Blockchain PSIG Call Notes

*2 Sept 2021*

# Attendees

* Mike Bennett
* Robert Rencher
* Ian Stavros
* Marilyn Pineda
* Bobbin Teegarden
* Ambrose Kam

**Apologies:** Rob Nehmer

# Agenda

* Smart Contracts RFI

# Meeting Notes

## Smart Contracts RFI

* How ready we are?
* Comments from Robert

### Readiness:

Document not ready to circulate in current state.

Can summarize the objectives and key points in the paper. Would enable us to get validation and feedback from participants.

Once the editorial work is completed we can do more with it.

Parts are more mature / complete than others. We need to prioritize specific parts of the RFI to work on.

A deadline will help.

At least December if not September.

Suggest: Late October deadline to finish it for the December QM.

Also consider timings for responses e.g. Q1 or Q2 2022.

Formal release is at Quarterly Meeting i.e. end of Sept OR early December.

### Comments (Robert)

2.2.1 in line comment on litigation

May be eg. unexpected system malfunctions tht result I non conformances that could result in litigation. There is not a solution that would not be litigated.

2.2.1

Editorial

Tiered or smart arbitration

Potential for autonomous (smart) arbitration.

Add questions on this e.g. combine analytics with AI. Opens up new fields of opportunity and potential research on autonomouc arirtration.

Can introduce and siuss briefly, plus add a question / space for comment.

#### 2.2.4 Testing

2 new kinds

Reason: Aerospace - see unintended system failures resulting from untested interactions between components that are tested OK in isolation i.e.. emergent from system. See System of System testing.

Add some notes on this.

We can look at the research on this at a future call if needed.

#### Smart Contract v DLT comment

e.g. history with databases with stored procedures. Based on this experience, we should pose that question.

 - add to questions.

#### Recourse

Damages – goes back to autonomous arbitration. Talk about recourse generally i.e. value to the recipient – diminished by legal system costs.

 - if we can automate this changes the commercial dynamic on that.

#### 2.2 end text

Case law:

Can a SC be used by multiple parties?

Can there be a standard template?

Can there be a standard arbitration SC people would agree to use.

Own code versus standardized – opportunity for standards bodies to get ahead of this.

Potential RFP. If we build it will they come?

IS: If we build standards, some will adopt. But to take hold, need an easy way for people to start using it eg make it available in a Github repo.

 - add that in questions

* Are they needed
* How would this be used e.g. GitHub repo for download
* Definition of standards

BT: Responses might include ideas for future SC opportunities

#### 2.4.1 Ecosystem / DLTs

Interoperability

MS have developed a token to facilite interoperability between different SCs.

Should we embed SCs into DLTs?

Q on whether SC type stds distinct from DLTs. Argument for potential standard.

### References

#### AIA Reference

See SAI G31 document

#### DD250

Ref to company – in link. Authenticiti / Cap Gemini

PoC in Aerospace industry association (incl Boeing, who contributed knowledge on the use case).

### Potential Responders

**Authenticiti** claims a working solution - not seen.

 - Potential responder?

Indicates there are working solutions. For DD250.

**DIDO Solutions** also has a thing for spinning up things for SCs.

 - also a potential responder

* Not name the vendor in the RFI? If so, include several. Let the know they are mentioned.

OR

* Not put names in the RFI.

Given something is in the public domain that is an example of a capability described in the RFI.

Letting them know will help ensure a response.

DIDO Solutions is a separate legal entity. Has a working demo on being able to spin up LT nodes that are concurrent.

Have IOTA node networks capability

Also SCs for Ethereum.

DIDO Solutions would also be able to respond to this RFI.

See video at:

<https://drive.google.com/file/d/101nfV9bX69RiPcJxXsnHIgOs6FD0x-n-/view>

DIDO have paired the spin-up capability with governance considerations e.g. communities of interest.

### Governance Considerations

See Parity, in 2018 – pushed an update that stole stuff. There is a need for some sort of governance – can't simply push a product to the chain. Can disrupt others' business or shut down the DLT network. Need to be able to verify that the solution is working as intended.

Given that SCs are generally fixed, non repudiable code. Meanwhile for new SCs, need some metrics on what tests have been carried out before using a new SC. Ned more intense QA.

Otherwise e.g. ETH had to do a hard fork for a bug that impacted 56% of the network. Break sybil protection.

