Blockchain PSIG Call Notes

*18 June 2020*

# Attendees

* Mike
* Rob
* Ian
* Bobbin
* Robert Rencher

## Apologies

* Neil Aeschliman

# Agenda

* LETS RFP

# Meeting Notes

## LETS RFP

### IOTA Exemplar application / Spec: Topologies

#### List-like Message Topology

[this implies an ability to access individual txns in a stream, and the kind of access in the above is ‘linear’ as distinct from polynomial; relates to how easy it is to find a given message in your branch]

Do we want to enforce any of this e.g. saying what kind of randomness is there?

No. Leave this to the application, so the submission needs to allow for these possibilities]

#### Discussion

Discussion: do we care about this implementation detail?

May want a signature for just one transaction – different architecture. Txn level v stream level signature are not the same thing. Do we want stream-level signature as well?)

#### What this seems to mean:

Be able to store references to an overall stream so you can access it from some point.

Spec: allow for various kinds of participation by participants. For the list-like one, we expect discoverability from any message in the stream.

Clarity: In Blockchain every node had all the txns. In Ethereum not every node needs to store all of the chain. In this requirement, you have to allow for a way of discovery, if you are not storing everything locally, whereby you can discover everything you need across the distribution.

This would also apply to Tangle v Permanodes. Should not need to store all the information in your local iteration of the Tangle, to get to al the message in the stream. That would not be in the RFC or the Submission, but the overall requirement might be.

#### How to find info:

2 ways:

1. Walking the stream
2. Random access

For (2) you might need some external map for everything in the stream and where they are? Or not. Need to be able to do comparisons from what you have without needing a map. Where is the information? Implicit in how the data store was structured. But there is no data store of this.

**Example:** if something was sequentially ordered I don’t need the map, e.g. I can dive into the middle and see if I picked up the ones I needed. Rinse and repeat until I get to the one I needed. Do not need to have the whole sequence if you know it is sequentially ordered. Just need to know the functional form of the structure [of the storage – but it is not, in the case of DLT!]

If you were to also require a map then that would need to be given as a requirement.

What we think they meant: the ability to do that walk. As long as you have the 2 txn that allow you to do that walk, we don’t say how you have to do that, but the proposal needs to.

Q: This relates to signature or encryption or both?

In this section, it refers to signature.

Could also apply this thinking to encryption.

Not the same thing.

Recall this is layered (like OSI) so the relations described here are not related to the relations in the blockchain or a Tangle.

### Packets

Packets in the IOTA Exemplar: you have the signature and the packet that lets you dip into the message stream, then we think the RFP is saying you have to be able to go back and get the relevant messages in the message stream. For this you need unlimited access to the Tangle or Blockchain (e.g. a Permanode).

We should mention this in the narrative somewhere e.g. in the bit about the example application. And a diagram.

Also show the layers – show the Tangle Blockchain and the relation between this and the layer that is the LETS conformant application.