Blockchain PSIG Call Notes

*24 Feb 2022*

# Attendees

* Robert Rencher
* Mike Bennett
* Nick Stavros
* Ian Stavros
* Bobbin Teegarden

**Apologies:** Rob Nehmer

# Agenda

* Smart Contracts RFI

# Meeting Notes

Pause for thought for the people of Ukraine.

## Smart Contracts RFI

Last spoke on that on Jan 27.

Scope (from Dec QM)

"Pattern Language for Smart Contracts"

We firmed up the scope last time.

We talked about some things that are really about the 'Blockchain' itself i.e. Level 1.

Firm our (internal) vocabulary:

* Level 1: the Distributed Ledger (Blockchain or DAG etc. DLT)
* Level 2: Smart Contracts

i.e. anything in this RFI does not need to cover questions about DLTs themselves but about Smart Contracts and how these are to be generated.

So the scope seems to be a lot clearer now.

MB summarizes where we got to so far and shows the (empty) RFI document.

## Comments

How shall we present the questions?

e.g. in a lot of technical writing things are not numbered but it will help is the questions are numbered.

**Proposal:** Number questions as an ordered list

**Consensus:** Yes, questions are numbered

(not 1.2.3 styles?)

If we want to categorize questions

#### Choices

Option 1: Single numbered list

### Clause

#### Sub Clause

Q1

Q2

#### Sub Clause

Q3

Q4

Option 2: Sub-clause structuring

### Clause

#### Sub Clause 1

Q1.1

Q1.2

#### Sub Clause 2

Q2.1

Q2.2

This second seems to be what Nick is proposing

If we have questions that are more complex, these can become sub-clauses.

Do we have any strong feelings either way?

**Consensus:** No strong feelings

MB as editor will decide; probably go for Option 1.

**Consensus:** Yes

## Questions Styling

#### Separate points:

Put all the explanations outside of the questions.

Example (from Governance Points)

**Atomic** - A Governance Statement only addresses a single topic. Indicators of non-atomic guidance are use of highly complex sentences, multiple sentences or conjunctions such as and, or, etc.

**Succinct** - A Governance Statement are short and to the point. The definition of terms or caveats that explain when a statement is applicable are not acceptable as part of the Governance Statement. Indicators of non-succinct statements are the use of words or expressions such as: consider, when possible, if, etc.

**Absolute** - A Governance Statement is evaluatable with one or more non-subjective questions. Indicators of non-absolute statements are those which are subject to the interpretation of the evaluator. For example, “All menus must be user-friendly“. No one produces menu's that they feel are user hostile.

**Definitive** - A Governance Statement is precisely worded and explicit in nature. Their words, terms and expressions need to be defined and not subject to interpretation. Indicators of non-definitive guidance are words that are not intuitively obvious to an outside reader. Some words that are examples of non-explicit words are: object, service and function.

#### Usage

So for questions the same principles apply.

What this means:

We have sub-clauses with introductory explanation on that topic.

Then we have the list of questions for that sub clause.

Then it would be e.g. 2.3.1 'questions about xyz'

- intro

Then a list of numbered questions.

#### Disposition

All under 2.2 (Detail)

OR add a 2.3 for Questions.

Then use 2.2. for general info

Then 2.3 Questions section structured as Nick proposes

Then 2.1 is just a high level abstracts.

- seems OK

### Questions

Open discussion of possible questions to have in the RFI.

#### Definitions:

Proposal:

And a question could be if the responders have a different definition that we should consider

Of what?

We would provide definitions for 'Smart Contract'

Then:

Use our definitions when answering any given questions and / or provide a different definition.

Definitions are in A.2

Intro material (in 2.2) we explain and expand on what we mean by those things and what the general idea, scope of potential RFP is. Also our own research and understanding on these things.

Then in opening para of Questions (new 2.3) we state what Nick posted above.

Not really a question but a qualification to be applied to ALL questions.

#### General Questions

In the general context of having something to be able to generate SC code.

Think about different stakeholders who may have different questions they could answer for us?

* Smart Contract developer
* Business End users (supply chain etc.; NFTs and economic exchanges etc.)
* Entrepreneurs / new business opportunities developers

### Proposed Questions

Q: Is there a taxonomy that the responders find useful?

* Existing taxonomy? Or other industry standard?
* Propose their own as an answer

Allow for both.

So give space in the answer.

Allows us a good insight into what their thinking is.

Q: What languages do you use to define Smart Contracts?

Good.

Q: will the advent of quantum computing alter how smart contracts are developed?

Allow space for a short answer

Sub-Q And if so how?

- allow space for them to expand on that.

Q: How important are these Non-Functional Requirements for Smart Contracts:

* Portability
* Reliability
* Maintainability
* Securability
* Manageability
* Usability
* Performance
* Interoperability
* Elasticity
* Scalability

Some of these have sub-sections in the source material.

Source:

<https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:2_nonfunc>

This lets us get input into stuff we've already written (in this case, the DIDO RA).