Was that with the DLT / Network or with the Smart contract architecture?

Can add questions on whether there is any interaction from SCs to the underlying DLT.

May or may not be a trivial question – so we can add that to the questions.

## Proposal:

Can we put this RFI out with the simple questions we are seeing? There's lots of other possible things down the line.

### Potential additions:

See IOTA slack questions:

Does that mean that a transaction made from one chain to another chain will always execute, but it's uncertain when and if you receive a return value or not?

### Emergence and Holons

BT: So there are cases where SCs may interact with other SCs – can we add questions that unpack the systemic relationships among these things.

Systemic Emergence – behaviors arising from the interactions between or among SCs that would not be predicted by looking at an individual SC in isolation (See Robert's comments earlier).

Architecture approaches to resolving these considerations e.g. a 'hub and spoke' thing where you have one overarching SC that pulls in the others.

Reusable components?

Separately there is the idea of a holon.

Have an over-riding contract that contains other contracts or kinds of contracts that decompose and can run in parallel. If these can spawn others, can act like a push and pop arrangement. Can have threads that come back together later. This scenario is then highly distributed, behaves more like a network.

Q (for the RFI) is that ever desirable? Or is it a thing to avoid in designing SCs?

 - may be impossible to avoid this, it is another creative architecture that could be used.

Add Q: what are the QA implications of these kinds of architectural choices?

More generally, you can't prevent people developing SCs in whatever style they see fit. This has potential implications for selecting, reusing, choosing to interact with other SCs.

[on this – provides more background to add to Robert's comment about systemic emergent faults]

### Systemic Issues

Can see systemic issues – need a way to have something that arbitrates between SCs.

A network is not arbitrated if you have a wholly independent set of SCs that have the potential to interact. This is Contract to Contract.

That is how it is today. But even at conventional network protocol level there is arbitration and sequencing. Can that be extrapolated to SCs – e.g. there are clear sequencing requirements e.g. 1 come 1 serve or other. Puts order in the sequencing of SC execution. Needs to be defined.

If you use that model, the Node puts the thing back together with ordered numbered parts, that can arrive out of order

(like LETS / Streams)

These behavioral alternatives need to be defined. Some will or won't be acceptable for different business scenarios. Some scenarios would not be able tolerate specific alternative arrangements.

Look at the value of the contract execution (to one or other party), would have some influence on the sequencing, the desired or accepted alternatives in sequencing and so on.

### Timing

Another point out of this: Contract activities and timing: if something arrives out of sequence and is late, after a contract (or a given step) is already closed. May make some contracts invalid for example.

Timing of performance (fulfilment) of the contract. Once initiated the SC is there a period of performance that needs to be determined.

Comparable with securities exchanges buy or sell orders – these have a drop-off of time in which they can be allowed, for the participant. Once these things are automated and autonomous there have to be (automated) ways of resolving these kinds of issues.

**For Questions**: how much of these kinds of scenarios are we seeing in SCs today? Are people instinctively avoiding these issues? Presumably in future we will see more sophistication in these things.

SC – humans as observers, can't be in the loop in real time. Can note afterwards that some outcome e.g. performance was not as intended.

Can anticipate some unforeseen issues resulting form these kind of issues, as well as or similar to what we have seen a the DLT network level.

Guardrail – discuss these, ask questions on what guardrails people maybe putting in.

For example inserting waiting periods (as in the Ethernet protocol). How satisfactory is that as a solution compared to e.g. something more like a handshake. Also how determined (hours, milliseconds?)

 - dependency on the underlying DLT?

Are we assuming transactions are in nanoseconds or a given timing (currently milliseconds).

How that will change as underlying DLTs change

A SC that works on one DLT may have different timing implications on a very different DLT.

Concepts of speed, over-the-wire etc. may change.

Talks to portability and interoperability again.

### Outcome

We hope to be able to have a simple enough set of questions to put the RFI out for September, but if not we can get it out in December.

Is there a sense of urgency on this? If not, aim for December.

However, value over time of the RFI will deprecate.

Do something smaller. Then focus on the potential RFP.

Proposal: Find e.g. 5 – 7 key questions we want answered by the industry, work on phrasing the Qs for those.

Additional info can go in the document background and / or the wiki.

### AoB

None.

Post Draft 5 onto the wiki with these comments from Robert.

### Next meeting

Continue with the RFI.