Blockchain PSIG Call notes

*5 March 2020*

# Attendees

* Robert Nehmer
* Ian Stavros
* Robert Stavros
* Rencher, Robert J
* Michael Bennett

## Apologies

* Char Wales

# Meeting Notes

## Actions from last week

None

## RFI Updates

No formal submissions

### Jackrabbit

The DIDO CLI was the submission

CW by email: needs to be re-framed and / or submitted as a submission.

Jackrabbit will try to do this.

### IOTA

MB to do a response

Fits under broader remit o the RFI to include integration generally – for which IOTA has a strong story. Also one of the things they have in flight does have a story for cross-Blockchain interaction.

MB to write up and submit the submission.

### GS1 (check!)

Waiting on resolution of some IP related issues.

### Any others?

Boeing team has gone quiet – not anticipating a response at this point.

## Meeting Planning on RFI

Plan was in 2 parts:

* Discuss formal RFI responses at MARS (Monday)
  + (possible overflow into BC-PSIG session) (Wednesday)
* At BC-PSIG, discussed and scope out potential RFPs for the various kinds of interoperability. (Wednesday

The Monday part should be quite short.

* Jackrabbit (CLI)
* IOTA
* Maybe GS1

General disposition (Wednesday)

Other sources of information on DLT interoperability

* Blocknet
* Monetha
* GS1
* Etc.

(MB to find the list)

### What we have going in

* Formal responses
* Details of previous presentations
* More general research

### What we need going out

A set of potential RFPs as scope descriptions.

### Possible scopes

For interoperability across blockchain / DLTs

* Semantic interoperability
* Cross-Blockchain integration (participating in more than one DLT)
* Message / protocol etc. interoperability
* Identification / identifiers
* Others?

For use of DLT in general integration / interoperability

* ?

Of these, what of them could result in a possible standard?

#### Semantic interoperability

What would a standard be?

* Common ontology
* Some common approach to ontology (cf. SBRM)
* Other?

Examples: the one we saw with a common approach to the exchange of commitments (comparable with REA)

For the exchange of commitments, was it because there was an exchange of barcodes (GS1). Having these registered in a standardized way was what enabled the exchange of information between the various blockchains.

This is also why the communities of interest are import. Make a standard so that people in different places can talk to each other. In this example, a standard way to read the baggage. Driven by Denver Airport.

Common identifier versus common semantics.

Identifiers and semantics go hand in hand in that there is a kind of thing and there is an identifier for instances of that kind of thing.

So the GS1 presentation was focused on the identification BUT has implications for common semantics, in order to be able to use identifiers more broadly (define what you identify)

This is why FIGI was important, and UUIDs are also important.

(So the GS1 approach can be applied more broadly if we have a good identifier)

SO they are currently using IDs that are specific to the specific Blockchain. There is no standardization for e.g. how you store the information so it can be queried. Some are encrypted, some are a hash of the thing. Might take e.g. the date, time and some other key fields to make up the hash value. We can’t standardize how they do the hash value. What we can standardize is how you query the hash e.g. be able to identify which blockchain it came from, no matter how they do it locally. Be able to encrypt who they are (identify) and so on.

There should be some way to be able to identify, especial in Supply Chain, what the thing is. Needs to be associated.

Can you in fact look at a hash and discern anything about it? Isn’t it a dumb string of characters.

Externally it is a dumb set of characters but internally there is information so you need to unhash it to do what Nick is describing above.

MB thinks it is not possible to do this given the fundamental nature f what a hash is.

NS: there are certain fields and there are certain fields you can decrypt.

MB: Surely a hash can only be decrypted by the party that has the corresponding key.

NS the algo that’s used to mine a coin requires something like a given number of matches to see if it is valid.

If there were to be a standard to do the above, if it turns out to be possible, then would it even be possible for every Blockchain ecosystem do make the changes needed to implement this.

**Outcome:** this is one of the possible standards ideas we can look at in Reston as RFPs.

More generally, under Identifiers and Semantics

* Is it possible to have some standard way of tying IDs to semantics?
* Is it possible and / or desirable to have a common ontology?
* Is it possible to have a standard approach to semantics
* Nick’s has idea above

These are candidates for our Reston structured conversation on what might be possible RFPs.

#### Common ontology

In terms of a common ontology…

* Ontology of things that might be identified by IDs (domain subject matter)
* Ontology of DLT concepts

That latter is what was presented at the DIDO CLI presentation. This articulated 2 things:

* Common concepts across al or most DLT ecosystems
* Concepts for things that are not present in DLT / DIDO ecosystems but would be beneficial if they were

These are typically 2 kinds of standard

* The ways people should do things
* Something that covers all the ways that people do do things

MB: One RFP should not embody both kinds of standard but there is no reason not to do RFPs for each of these kinds of standard.

**Summary:** an ontology of DLT concepts could be a good enabler for interoperability.

So, the existence of an ontology of common concepts for DLT itself, will enable those kinds of DLT interoperability thing that have a foot in each of 2 or more DLt ecosystems. Otherwise, without standardizing on the common meaning of those DLT concepts, whatever each of those things does, can’t be replicated to other DLTs, and therefore is not a standard, just a product.

So they basically point to point mapping, just like P2P mapping in financial or other data, you have 2 issues:

* The non scalability (non linear) for adding new sources
* The non auditability of the mappings made

#### Cross-Blockchain integration (participating in more than one DLT)

Requires some common model, ideally an ontology (concept model) for the problem domain which is DLT / Blockchain. See previous heading.

Without that, there is not a lot we can think or to standardize for this kind of product?

BM asserts that without some common model (even if it were just a data model) there is nothing that would be a standard, as distinct from a product.

**Consensus:** all agree.

**Ambition** is to create a concept model that is ontological (DL, (OWL?) or similar).

(MB puts OWL in extra scare brackets because it is usually an implementation language so any concept model expressed in OWL tends to be treated as such, to the detriment of the concept model)

It is important to frame a concept model here.

MB usually a concept ontology would have NO datatype properties, since these represent computational commitments. HOWEVER anything that exists natively as computational stuff only, would have a datatype property.

NS: Uses the notion of a ‘type’ e.g. something that is textual, a number, a scalar etc., integer scalar versus string scalar.

Modeling tools are poor at capturing the conceptual nature of what will become a datatype.

So we are in a good position to understand what’s needed to do an ontology for CLI. The CLI itself is conceptual including identifying the nature of what MB calls ‘information kinds’. Then when you go to implement a logical design you make the relevant computational implementation decisions.

MB: the art of ontology is the art of not designing something.

#### Message / protocol etc. interoperability

Is there something here? See e.g. some of the IOTA things that will ne in the RFI response might have something here.

Should that be one (or more) to discuss.

## Summary

We have one v strong candidate for an RFP

We have possible other RFPs

We made good use of this call in fleshing out 2 possible RFPs already.

The Monday discussion could be quite short

* Slides from MB on IOTA
* Slides of NS on DIDO CLI (already covering in another session)
* General deck to hold that together (MB)
* Plus others if seen
* Plus a summary of the GS1 ID v Semantics conversation (today)

The Wednesday session

List the possible RFPs

* Continue on that on these calls
* 2 more before the meeting

### Outcome

May not be government people attending at Reston

People need to plan on participating virtually

MB needs to be there if we have a virtual arrangement

If we do the whole thing virtually then MB does not need to go there, otherwise I do.

Use the next 2 calls to continue this conversation.

## AoB

No.