Blockchain PSIG Call Notes

*7 November 2019*

# Attendees

* Mike Bennett
* Nelson
* Nick Stavros
* Simon McQueen
* Ian Stavros

# Agenda

* Updates
* Continue the conversation from last week…
* The LETS RFP

# Meeting Notes

## Updates

Next week – Anne Smith from IOTA will be able to present on IOTA work with Jaguar Land Rover etc.

Nelson will be able to show platooning demo at Long Beach? Not yet ready. In order to show the MAM version, needs some things worked out. Will show at the Braunhofer Group – available on line

<https://www.youtube.com/watch?v=GLkfJwxLhcg>

Also Nelson is eating fresh kale grown by the IOTA Autonomous Gardner.

IOTA have some PoCs on using MAM for supply chain integration.

LETS RFP – some comments etc. from Nelson and Mike on this – for today’s meeting.

## From Last Week

At the end we were talking about the RFP and the different profiles.

### Profiles

By ‘profile’ here we mean coherent sets of conformance criteria that may be included in any response to the RFP.

The current draft material does not have profiles. We would parse these later into profiles. For example, if using a DAG I might have a different profile of requirements to what I might have with a Blockchain, and likewise if we had or did not have Smart Contracts.

Then different submissions might reflect different profile level.

### RFP

#### MB Feedback on RFP

There appears to be material at several different levels. For example, part of the material describes potential improvements to how ‘postings’ (transactions in one sense) are made to a Block of Tangle. At the same time, many of the proposed features would belong to a messaging level such as MAM (other DLTs don’t necessarily have this layering or distinctions).

That is, what Nick has written sets out what may be a powerful new vision for how things may be done on blockchains, such that information posted to a block or other immutable resource may be liked to other such material. IOTA does this with the MAM messaging layer which is a higher layer in the IOTA architecture stack.

The layering in IOTA is something like this (using bullet levels as layers):

* The Tangle (IOTA Node RFC – How to talk to the Tangle)
  + Layer 2 – an enabling layer for the provision of additional protocols
    - Flash Channels
    - Masked Authenticated Messaging (MAM)
      * Possible 3rd party extensions to MAM; implementations

That is, MAM and Flash Channels are identified as ‘Layer 2 Protocols’ by IOTA, along with the ability for people to create their own protocols on the same basis.

Think of it like

* IP at the bottom level (analogous to posting to a block or Tangle);
  + TCP and UDP on top of that
    - HTTP, FTP etc.
    - The ability for anyone to create a protocol that works at this same level

For the same reason, MAM can be used without necessarily being posted to the Tangle, much like you could create a TCP/IP message and use pigeons as the transport layer (different layers to the above analogy but th same principle). So you can create a linked message stream in MAM and put it on an XML message stream or something instead of on the Tangle; or even post to another DLT e.g. Ethereum, at least in principle.

Some of the features proposed are similar to work done within the IOTA community as potential extensions to MAM and not as part of MAM itself. This could be nicely reflected in the proposed Profiles, extending the standard beyond what MAM provides.

However, we first need to disentangle the various features in this draft material.

#### Nelson feedback:

2 levels of encryption:

* Encryption on the network
* The encryption of the transactions themselves

The push for private networks tries to overcome this by combining the two uses of encryption.

We need to talk about multi-level security (MLS). So far, no MLS system has been approved by the authorities.

DDS is a technology looked at by NSA for driving MLS. One of the only such.

Otherwise 12 different security departments would need 12 different networks. Leads to fragmentation. Also workarounds with their own risk.

In the LETs, 2 kinds of encryption:

* For the network itself
* For the stream

MB: In terms of scoping, LETS would only cover the latter. Each DLT already has its encryption.

### Overall Vision

N: The Google Doc has a great vision, across all layers. From this vision can we create the overall roadmap and vision and take out pieces of it so that the LETS standard becomes one component of the overall vision.

We can take out the material in Section 6 and make it a separate document setting out the ideal future Blockchain roadmap.

Then LETS RFP would be extracted from that, for this layer. IOTA MAM is one component, like a transport layer. Identification of the profiles is a layer on top of that.

### Profiles

* Profile for the spec itself (LETS), and potential responses incl. MAM
* Profiles in the broader DLT vision

We can take what is in this Google Doc and put it in the Blockchain wiki.

MB: Put it in its own Google Doc, as a Roadmap, separate from the RFP.

Q: Whether to make this public or private?

### IOTA and Roadmap

See <https://blog.iota.org/eli9-the-qubic-computation-model-623417f94777>

Shows the IOTA style and approach. This is what they are expecting in terms of the level of understanding.

ELI9 = Explain it like I’m 9.