- that’s not a bad thing

#### Options:

We could get them to

* Yes or no
* Scale of 1 – 10
* 1 - 5
* Other

The Scale of 1 – 10 seems the most useful. Do this.

Also helps us figure out where gaps might be.

See also 'Attitude and Satisfaction' metrics:

[https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4\_req:2\_nonfunc:30\_usability:satisfaction&s[]=scale](https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:2_nonfunc:30_usability:satisfaction&s%5b%5d=scale)

**Outcome:**

NS proposes that we should qualify the numbers we use (rather than using 1 – 10 where people generally have a common understanding).

**Consensus** is we need to do a table with the intended meanings of the numbers, and use 1 – 5.

Q: How do you handle off-blockchain data (i.e., Oracles)?

Possible question: do we need to distinguish kinds of oracles? Are there 2 kinds e.g. an agreed 3rd party source (per the above question) versus an oracle that is part of the proposed solution.

Q: What do you understand by 'oracle'

Q: Do you create SCs that include their own oracles?

Q: Do you create SCs that call out to some established 3rd party data source as an oracle

Q: Do you create SCs in which the feed of data from some physical instrument is treated as an oracle?

(then the preceding question is asked where the answers to the 2nd oracle question above is Yes).

#### THEN for 3rd party oracles

This is really fundamental to SCs. It defines some of the things you can't do that you can do in other architectures, and some of the ways around these.

This needs some sub questions:

Sub-Q: We are interested to know the method that you follow to decide on these things.

That is, what is there about some data or requirement etc. that leads you to put it on an oracle versus on the chain.

Q: Do you have a decision process for this

Q: Is that decision process repeatable?

Q: What is there that leads you to know you have to follow that decision process?

e.g is it size of data, speed, accessibility of some datum to different participants, something else, all those?

(so far we mostly assumed it's size but we want to flesh out if there are different factors)

**Consensus:** Yes, we do need to get them to expand on this.

**Example:** Suppose I have some data that we need to get from an exchange, what additional metadata is used to describe this kind of ancillary data, such that I could go back in a few months and recreate the same data. Need repeatability, for accountability.

In conventional contracts we always define the parameters (ancillary data) for variables that have to be read. This same idea needs to be considered for smart contracts.

Oracles 'we need data from the outside' – needs more specific thought, that some DLT devs might miss.

Also these kinds of gaps can present attack surfaces for a hack.

We feel that ancillary data like this has often been ignored.

Would like to see some insights, from those who have them, in the answers.

#### Attack Surfaces

Do we need to ask questions more generally about potential attack surfaces?

(develop this later)

Q: What do you use to develop and test smart contracts before development?

Given people are developing the SCs, how do we know what level of rigor there has been in an SC before they push it.

So 'what do you use'

* Tools
* Method
* Kinds of test (unit test v others)
* Agile?

Use the DIDO per link below and do a 1 – 5 Question on each of those items:

<https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.g_testing:start>

**Consensus**: sounds good

Q: How do these tests account for dependencies (see next section)

#### Design and test

Q: How have your designed smart contracts to handle DDOS attacks?

(question for design and also for test)

General section on design considerations, resilience, continuity etc.

See GBA on Sustainability (stability / maintainability / continuity)

Also network complexity.

Ask some qualifying questions about their SC:

* What DLT
* What kind of DLT
* Permission v permissionless
* PoW v PoS
* Etc

(to qualify what the answers to the rest of the questions imply)

### Similarly:

Security Audits.

Do a Q on that

Ask that before the more general testing questions

### Dependencies

Q: How do you determine what the dependencies are in a massively distributed system?

(we suspect that at present this doesn't arise because the SCs are quite simple)

Frame the question in such a way as to filter out some of those.

### Times / Longevity

A transaction may live on for years and the underlying technology may change

Q: How does SC deal with longevity of contractual commitments versus that of the SC code?

### More Questions

Q: How important is throughput?

Q: What is the definition of realtime?

- need to refine that one – in what context?

Q: Do you have a concept of Settlement: <https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.2_views:2_tech_views:defilayers>

Expand on this on our next call e.g. timing and other considerations

Q: What Consensus do you use?

See:

<https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.k_consensus:start>

### General Questiona

(**general note:** the kinds of things we needed to know in the previous RFI may be the kinds of things that determine the NFR that generated SC code need to take into account – e.g. oracles, statefulness, typing)

## Next Steps

Put the questions we have so far into the document.

Next call 10 March on this topic.

Next week 3 March: DIDO

(or CBDC Responses to the US Fed questions, that the CBDC WG are working on)

How would we as Blockchain PSIG contribute to that? Valid to discuss that on the 3 March call.

3rd potential topic for next week.

Can also be part of a contribution to the Civic OCAF. Specific: is Blockchain part of OCAF?

So we have 3 potential topics for next week so we will decide on the topic on the day. We will NOT attempt to do all 3 topics.

If we do pick DIDO, it will be on Data In Motion v Data at Rest (as previously identified) and potentially identify how someone can help.

## AoB

See NS article on the coal mine.