Blockchain PSIG Call Notes

*27 Jan 2022*

# Attendees

* Mike Bennett
* Rob Nehmer
* Robert Rencher
* Nick Stavros
* Ian Stavros
* Lars Toomre
* Bobbin Teegarden

# Agenda

* Quarterly Meeting Plans
* Smart Contracts RFI Take Two
  + Code Generation

# Meeting Notes

## Quarterly Meeting Plans (day and time)

Agenda itself we can figure out later, need day and time today

Other inputs: see GioDTF (with FDTF)

### GovDTF Plans:

Draft agenda:

* CBDCs
* Coffee
* Money concepts and VCoI
* Lunch
* Statistics WG
* Secure voting
* Potentially something from GBA

### Current proposal

BC-PSIG – meet Tuesday afternoon (half day)

* Guidelines spruce up and post / see if good to go or needs more work

AI PTF etc. Bobbin propose that BC-PSIG need only meet on the Monday

- normally do Monday jointly with MARS

- usually use Tuesday afternoon

For example Monday morning?

HOWEVER: Staff require we not start anything before 10:00am. Realistically 10:30 after coffee break.

What stuff we will be doing with MARS this time:

* LETS RFP Response
* Expecting a draft Smart Contracts RFI
* (anything on D-SSI RFP – suggest not; will still be rough draft)
* IOTA Update

Stuff we want to ourselves / with or without MARS feedback:

* Smart Contract RFI – followups / potential for issue that week (though unlikely)
* Disp-SSI RFP drafting
* DIDO

### Discussion

MB: Stick with Tuesday afternoon.

Who will be in Reston?

* Lars -yes
* Mike B – to be confirmed (else Remote)
* Nick – Yes
* Ian – Yes
* Rob – No
* Robert – Not in person

Other potential attendees:

* Bobbin (unless going to AI PTF)
* BoD folks won't be wandering in as there's a BoD meeting Tuesday afternoon

Other possibilities include Wed morning and Wed afternoon.

**Verdict:** Stick with Tuesday afternoon for now; revisit later for e.g. Wednesday

Any other Finance ideas that we could use to meet on Wednesday morning (combined with Blockchain)?

* FIGI Crypto
* FIBO
  + Content
  + Reporting formats

Also means that Elisa, Richard Beatch and others.

**Proposal:** We meet on Wed morning (not Tues afternoon) and jointly with FDTF.

Anyone against: No

**Conclusion:** We do a joint meeting on Wednesday morning.

**Action:** Put in a meeting request for Wed am for FDTF and BC-PSIG jointly.

**UPDATE (later in the call):**

Claude still finalizing the AI and Cloud stuff – revisit this next week and finalize. Either Wed morning or Tuesday afternoon.

## Smart Contracts RFI

Including code generation.

### Proposed Title and Scope:

"Pattern Language for Smart Contracts"

Plus broader scope per the slides from Dec 2021

### Notes from December QM:

* Might be too narrow?
  + May also want to associate database storage
  + Process as a whole – to be deployed across a range of DLT and DIDOs and other non DLT things also
  + Process language + use of language to generate a library of patterns

Something could be a clear RFP.

In doing the RFI, think about:

* What would the RFP look like (scope)
* What would we need to know from the industry to support that scope

### Discussion

Note that Smart Contracts are not strictly Distributed – the application is replicated.

Literal 'Distributed' would mean e.g. edge computing

There is some distinction in that there are different kinds of nodes e.g. permanodes.

So there is decentralized. Different things run on different places

Distributed in the DLT sense is that whole thing is 'distributed' (actually replicated) across multiple nodes.

The ledger is distributed? (different kinds of nodes) but also replicated.

#### Why mention it?:

Some of the scope and applicability of a pattern language could (may or not be) applied to non DLT / non Smart Contracts.

