first implementation of the Coin.AI algorithm. Its preliminary success is hopefully indicative of the technical feasibility of the scheme. If such a proof of useful work were to be widely adopted, it could go a long way towards reducing the energy usage of blockchain-based cryptocurrencies. Even if the problems being solved were not climate related, the double-usage of the expended energy for the proof of work and the training of ML models would reduce the amortized energy cost of the blockchain.

More work is needed to confirm the security properties of the Coin.AI scheme, however. Without a formal analysis showing that this scheme provides similar security properties to Bitcoin's current proof of work, blockchain experts and consumers alike would be wary of adopting it.

9.2 Ensuring the adoption of terraCoin

Ensuring the widespread adoption of terraCoin would involve appealing to two demographics: current users of cryptocurrencies, and those who do not currently use cryptocurrencies but may be open to using them if convenient.

Current crypto users: The best way to ensure the support of those who already use cryptocurrencies is to convince them that terraCoin provides similar security guarantees and functionality as Bitcoin. This involves two major challenges: first, the proof of useful work algorithm must be formally proven to meet the requirements laid out in Section 4.1; and second, the terraCoin infrastructure itself must be shown to be as trustworthy as Bitcoin. The latter may be particularly difficult due to the fact terraCoin, unlike Bitcoin, is not decentralized, thanks to the inclusion of the terraCoin engine.

This brings up the question: Is this centralization necessary? The terraCoin engine is responsible for maintaining the current active problem, and for reporting solved problems back to researchers. This is necessary in order to ensure that the problems solved by terraCoin are truly climate related.

This could be addressed in a couple of ways. One option would be to accept this limitation, and instead focus on convincing the public of the trustworthiness of the terraCoin engine. For instance, we could make all terraCoin code open-source, and ensure that we are transparent about all design choices. The other option would be to overhaul the terraCoin design to a fully decentralized system. In order to do so, we would have to replace the terraCoin engine with another means of choosing the active problem. One way to do so, proposed by Coin.AI [13], is to allow successful miners to choose the next problem to be solved. This system, while elegant, would make it impossible to ensure that the problems being solved are climate related. Therefore, I believe that the best course of action for terraCoin is to take the first option and remain centralized.

The general public: One of the best ways to ensure the adoption of terraCoin may be to appeal to the general, non-crypto-using public, who are less likely to be concerned about the centralized nature of terraCoin. One way to appeal to a wider audience might be to embrace terraCoin's centralized nature by marketing it as trustworthy organization. This could go as far as convincing governmental organizations to accept terraCoin as payment for taxes. Furthermore, marketing for terraCoin should emphasize its environmentally-friendly nature (compared to traditional cryptocurrencies).

The ideal target audience for terraCoin will likely consist of environmentally-conscience people who have an interest in or need for cryptocurrencies.

9.3 terraCoin is still expensive

Even if terraCoin were to be adopted, it might not provide a perfect solution. terraCoin's proof of work is still energy intensive; even if that energy is used to perform useful computations, there is still the question of whether this energy expenditure is worthwhile. For instance, if terraCoin were to take the place of Bitcoin, and if it were responsible for 2 °C of warming, would it be worth it? At that point a huge number of machine learning problems would have been solved in addition to supporting the cryptocurrency, but the cost still seems enormously high. One might argue that these machine learning problems would have been solved in any case, but it is not obvious that this is true; terraCoin may result in problems being solved that would otherwise have been considered too computationally expensive. Additionally, the terraCoin proof of work may not be the most efficient means of solving these problems, since the hyperparameters of the model are determined by the input hash rather than being tuned by the scientist. Hyperparameter optimization is typically required in order to generate models with good performance [18], so these hash generated hyperparameters may lead to the training of sub-par models.

From an environmental perspective, traditional currencies should therefore still be preferred over terraCoin. However, in situations where a cryptocurrency may be wanted or needed–for instance, in the case of a weak or collapsing currency–terraCoin should be considered an environmentally-friendly alternative to Bitcoin.

