Overview

Goal

We are trying to build a ledger which records the transactions of and available amounts of resources across the Island.

The benefits of these we are hoping to achieve are;

- Facilitating trade between communities by giving everyone visibility of who has and needs each resource, and providing an open, transparent and trustworthy record of transactions to prevent and resolve disputes.
- Giving the Government, Central Bank and NGOs a better understanding of the needs of different communities and the performance of the economy.
- Have a reliable record of infrastructure resources like roads and electricity networks so that governments know where repairs are needed, and travel can be better planned, helping trade, tourism etc.

Problems to Solve

- Network will operate across a very rural area with poor roads and electricity.
- Cultural and Language barriers
- Lack of understanding of technology
- Limited budget

Main Ideas

- Build our own Blockchain from scratch so that it is based on a ledger of resources instead of being a ledger of financial transactions with a resource ledger bolted on top.
- Use public and private Keys to validate the source of information is genuine.
- Make proof of work very easy to keep processing power and electricity requirements low.
- Communicate over radio given the lack of other infrastructure and long-distance communication needed.
- Use a mesh network to communicate across the network, so that a message from one node can reach every node without all nodes being able to communicate directly with every other node.

Implementation

- Every submission of information to the blockchain is signed using a private key to prove who it has come from.
- Who has each public key is public information and the creation of new public/private key pairing is carefully regulated (approval by current nodes?)
- Every time a community submits information to the blockchain about it's resources this creates a new block.
- In the case where there are 2 chains claiming to be genuine, instead of accepting the one that is hardest to create in terms of proof of work required we can look at the number of unique

private keys that have signed new blocks since the 2 chains last agreed to decide which chain to accept. This means that someone can't overwrite the chain by using a powerful computer unless they forge the private key signature which should be basically impossible. We can use alphabetical order of public keys as the tie breaker.

- Use open source python packages (probably PyCrypto and TCPiP) for the public/private key encryption and Mesh network.
- Network designed so that extra resources can be added to the network at a later date.

Things to think about

- How do we create a UI for the community to interface with, especially given language barriers, financial restraints, lack of computer skills and potentially even different counting systems.
- We are reliant on communities being honest about the resources they have.
- If each block only contains a submission from one node then can the chain hash and the private key signature be combined?