### Decision on Scope:

Options:

* DLT based Smart Contracts only (replicated applications only)
* All distributed and replicated e.g. edge computing as well as DLT

**Implication:** how much of the logical and physical design requirements for e.g. Smart Contracts, need to be in the scope for the proposed future RFP.

**Or 3rdly,** the RFP could be tightly constrained to DLT but the RFI could be used to make that choice.

#### Discussion:

Scope of the 2nd option is too large.

So DLT based only – these have very specific requirements.

### Scoping Overall

* We have the proposed scope of a proposed RFP
* We have the scope of the current RFI

Where there may potential for using the RFI to help firm up the formal scope of the subsequent RFP.

#### Other scope questions

* Storage
* Process
* Process language

Or we could decide today without waiting for the RFI responses e.g. to focus only on the generation of Smart Contracts code.

How the suggested scoping evolved:

Started with patterns for auto-generation

Issue was going from CIM to LM to PM. Don't usually use those patterns in the Conceptual Model

So that's where the discussion came about. So Patterns is a bigger topic than it seemed.

For example I Ethereum. ERC20 is a 'pattern' for Smart Contracts, but not based on modelling. Same for the other ERCs. Basically interfaces that you implement the bodies of. All at the physical level.

It seems fundamental to take account of the logical and physical constraints in the Smart Contracts world.

Whereas a CIM would be e.g. how do you model a mortgage closure process.

* Logical: statefulness constraints
* Physical:
  + typing considerations
  + Security considerations

MB: Can't hope to simply generate SC code directly from a concept ontology without something that takes account of these logical and physical requirements.

NS: Counter point: can define something at a business level e.g. whether a thing an be payable, ad the pattern language deals with the logical and physical requirements – these are the 'patterns'. For example you might have an Inventory pattern.

In crypto even 'payable' is a patter e.g. someone might be trying to pay with something they do not have.

Most of the effort in crypto so far has been on payment. There are other interesting things we can do like data non-repudiability in applications.

Security is also a potential issue (physical constraints)

See latest DIDO for more material on Security. Some to be completed.

#### Scope Firming Up

So for the following things:

* Storage
* Process
* Process language
* Logical: statefulness constraints
* Physical:
  + typing considerations
  + Security considerations

We think that:

* Storage – out of scope
* Stages of archival activity in Blockchains (else everything gets too big).
* Also transaction costs (all except IOTA)

**Scoping question:** whether economic parameters come into play or not? Gas fees, cost v speed considerations

### Other questions:

Has anyone come up with a command to purge a chain?

ETH has some mechanism for this.

Controversial.

Is this relevant to a pattern language for SC? YES since garbage collection could be a really strong pattern.

There is a way of pruning, Kinds of Nodes

- in certain DLTs.

So scope includes archiving, deleting, pruning etc.

* Lightweight nodes
* Lightning nodes
* Permanodes
* Authority nodes

In Blockchains – there is no ownership of a transaction. The point of being decentralized is that nobody 'owns' anything.

EXCEPT with Centralized / permissioned DLTs e.g. Hyperledger, CORDA/R3 and so on.

Streams is part of the solution. Lets you say in a message that it over-rides or negates a specific previous message.

See link:

<https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.2_views:3_taxonomic:3_node_tax:full:pruned>

on Pruned Node.

**Scope:** all of these things.

**Frame as:** What are the logical and physical constraints that apply with SC code

- so that the pattern language OR whatever is generated from those, can with these, oof which the above are simply examples.

Note that the answers to some of the questions relaying on centralized v decentralized (e.g. Hyperledger, R3) may be different. Standard should embrace the full range of styles of DLTs.

Also for permissioned v permissionless.

The RFI could cover both, even if the resultant RFP might later elect to be limited to one specific style of DLT.

Summary: We need the RFI to figure out these scoping questions in the overall RFI in order to determine the scope of any proposed RFP.

## AoB

See update in QM Planning above.

Looking for potential new co-chair for AI PTF.

**Next Week:** DIDO