Blockchain PSIG Call Notes

*8 July 2021*

# Attendees

* Ian Stavros (643024 - Jackrabbit Consulting)
* Char Wales, Jackrabbitt (265922)
* Marilyn Pineda
* Nick Stavros (Jackrabbit 569992)
* Rob Nehmer
* Kam, Ambrose (US)
* Mike Bennett

# Agenda

* Smart Contracts RFI

# Meeting Notes

## Quarterly Meeting Feedback

Presented at MARS – various (LETS RFP, IOTA Protocol RFC, Disposable SSID RFI, Smart Contracts RFI)

BC-PSIG meeting was mainly on the Disposable SSI stuff.

We did not tinker with the Smart Contracts RFI at the QM

## Smart Contracts RFI

### File Management

Current draft called 'Draft 4' – clone of Draft 3.

Could have posted as a working draft but we did not.

### Where we Were

At MARS: considered structure of the questions and of the responders.

"Proposal to provide tabular map of how and who to answer each question ..."

Was part of a discussion on how to guide the responders in their answers.

### Recap: Structure

Whether to have:

* One lot of questions that different people might answer differently
* Sets of questions per audience type

We decided to do the 1st of those.

Example: 'Whether a SC is a Contract' – could be answered very differently from Business / Legal versus a technical responder. We want to hear about those kinds of difference.

### Structure Decisions

With that in mind:

We want to structure the question by topic.

We have a topic structure in the 'background' stuff.

Logical: align those.

### RFI Edits

Have a go (see RFI changes for this)

Gaps?

* Topics we don't have questions on?
* Questions that align with a topic we haven't described

i.e. any question we ask should have background material to go with it And any background material should have a purpose (and therefore a question?)

As always: summarize what we should already know (not ask dumb questions) versus what we want to know.

Also on this: 'Is there anything you know about that we don't know about – please feel free to fill in gaps'

(may be stuff specific to a given ecosystem)

### Example: Gas

e.g. questions

* 'Whether a Smart Contract requires gas payments?'
* 'Why a Smart Contract requires gas payments?'

And from that, whether that gas, money etc. is derived from miners?

e.g. in IOTA, there is no mining. So where does the 'money' come from?

At the Layer 1 (Tangle) level, the money come from existing issue, and the 'earning' is about doing transaction validation not from mining.

So where should the money come from.

Separately: if you do an Ethereum SC in IOTA, does it need to have gas denominated in ETH?

### Proof of Work / Proof of Stake

The whole money / gas thing relates to PoS versus PoW.

How to ensure that the SC is built from the consensus model.

#### Recap for IOTA:

When you go to post a txn you volunteer to validate 2 txns, that are randomly picked for you.

Since this is not real money, you can arbitrate / decide on how much gas / money each party has. Not tied to e.g. USD.

Separate from interoperability problems.

For example if you run ETH SCs on the IOTA Tangle – that's an interoperability question. But with own SCs should not need to need gas.

Should be able to run stuff overnight validating transactions (donating your processing power)

#### Gas: Questions for the RFI

Why gas?

General – unpack all the questions. Speculate a bit to see what we don't know.

Maybe (for IOTA):

Potential issue with throughout and capacity.

e.g. If it costs nothing to post a something from a SC then you end up with bottlenecks and stuff.

- congestion control

In Layer 1 (the Tangle) they deal with congestion via a mechanism called 'Mana'

Mana is a kind of rewards / points system. Based on activity, being a good node approver etc. Some measure of how you have contributed value to the ecosystem.

Why isn't Mana used to control capacity / throughput / congestion etc. in IOTA SCs rather than something new that looked like gas.

Potential issues (we want to hear these issues as answer to questions; so we want to make sure the questions elicit those answers):

#### Break down:

* Gas as reward for miners
* Gas as something to mitigate something (e.g. congestion)

That is, different goals.

Did IOTA choose gas in SCs in order to mitigate something and if so, what?

#### Broader question:

The reasons for gas in Smart Contract generally – articulate as many distinct reasons as possible.

e.g. reason for gas as a reward v reason for gas as congestion control

Whereas when there is not a reward reason, other reasons may still apply.

#### Gas and Money Questions

Gas = Real money?

If e.g. IOTA not using mana but using some kind of payment, then that's MIOTA currency.

MIOTA is not generated by mining but still exists – as single issue at the start of time.

If IOTA SC uses gas, s the gas in MIOTA ad how do you get hold of it? Do you have to go and buy yhr MIOTA off an exchange in order to participate in a SC.

#### IOTA Specific Questions

Related to that (IOTA only):

When you set up Blockchain (for the reasons we hope to find out about above), then you get to choose certain parameters.

* What are the parameters?
  + E.g. price per txn (gas fees) versus something…
  + Something?
    - Speed?
    - Congestion related? (or are those the same thing)

Q: Suppose you are setting up a new Smart Contract arrangement on a new Blockchain, what are the design considerations that have to be balanced out.

### Structure

Back to our structure:

In the explanatory sections – what some of these might be?