We need to be able to communicate across intergenerational schemes for how we think about things.

## Vision

MB: Is this a future vision for DLTs What about now? e.g. LETS / Level 3 protocol (like MAM) on a Layer 2 protocol, with DLT posting transactions at Level 1. If future applications use all these layers, then it becomes possible to have powerful interchange of information that is linked and is all posted to the / a bloc or Tangle.

Meanwhile we need to address what there already is, not only the ideal future.

NS: there were issues earlier with DDS where you needed more information so e.g. you can discover things based on topics. So the new doc is analogous to what was needed in DDS.

Example: Locations have X and Y. Then in a new version we add Z. Can’t break down the existing stuff to add this – we would rather have some standard for X and Y, such that when you add Z it is seamless.

MB asks Nick to clarify what is DDS, as not everyone on the call is familiar with what this is.

### DDS

#### DDS History

Originally created for US Navy. Is a real time publish subscribe, for command and control on a ship. Events come in. Need to handle 200k events per second. Nothing handled that. Real time pub sub paradigm comparable to ZeroMQ.

Near real time, given latency in the network. Which is minimal in DDS.

RTI developed this for the US Navy. This was commercial rather than a standard at that time.

#### Topics

DDS: has ‘Topics’

* You publish to a Topic
* You can subscribe to a topic.

Is a Many to Many – one Pub to many subscribers, one subscriber subscribes to many publishers.

QoS parameters built in to DDS. Suppose I have 4 sensors. 737 Max – 2 sensors on per wing. Control system can listen to one or the other. A DDS sensor listens to both. Typically odd number. Has fail-over.

MB: If so, DDS comparable with what August Systems use in fire and gas / ESD systems, using technology originally from the Space Shuttle. This has triplicated redundancy of inputs loops, processors and output loops. This used simple voting on outputs.

NS clarifies:

Say I subscribe to a Topic, e.g. 3 events a second. Publisher software may still produce 1k events a second. So the thin layer on my side (the originator) will only put those 3 events per second out on the network. Another client wants 10 events a second – the originator puts out 10 events a sec to Nelson and 3 events a second to Mike.

Also has filtering. E.g. for geographic region. May be interested in when an airplane comes into a given user’s airspace. Then start getting information on that.

Filter may be one of many shapes. Also time based. So there are ‘series’:

* Geographic
* Time based
* A third one

The entities play together using an API that lets them write and read the info, and a set of QoS parameters.

### So, what is DDS as a standard?

A ‘Topic’ has 3 things:

* Name (namespace)
* Definition of Structure (lets subscriber unpack the info)
  + Simple scalar types
  + Complex records
  + Variants
* QoS
  + The same QoS that the network has
  + Networks have 3 QoS parameters in the network protocol
  + DDS adds 27 of these, and in other implementations there are up to 50 of these.

Use IDL to unpack that structure, using the QoS parameters.

Can them map to a language e.g. IDL to C, C++ etc.

There are standards for this mapping.

### What is the DDS Standard?

DDS is a family of standards:

* API standard
  + For code portability
* Materialization method (how to put the data on the wire e.g. big endian, Int, 4 bytes)
  + Ternary would go here
  + Protobuf does some of this
* XTypes
  + For extensibility – see above. E.g. (X, Y) to (X, Y, Z), or changes in precision
* Web-enabled DDS
  + Goes to JSON
  + From browser
* DDS Security (built in encryption for messages and their payload)
  + This is where we identified the need to have 2 levels of encryption, as noted for LETS above
* Mappings standard
  + To each language e.g. C, C++, Java etc.
* Narrower version for small implementations
  + E.g. for IoT, Raspberry Pi

So DDS is something that EEE may be an implementation of.

For LETS, Nick is using this as an analog in the notes above.

DDS is about the messaging. Includes ZeroMQ, others.

Can look at how IOTA work fits into or extends DDS and where it doesn’t.

DLT communities tend to look for what is available open source. E.g. for finding messaging queue systems like ZMQ and its predecessors. There were no OS solutions for DDS. Now there are. E.g. OCI, PrismTech (old versions released as open source) and others. RTI has a community licensing agreement and a research development license agreement whereby you can use your software with anyone in the community. Can decide to use RTI, write a one-off payment and anyone can use it. Likewise for OCI.

OCI – aims to be compliant with the DDS Standards set e.g. DDS Security, CRM and the rest as needed.

## Way Forward:

Move the 6.n stuff into a new Google Doc.

Split into layers more explicitly.

Look at where e.g. IOTA ZMQ, EEE etc. fit in with the DDS standards.

This would be a clear benefit to IOTA, which is well placed to work on this basis.