A Wager-Based Blockchain Protocol for Tracking International Carbon Offset Credits

(Written in response to Option 2 of the Inaugural Blockchain Case Competition)

Ashley Herman, Rooshan Aslam
March 30, 2018

Overview

Often when people think of blockchain, cryptocurrency comes to mind. However, the idea of a blockchain can be applied to solve a wide variety of problems. Here, we will describe a blockchain based protocol to be used to keep track of the carbon offsets of different nations.

In our protocol, a decentralized ledger would keep track of carbon offset data. Each piece of data stored in the ledger will be an *offset tuple.* Carbon offset audits must occur multiple times within some specified timeframe, since a confidence bound will be used to determine whether the country has made their wager. Once a number of audits have been made, a confidence bound for each nation's carbon offset will be computed and the block will be added to the chain.

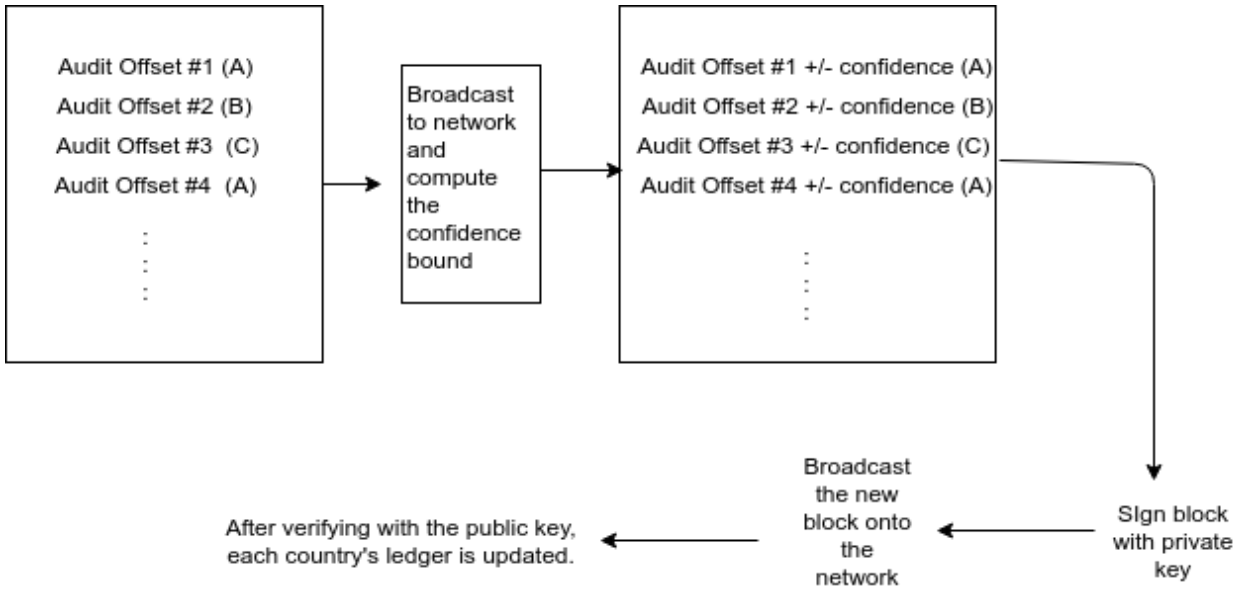
Incentive

The goal of each participating country will be to *lower* their overall carbon offsets. Although the original investment in the system is meant to be based on a sincere desire to improve the future outlook of the planet (as well as an understanding of the possible economic benefits of investing in clean energy [2]), each country will make a wager to enter the system. They will bet on what their carbon offset will be. They can only bet that their carbon offset will be lowered by some amount - they cannot wager that it will increase or remain stable. At the end of some agreed upon period of time (five years, for example), the total carbon offsets are computed and it is determined whether countries met, did not meet, or exceeded their goal. If they meet their goal, they will receive their money back. If they exceed their goal, they will stand to gain money because other countries will pay to buy their carbon offset credits and meet their bets.

Different auditors are more often than not going to come up with different values after evaluating what a particular nation's carbon offset should be. An offset tuple consists of two things: an estimate based on an external audit, and a confidence bound. Basically, to add a block to the blockchain, a certain number of audits must have taken place. Then, using this data, an overall confidence bound could be computed. Of course, the more audits on a particular country take place, the more accurate the confidence bound. Our system requires that a number of auditors must assess the carbon offset within a similar timeframe. However, audits

may be time-consuming and costly, and it is still assumed that relatively few audits are conducted and that the resulting confidence bounds are relatively low.

First, we broadcast the new block on the network to see who else has audited the country. Then, the confidence bound can be computed. The confidence interval is added to each audit value. To win the bet, the total carbon offset amount wagered by the nation must be within the confidence range at the time it is evaluated.



Security

Joining the blockchain network will be permission based. Countries cannot join unless they place a bet. Each nation must have a unique ID to enforce the rule that a nation can only join the blockchain once.

The ledger itself will be public, for viewing purposes only: countries will be able to know what other countries are betting. This is because environmental concerns are a public matter; citizens of any country may wish to know this information, even though they must not be able to alter it.

To keep the blockchain network secure, the following methods will be employed:

1) The security inherently comes from the concept of each country holding its own local copy of the blockchain. A decentralized system would mean no single country hosts all the available data, preventing data tampering from that single country. All new blocks must be verified using RSA encryption [3] (i.e. each new block will be verified by use of a public key before being added to the chain).
2) It is vital that countries do not add false data to the ledgers. *The system relies on the auditors reporting correct and unbiased information*. Auditors should be

neutral third parties. To help with the integrity of the offset data gathered, a limit will be placed on how many times an auditor may audit the same country within a year.

3) The system will use RSA encryption. When an auditor adds new data to their ledger, a 'digital signature' will automatically be generated using a private key and be stored along with the offset tuple. The data can then be verified using the public key for that country. Keys are generated using a cryptographic hash function, standard practice for RSA encryption.
4) Each block will contain a 'pointer' to the block that follows it. If the order of one transaction is changed, every block after it will be affected. (A similar system is used by bitcoin.) This is to preserve the order of transactions.

Conclusion

There can be no perfect answer to the problem of creating an international system to promote climate change. Our system has clear benefits and drawbacks.

Two main drawbacks of this protocol are that we assume auditors will enter correct data and the possibility that there may not be enough data to compute good confidence bounds.

We aimed to keep our system relatively simple, which we think of as an advantage. Following from the simplicity, this system would be feasible to implement for any country wanting to join the system. It also has the potential to promote international cooperation on environmental issues, since countries may set up deals with each other in order to make their wager.

References

[1] We watched this video to help us come up with ideas:
https://www.youtube.com/watch?v=bBC-nXj3Ng4

[2] Pollin, Robert, James Heintz, and Heidi Garrett-Peltier. "The Economic Benefits of Investing in Clean Energy: How the Economic Stimulus Program and New Legislation Can Boost U.S. Economic Growth and Employment"**.**
https://ideas.repec.org/p/uma/perips/economic_benefits.html. Using the USA as an example under the assumption that other developed countries could be similar.

[3] For an overview of RSA encryption please see
https://en.wikipedia.org/wiki/RSA_(cryptosystem).