**Action:** dig into a couple of existing SC arrangements to figure out at least some of these)

In the question section: ask that question wrt those things

Examples to start with:

* speed,
* throughput,
* message sizes / bundles,
* complexity of the SC / of the txn generated by the SC

e.g. simple movement of funds versus something tha is very intensive in terms fo what computing needs to be done.

### Transactions Consensus Algorithms

* PoW
* PoS
* Zero Proof
  + PoW is a zero proof

#### Meaning: Zero Proof

The principle: Ask a bunch of questions, get you to respond with an answer. Do I get 'n' right answers in a row how many in a row e.g. 10 or 100 right answers in a row. That is, to do the proof you solve for n decimal places at the start of the hash. Recalculate … you are reverse engineering a hash. What did it take for everyone in the group to get a given character in the 1st position, then the 2nd and so on, where it becomes progressively more complicated.

See e.g. <https://www.bitdegree.org/crypto/tutorials/proof-of-work-vs-proof-of-stake>

#### Question / thing we don't know:

Does the SC do its own PoW or PoS work or does it always make use of the existing Layer 1 protocol

e.g. Ethereum 1.0 (PoW not PoS): smart contracts (Ambrose was doing) made use of the existing Ethereum blockchain arrangements.

In general: you put your SC onto the Blockchain as a 'transaction' in the Blockchain sense, so it is the block that provides those mechanisms.

Is it a sensible question to ask 'can a SC do its own PoW or PoS implementation or must it always use that’s provided in the underlying Blockchain.

(this might be a dumb question in most architectures and yet not a dumb question for specialized ones like IOTA)

OR it may seem not a dumb question but something where you would never have a good business reason to do that thing.

IoW you still had a make that choice at the design stage even if it was an obvious one.

**Conclusion:** worth asking this question AND explain why we ask the question.

### Outcome: Explanatory Material v Questions

So the Background sections are not just explanations of what we think we know but also some rationale behind why we are asking some of the questions.

Example: "in some e.g. graph /DAG based DLTs, there may be sensible different choices to make on this question"

**Category of questions:** What are the design choices you make in setting up a Smart Contract?'

Similarly: design questions in setting up a Blockchain for use with Smart Contracts?

### Different angles

#### Business questions

Suppose you end you needing to pay gas money, that has to come from somewhere. So the end user has to find real money (USD) somewhere along the line, and get it int the relevant crypto standard (unless instead they can mine it).

See below for why.

## Why we do the RFI / What we can standardize

CW: let's not lose sight of the reason for this RFI .. that we are gathering information to help us decide what aspects of Smart Contracts can be addressed with one or more OMG specifications (via the RFP and/or RFC process) .. Let's make sure that the questions we ask .. even if they're open-ended .. help us do that. Just a thought ...

MB: We have business and technical things to find out that may lead to different kinds of potential standard.

### What can we standardize?

* Semantic interoperability
* Syntactical interoperability
* Business Process / workflow interoperability
* Data structures etc. (syntactic?) interoperability

### Also: Existing Standards

What is already covered in standard e.g. W3C, ETH (ERC) etc. (ERC20 among other)

What are the variables that cause something to be or not be a sensible proposal for an Ethereum standard?

ETH – based their RFC process on that of the IETF.

Also what implementations are out there that can form the basis of what could be standardized.

e.g. is IOTA do something in a standardized way it becomes a de facto standards, which can then be brought to the OMG (as an RFC) if it's more widely usable.

We need to understand the broader field of what is out there.

That is why we need an RFI.

### De Facto Standards

There may be lots of de facto standards out there (as we've seen with Ethereum – is that de facto or do we regard Ethereum as a standards body?)

NS: we should regard ETH as de facto standards for reason:

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

Depends on the definition of a standard body (see DIDO definition on this, from Inner Cloud )

See: <https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:xapend:xapend.b_stds:tech>

This is from an O'Reilly book (not our own made-up definition)

There are nuances among these e.g. whether ISO is de facto or de jure: since countries vote, this is regarded as de jure. As compared with consortia like FIX, even OMG is a consortium.

Meanwhile ISO recognizes the process that OMG follows as being of a suitable quality for ISO.

So that's a way of defining what's a standards body.

Assertion: Ethereum does not have a formal process?

Ethereum does have a formal process but not one that follows the usual rules of order (Roberts Rules; OMG White ballot like rules)

See recent studies on this. Different arrangements are and are not possible in a decentralized environment. Uses consensus arrangement e.g. consensus algorithms comparable to what there is for the Blockchain itself. May also relate to reputation points (proof of stake).

For example OASIS has different rules.

IETF goes by the 'group hum' i.e. consensus. Also has a stated protest mechanism to address shortfalls in that arrangement.

Ethereum based on IEFT but may not have those arrangements that IEFT has on protest

## AoB / Next meeting

### Architecture (for next week)

Liquid Avatar app, uses BC. Used for identity.

<https://floridanewstimes.com/liquid-avatar-app-review-free-cartoon-creator-app-to-protect-your-identity-online/251868/>

Start on that for next week.