Distributed Carbon Chain and Audit Protocol Proposal

Proposed by: Mihai Esanu, Peter Atrazhev, and Nathan Doraty

Blockchains have promise in applications over a wide spectrum of industries, such as financial services, logistical systems, asset tracking and even orbital defence. While the number of incredible decentralized technologies has increased, blockchains are still intrinsically limited in multiple ways. For one, blockchains suffer from the so called “oracle problem”, in which a blockchain ecosystem does not often have an easy, built in and flexible way to access external information. In order to provide on chain information, a third party that acts as a middleman which interacts with both the chain and the outside world is required. These middlemen are commonly known as “oracles”.

This problem is also present in any proposed system where there needs to be external auditors to verify specialised information such as Carbon audits. While you can issue a primary ERC 20 token that is publically traded to cover a business carbon credits, you still need to distribute and verify the integrity of each report produced by an auditor. The reputation of each information source can in turn also be represented by an ERC 20 token. Together the separate chains information can be combined to produce reports and used to possibly assess penalties by the province to policy violators.

By leveraging the power of the ethereum blockchain, through ERC 20 tokens, we can create a public ledger out of the box that will ensure public accountability toward carbon fund auditing and trading. Increases in token supply can be implemented through contract logic.

While centralized oracle solutions are already extant (such as the smartcontract.com oracle), decentralized oracle solutions are far more difficult to implement. The oracle problem is pertinent to the issue of carbon tracking, as, in many ways, the various statisticians and parties that are involved in carbon auditing can be modelled as individual oracles as well. As such, the chainlink architecture, which purports to established a decentralized oracle network, can be used as a base and adapted to the particular situation of carbon auditing.

The chainlink white paper specifies a system by which those wishing to extract data from off chain sources place postings for oracle contracts publicly on some off chain listing service. Operators of chainlink nodes (i.e. servers capable of scraping data and pushing it on to the ethereum chain) would then bid for particular contracts. The amount they bid would essentially amount to the amount of capital those nodes would be willing to lose should the provide inaccurate data or not be able to provide data at all in a timely fashion. Those putting contracts out would obviously be incentivised to accept a contract bid from those willing to offer the most

of an asset in collateral. This would be used in conjunction with a conventional reputation system. In our case nodes are auditors and the central contract issuing service would be the Province Enforcement for Neutral Information Services as seen in Figure 1.

In this case, a secondary currency (or ERC 20 token) that's representative of the reputation of each individual auditor would be used, and would be "staked" in the same way that chainlink is staked. This token is completely independent from the carbon credit tokens. A statistician that provides data for an audit can stake a particular amount of given "reputation" in a particular audit. The more reputation staked, the more their results of a particular party will be weighed in the overall audit. However, if a statistician reports results that are not in line with overall consensus, they can be punished through the deduction of the amount of "reputation" staked as well as having their overall results discarded. This deduction would not have to be done manually, but would rather occur automatically as part of the contract logic. This creates an incentive for all parties to behave in an honest fashion, and allows the efficient development of consensus through game theoretic principles.

A necessary modification to the chainlink system for this particular case would be a restriction on the trading of "reputation". The Government body would be the only body that can give a node tokens. Tokens will then only be gained by nodes through the staking process, removing the ability for nodes to arbitrarily transfer reputation tokens between each other.

What happens if the consensus achieved naturally among statisticians and auditing personnel is not necessarily reflective of objective reality? This is not necessarily an issue with a chainlink style oracle system, but rather with the process of scientific consensus as a whole. Repairing the fundamental issue of scientific consensus is outside the scope of this document. What we are trying to achieve is the reaching of scientific consensus through decentralized technology in a manner that is potentially more efficient than conventional academic methods (tedious research aggregation, the compilations of meta-analysis, and the need to qualitatively weigh the reputations of individual researchers and statisticians in the field of carbon auditing).

What about the problem of a proof of work blockchain that literally burns energy to track carbon emissions? This could create public push back against this system and will create bad public optics for the province and its stakeholders. The primary advantage of using the Ethereum platform to track both reputation and carbon offset credits is that ethereum will eventually move off of proof of work for consensus, and will eventually move to proof of steak, which will be a far more energy efficient. Thus creating a smaller carbon footprint and reducing overall carbon consumption by the system.

