Blockchain PSIG Call Notes

*26 August 2021*

# Attendees

* Mike
* Rob
* Ian
* Bobbin

# Agenda

* Updates
  + LETS RFP Response expectations
* Smart Contracts RFI

# Meeting Notes

## Updates

### LETS RFP

#### IOTA Streams spec

New version still coming out.

They will expand the spongos details and segregate the 2 concerns.

Meanwhile ''Documentation' = user documentation? Unclear. Good guidelines. Does not cover types of spec. Aims at end users, who are developers, and may well be implementation neutral to some extent.

BT: Similar to the distinction between Architecture v Implementation?

MB: Requirements v Implementation

Early phases (pre-alpha, alpha) = 'hybrid' eng spec (i.e. too early to segregate std v implementation detail);

Later: Requirements spec: based on the context of the user and their desires.

Req Spec = CIM i.e. independent of the design of the solution.

What we call a 'Protocol' = standard is a kind of requirements spec.

End user language is that of a developer i.e. design independent but technical.

#### What we await:

The Streams 'Framework' (protocol).

Also the Streams 'Framework' defines how to develop a local 'Protocol' with which to develop one or more local applications.

The IOTA Channels App is one such app.

#### Timings:

Streams spec will not be available in time for MB to write up the RFP Response specification.

Also re-writing spongos itself.

Still unclear what sub-set f the Keccak standard they are using and in what they they are using it.

Need a one-page write-up on what Spongos is with a diagram.

See previous QM on the Keccak Sponge standard (published document).

Need to do the same 'Spongos' thing (and find out if that is written from the ground up by IOTA, or adapted from some third party library, or some combination of the two.

#### Comments:

Sounds like a work in progress.

Not ready for a formal 'Release' version; questionable if this is beyond Alpha at this time.

Meanwhile the IOTA Tangle consensus mechanism is being re-written. This may impact Channels but may have an effect on the Streams protocol.

At what point can changes be handled under the OMG FTF/RTF process?

* Has to be non breaking changes

Keccak Standard – nice slides:

<https://csrc.nist.gov/csrc/media/projects/hash-functions/documents/keccak-slides-at-nist.pdf>

We don't know what amount of this they use e.g. the different Greeks. And also HOW they are using it

For example it seems like they use it to squeeze subsequent messages content, which is innovative and useful. They also seem to imply some reversibility, which (if MB read it right) can't be done in Keccak if you use all of the Greeks, specifically the one called *iota*. That makes it not reversible.

MB to encourage the Steams person who is 're-writing' the Spongos (the code or just the documentation) to address these questions i.e.

* What parts of features of the Keccak specification they are using?
* How they are using those parts
  + E.g. are they deriving a hash code or using it to provide a reversable in / out feature, and how is that intended to be used

Like Mux / demux or digital to analog conversion.

Single Input Multiple data versus Multiple input / single data

See: SIMD v MIMD

### LETS Proposals

BT: delay by one quarter at a time and peg a version when this is just good enough.

MB: delay by 2 quarters and hope

This only works because no-one else is submitting a response to that RFP.

RN: have IOTA got it together to the point where they are ready to submit something as e.g. an RFP or an RFC? Are there data points?

Yes there are data points; = no, they have not.

That would lead us towards extending the RFP response by at least 2 quarters.

**Consensus:** Put off by 2 quarters and submit when we are ready.

Alex Renz is still on the IOTA Advisory Board. Invite him to speak

#### Why no other LETS RFP responses?

Likely partly because most DLTs have Smart Contracts, so there was less of a need for streamed messaging.

## Smart Contracts RFI

Document: Smart Contracts RFI Draft4.doc

Some of the questions arising above on Steams can lead to possible questions here

A contract is a fixed thing; everything else leads to that. Meanwhile supply chains (and IoT) are more needful of something like Streams, where they morphed. See also the 'advanced' implementation we included in the RFP as additional stuff.

Is it the case that you can implement streams in smart contracts but you cant implement smart contracts in streams. That is, Streams is a broader architecture. And as such, it addresses many of the questions that many SCs set out to address.

A stream could be the set of messages interchanged in a very long Smart Contract.

i.e. SC may have:

* A very basic process e.g. post something other than crypto funds to a DLT ledger
* A complex process workflow
  + Where:
    - The Contract defines the exchange of commitments
    - The Process model defines the events and actiosn within each side of the contract
    - The Streams messages may implement the exchanges of information needed in each of these contexts defined by a process point.