9.4 The ideal case

Ideally, the adoption and widespread use of terraCoin would put pressure on Bitcoin and other cryptocurrencies to transition away from their current proofs of work. While there is a good amount of ongoing research into alternative consensus algorithms, Bitcoin, Ethereum, and many others are still employing energy-intensive proofs of work. In the case of Bitcoin, there is little to no evidence that a shift to a less energy-intensive consensus algorithm will be forthcoming. Unless they are forced to do so by market pressures, it seems unlikely that cryptocurrencies will transition away from traditional proofs of work in time to prevent their contributing significantly to warming. If terraCoin were shown to provide the same functionality and security as Bitcoin, it may inspire other currencies to adopt similar proofs of useful work. Furthermore, the popularity of an environmentally-friendly coin may drive greener blockchain innovation in general.

10 Conclusion

Blockchain-based cryptocurrencies are a significant, and rising, source of greenhouse gas emissions. Employing a proof of useful work could significantly reduce the amortized energy usage of these technologies. One such proof of useful work is Coin.AI, which requires the training of machine learning models. This concept could be applied to climate-related problems such as the parameterization of moist convection. The resulting proof of work performs useful computations for climate science.

terraCoin is a proposed cryptocurrency that provides similar security features as Bitcoin, but employs this proof of work for the climate in order to reduce the amortized energy usage of the cryptocurrency and contribute to the advancement of climate science. Preliminary work indicates that the terraCoin is technically feasible, and provides the necessary security guarantees. The widespread adoption of such a cryptocurrency could help mitigate the high environmental cost of blockchain-based cryptocurrencies.

References

[1] C. Mora, R. L. Rollins, K. Taladay, M. B. Kantar, M. K. Chock, M. Shimada, and E. C. Franklin, “Bitcoin emissions alone could push global warming above 2 c,” *Nature Climate Change*, vol. 8, no. 11, p. 931, 2018.

[2] S. Nakamoto *et al.*, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[3] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, “A blockchain-based smart grid: towards sustainable local energy markets,” *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 207–214, 2018.

[4] A. De Vries, “Bitcoin’s growing energy problem,” *Joule*, vol. 2, no. 5, pp. 801–805, 2018.

[5] “Bitcoin energy consumption index.”

[6] A. De Vries, “Bitcoin’s growing energy problem,” *Joule*, vol. 2, no. 5, pp. 801–805, 2018.

[7] C. Bendiksen, “Beware of lazy bitcoin research: Insights,” Aug 2019.

[8] A. de Vries, “Renewable energy will not solve bitcoin’s sustainability problem,” *Joule*, vol. 3, no. 4, pp. 893–898, 2019.

[9] S. King and S. Nadal, “Ppcoin: Peer-to-peer crypto-currency with proof-of-stake,” *self-published paper, August*, vol. 19, 2012.

[10] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, “Proofs of useful work.,” *IACR Cryptology ePrint Archive*, vol. 2017, p. 203, 2017.

[11] T. K. Sharma, “What are the alternative strategies for proof-of-work?,” Feb 1970.

[12] S. King, “Primecoin: Cryptocurrency with prime number proof-of-work,” *July 7th*, vol. 1, p. 6, 2013.

[13] A. Baldominos and Y. Saez, “Coin.ai: A proof-of-useful-work scheme for blockchain-based distributed deep learning,” *CoRR*, vol. abs/1903.09800, 2019.

[14] B. Academy, “Ethereum casper explained,” Dec 2019.

[15] P. A. O’Gorman and J. G. Dwyer, “Using machine learning to parameterize moist convection: Potential for modeling of climate, climate change, and extreme events,” *Journal of Advances in Modeling Earth Systems*, vol. 10, no. 10, pp. 2548–2563, 2018.

[16] D. Rolnick, P. L. Donti, L. H. Kaack, K. Kochanski, A. Lacoste, K. Sankaran, A. S. Ross, N. Milojevic-Dupont, N. Jaques, A. Waldman-Brown, *et al.*, “Tackling climate change with machine learning,” *arXiv preprint arXiv:1906.05433*, 2019.

[17] E. M. Stansifer, P. A. O'Gorman, and J. I. Holt, "Accurate computation of moist available potential energy with the munkres algorithm," *Quarterly Journal of the Royal Meteorological Society*, vol. 143, no. 702, pp. 288–292, 2017.

[18] C. Thornton, F. Hutter, H. H. Hoos, and K. Leyton-Brown, "Auto-weka: Combined selection and hyperparameter optimization of classification algorithms," in *Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 847–855, ACM, 2013.