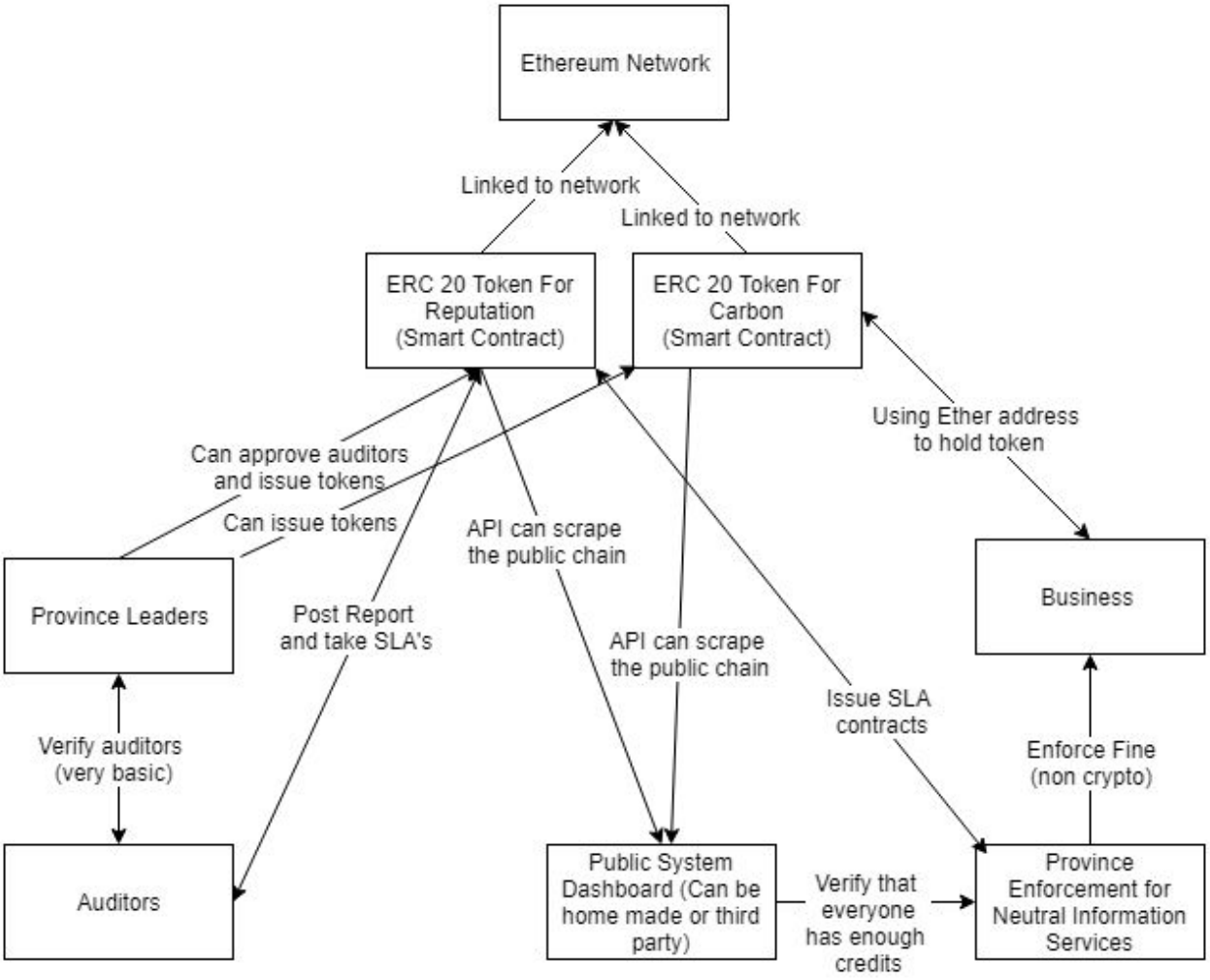

Figure 1: High Level Architecture

References

- https://link.smartcontract.com/whitepaper