Overview

Goal

We are trying to build a ledger of records which can record information about landownership, infrastructure, resources and trade across the Island.

The versatility of our design means that there are many applications of our blockchain, but we will probably focus on one or two in our presentation.

The potential applications 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.
- Preventing Land Grabs, by having a clear record of ownership of land.
- 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.
- Recording weather in different parts of the island and using this information to improve weather forecasting, disaster relief 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.
- Hash each block using the private key of each node to prove that it came from them. This means that we only need to hash once instead of twice.
- Design the ‘Correct’ Chain selection algorithm so that it selects the chain with the most Unique Contributors, so the chain cannot be overloaded by a more powerful computer with a higher has rate. This enables us to have high security without having ‘proof of work’.
- 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 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.
- The hashing of blocks and the private signing that proofs the origin of a statement are one and the same.
- Use open source python packages (probably PyCrypto and TCPiP) for the public/private key encryption and Mesh network.
- Network designed so that extra records can be added to the network later.

Blocks accepted if:

- The hash was creating using the private key of the Node that the block came from. This can be checked by anyone knowing the public key of the Node.
- The hash of the previous block is included in the information that is being hashed

Hierarchy of the chain selection algorithm:

- No. of Unique Contributors since the divergent point
- Number of blocks since the last contribution from the first contributor after the divergent point
- First public key alphabetically, looking at the public key of the first contributor since the divergent point. (This can only occur when neither of the 2 first contributors since the divergent point have contributed before)

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.
- What protocol should we create for adding new nodes and adding new records?