Blockchain PSIG Call Notes

*28 Jan 2021*

# Attendees

* Mike
* Rob
* Nick
* Ian

# Agenda

Map out the program for Q1 - possible new RFIs etc.

* Smart Contracts: RFI for Q1; possible RFP to follow
* Oracles: initial knowledge gathering, possible RFI in Q2
* Other items not yet covered e.g.
  + Crypto Exchanges
  + Digital currencies - stablecoins etc. (with FDTF)
* Other stuff coming through from IOTA - potential RFPs?
  + Access
  + Stronghold
  + Wallets
* What else?

# Meeting notes

## Updates

Meeting notes are now up to date on the wiki!

### CBDC

The FDTF is starting a new broader RFI initiative on digital currency. Expect to liaise with this BC-SIG as well.

* Someone reached out to Juergen about that – contact them
* Mark Montoya interested

## Q1 Program

See 21 Jan notes for overview:

* Smart Contracts
* Oracles
* Digital Currency (with FDTF)
* Crypto Exchanges
* Etc.

### Summary

**From last week’s notes:**

Do the RFI on Smart Contract in Q1

* Would not be ready to do RFP in Q2
* Do RFP for Smart Contracts in Q3

Oracle - this shorter list:

* Start the conversation in Q1
* Aim to do something formal on that for Q2
  + RFI or RFP depending on what we know

Stronghold – not until Q2 or Q3

Access – discuss on a call in Q1 – figure out what it is and schedule accordingly

Digital Currency

* Figure out CDBC status and FDTF in Q1
* Segues into Smart contract
  + As part of the fungible currency discussion for SCs
  + SC may alternatively relate to EFTs\* as alternative to cryptocurrency
* Discussion in Q1 in the lexical context we create for the SC RFI in Q1.
  + Gives us a clear scope – we can stop the discussing if it gets out of band
  + Determine what we need to say about it

\* EFTs electronic funds transfers

### Smart Contracts

Reasonably well known – we should be able to go straight to an RFI on this

### Oracles

We seem to know less about this. Recommend internal discovery initially before an RFI.

#### Comments:

RN: understanding of oracles is that it is something outside of the smart contract, that questions questioned / appealed to. So in some sense that is not standardized. Maybe it need not be? Like internet of things – anything out there can be an oracles. So the standardization might be some kind of protocol with which to ping that IoT device / that oracle.

We should explore IoT and messaging within the IoT. That would give us some clue on structure we would want to be looking at for oracles. *De minimis* it would need to be able to tall to anything on the IoT.

In other words – we need to some internal discovery 9not RFI on IoT specifically.

RN working on something to help auditors with initial profiling of clients – so is working on initial research (with Deniz Appelbaum).

#### Implications for DIDO-RA

NS: Working on this, and the CLI. Once we establish a CLI you can start doing things like handling different kinds of devices. Currently not uniform.

So this will impact on the IoT internal research.

### CLI RFP

NS: Also an RFI or RFP on command Line Interface would be a worthwhile effort.

e.g. retail are interested in the CLI concepts. Comparable to Rest, but less clear what you would send back or forth.

At another layer, there is Posix, SQL etc. but there is a lower level where this interacts. CLI is key to having things map to the platform. This addresses smart contracts, exchanges and other DLT features.

Consider what ‘goes across’ – e.g. is it always text (no). Can send code for commands like copy (cp). This is the only thing that would be durable Solidity smart contracts would end up like Cobol – essential but organically grown versus designed and engineered.

MB: Distinction we need to understand

* When we to improve the DLT world from how things are now
* When we aim to standardize aspects of what things are

NS: DIDO Solutions will be working on a CLI, and would be interested in seen an RFP for CLI and would be a submitter for that. As DIDO Solutions.

#### CLI RFP Timings:

Wrap up the DIDO-RA work (mainly done). Trade study for DIDOs product evaluation would be included in the DIDO-RA. See email to IOTA (to Mat and Mike) on how they would fill out the requirements. That would be done by the platform vendor (or foundation etc.)

A 2nd phase would be on vendors of solutions within a DLT – ranking requirements and relative importance. Has a scoring mechanism on that.

If they get IOTA to respond on these things, would then challenge Ethereum to do the same things, and be able to compare them.

#### CLI RFP General Issues and Discussion

MB: What about Hyperledger?

Permissioned versus permissionless

* This is a functional requirement so not covered in the above

Also public and private. These and the P v P are functional requirements.

For someone doing a CDBC they would look at the functional requirements.

MB: Permissioned and Permissionless is a feature of the overall DLT – it is always and only one or the other.

That is distinct from whether individual sets of Smart Contracts are Permissioned or Permissionless

NS: the choices of P v P are relevant to the community. Not the product (platform). Domain v platform.

Are you sending these questionnaires to – domains or platforms?

Functional requirements – going to the domain not the platform.

BT: The domain can say they want a choice, or want to support both.

NS: For the Domain users, for the functional requirements, they are not yet thinking about those questions, they are jumping into either Ethereum without addressing the P v P question (!)

e.g. CBs might want private, permissioned

NS: expect to finish the questionnaire stuff in the next 2 weeks. Expect to see in the wiki.

### Oracles

BT: Jumping right in, if oracles are more like browsers/search engines with a blockchain focus, what kind of thing is standardized around browsers/search engines

but in one browser, you can use http or https your choice... e.g. So the 'choice' may be a functional requirement.

### Program So far…

* Smart Contracts – RFI in Q1
* Oracles – internal discovery in Q1
  + IoT discovery
    - Precedes Oracles
  + Browser / search engine equivalences
* CLI – RFP

#### Timing on the CLI RFP?

Have a draft by June – for review by the appropriate TF

What TF? MARS

## General Topics

### Layers

BT: Do you have a diagram of the 'layers' (like the ISO Layer diagram for networks)? E.g. 'streams are layer 2...' Did I miss it?

Blockchain interoperability RFI in March 2020 – did not yet follow up 2 potential areas:

* Defining the semantics of DLT basic concepts (blocks, ledgers, transactions etc.)
* Defining a way to reuse business (concept) semantics

Ongoing discovery: more fundamental discovery e.g. the layered model, the underlying semantics.

### Digital currency

Aside: the current thing between the Reddit group and the hedge funds; now going after crypto:

DogeCoin – started as a joke. Is crypto not just a digital currency. Is accepted on e.g. PornHub where respectable payment systems don’t tread.

Ongoing conversation with FDTF. Creation of different crypto coins.

This is where the DIDO RA NFRs become important.

#### On Money

BT:

Got this from the Long Now Society, let me know if you want the email:

Members of Long Now,

Our Long Bets project was founded on the premise that we can improve our long-term thinking by holding ourselves accountable for the predictions we make about the future.

One of the project's inspirations was a $1,000 bet made in 01995 between Long Bets co-founder Kevin Kelly and self-described Neo-Luddite Kirkpatrick Sale. In a WIRED interview with Kelly, Sale expressed his belief that by 02020, humanity would suffer “multinational global currency collapse, social friction and warfare both between the rich and the poor and within nations, and […] continent-wide environmental disasters causing death and great migrations of people”-a perspective that, suffice it to say, Kelly did not share.

In this month's newsletter, we are featuring Steven Levy's deep dive on the bet: its origins, its implications and-now that 02020 has come and gone-its winner.

"Much more than a thousand bucks was at stake," Levy writes in

#### Outcome

We need to figure out how to progress the conversation on digital currency with BC-PSIG and FDTF.

## Meetings Cadence

Start with one thing at a time

Next week: Smart Contracts RFI

Then quantify the work and how to proceed.