Blockchain PSIG Call Notes

*22 July 2021*

# Attendees

* Mike Bennett
* Nick Stavros
* Ian Stavros
* Marilyn Pineda

**Apologies:** Rob Nehmer

# Agenda

Continue to alternate with Smart Contracts. Look at Mike's notes from the Cloud WG call from this week.

Also DIDO-RA – Nick will have a few minutes to go over what he's been adding there for Consensus.

Are there recent articles on how IOTA manages consensus. E.g. FPC and cellular consensus.

See: <https://blog.iota.org/iota-research-status-update-july-2021/amp/>

# Meeting Notes

## DIDO-RA

Nick Stavros presenting.

2 kinds of 'Consensus'

* Classic
	+ PoW
	+ PoS etc.
* Consensus from Community of Interest

SCs: we were looking how changes to the Smart Contract code are done. Different consensus mechanisms? Are these always Community of Interest Consensus or do some of them use the classic Proof / Consensus arrangements to arrive at consensus on the code base?

* Ask questions on this in the RFI

## RFI Questions - Proposed

Frame some questions for the RFI:

'Is the SC code immutable for all time or are there arrangements for updating the code?

If 'Yes' to updating:

What are the consensus mechanisms?

e.g. do you use some 'Proof of' mechanism already allowed for in the DLT itself? Or do you use some other means of arriving at a consensus e.g. x number of named participants votes Yes etc.

Describe in more detail:

In terms of arriving at a consensus on a proposed change to the Smart Contract code based:

What arrangements are made for testing and / or code design review

What other QA mechanisms. How are these described.

Do you use a code repository such as GitHub or Bitbucket?

Do proposed changes to Smart Contract code go through an end to end process e.g. issue ticket; proposed change; design review; test; ull request; pull request approval.

If pull requests – how is the committee or group of people who can authorize the PR set up.

Anther question - might not ask but… recent events causing real monetary losses as a result of rushing to fix an issue in Smart Contract code. Add a reference in the RFI if there's anything in the public domain. There is:

<https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether>

### Organizational Questions

Broader organizational questions (for some of the potential answers above)

e.g. pull request / GitHub (or any change management arrangement)

Suppose a given number of approvers.

What happens when 1 or more of those retire, die, move on, become unreachable etc.?

That is, organizational questions. Even if the entity does not think of itself as an organization.

### Other Issue Management Questions

Any other questions on how different groups deal with bugs and issues in Smart Contract code?

For specific answers in the above

What about the option where thy are completely immutable with no updates or modifications.

 - how did you obtain that robustness?

Were there some kind of tests that recorded and defined the scope for that.

e.g. in some very simple requirements (e.g. just moving funds in something other than the native cryptocurrency)

### Testing Notes

Encourage responders to identify specific kinds of tests e.g. smoke test v regression test (synonyms).

Audits - existing: DLTs may not have QA Audit but refer to 'audit' as e.g. security audit.

Also as about various 'audit' activities. Specifically security audit (commonly done in crypto).

How are security audits requirements defined for a given Smart Contract, how it is set up; how are results made available etc.

Any other kinds of audit?

### Note on structure

Start with basic questions about change; some of the later questions apply to one or another answer to those questions – see the immutable code above.

## Broader questions for the RFI

### Consensus

IOTA Specs status on that…

## Layered Model

Latest from IOTA:



## Semantics

The semantics of the layers in the above are clear: it is how one piece of code run on top of the other.

Nick:

The above seems to correspond to layers of abstraction e.g. information, knowledge, wisdom.

See:

<https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.a_glossary:a:autopyramid>

Mike disagrees.

These may converge in interesting ways but the semantics of the IOTA and ETH layers is one or other of:

* Code running on Code (e.g. ETH Go Code)
* Payloads containing payloads (IOTA Layer 1 and 2)

Do these layers have any relations to the DeFi layers:

* Aggregation
* Application
* Protocol layer
* Settlement layer

See <https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.2_views:2_tech_views:defilayers>

### Outcomes

Put that in the RFI: 'Can you align the layers of your Smart Contacts solution in terms as described in the DeFi standard layers'

## Next Week:

Back to general Architecture considerations

Maybe revisit the semantics of the layer.

Look at different ways of slicing the deck.