Blockchain PSIG Call Notes

*15 July 2021*

# Attendees

* Mike Bennett
* Nick Stavros
* Robert Rencher
* Rob Nehmer
* Ian Stavros

# Agenda

* Architecture progression

# Meeting Notes

## Why we Do This Work?

Purposes include:

* Potential for standards
* Identify existing standards
* Understanding of the landscape (for future standards, member knowledge)

## Updates

### CBDC WG

CBDC was not intending to meet this week – there is an error in the FDTF notes for last week suggesting there would be. To be corrected on the FDTF record.

### ECB

CBDC – thing from the ECB on proposals for CBDC for Euro. Mentions that it might or might not be crypto.

<https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html>

As Blockchain PSIG we have one foot in this – the crypto side. DC is broader as a concept and ECB confirms that concept is not an empty set.

- will be discussed at next FDTF weekly call.

## Also of Interest

#### Figure

Adverts for a loan company, with 'Blockchain' as the spokesperson so we infer that the technology for that loan is blockchain based.

<https://www.figure.com/blockchain/>

Another kind of thing to keep an eye on.

### Cloud Security Alliance - Blockchain WG

Blockchain WG of the Cloud Securities Alliance – presentation on the legal implications of the smart contracts stuff. Detailed forwarded by Claude Baudoin to Mike, Bobbin and Nick. Mike attended and took informal notes.

More ideas for more questions for the FDTF's SC RFI. Some went beyond SCs to crypto currency (trading, front running, exploits etc.) and may be of relevance to BC-PSIG and / or our Smart Contracts RFI.

Q: If we are looking at architecture on these alternate weeks, does that include matters to do with currency, economics, trading, security, bad actors etc.?

**Comment:** We think that maybe a lot of what goes on in financial interactions involves Smart Contracts.

## Smart Contracts

**Clarify:** when we talk about SCs, is there a specific context we have in mind when we talk about Smart Contracts. Can have different types of SCs that fit the need of the agreement. Anticipate that based on different kinds of agreements we have today that require an exchange of value, there would be a kind of Smart Contract to support that.

This can be from something as simple as buying a stick of gum, to buying a house.

Back to our 2 views of SCs:

* **By internal properties:** what kinds of thing that are (objects)?
* **By purpose:** what kinds of agreement would they support or mechanize?

May start to see SCs build out into different kinds of structure (internal) to support the different applications (external). That is, we may be able to classify them according to patterns.

These are 2 separate dimensions for how we would define that taxonomy.

In terms of taxonomy theory: Topic v Type taxonomy

### Smart Contract Security Questions

Secure communication but no secure computing in the distributed world.

But a large part of SCs is computational but is not secure. Anyone who has a machine can execute the SC. Does this mean that can execute a Man in the Middle attack? Can't hide things inside the SC.

Then possible patterns:

* A SC that is something for an oracle
  + The computing happens off the contract and communicates with the smart server where the (secure) computation happens
* Collection patterns
* Different layers (presentation, middle tier etc.)

These may feed into a yet more layered architecture view.

At this point it seems they have not yet defined smart contracts in terms of the inter-relationships between SCs.

There are patterns that remain to be done

Consider a table in a DB – can think of SC as a set of independent tables; have not yet thought about the relationships among the tables. Like having entities but not the relational dimension. In reality these would more hierarchical than a relational model.

## Governance

[Ed: while most of the above was discussion on Smart Contracts based on what we learned in the CSA Blockchain WG call, the conversation keeps trending towards Governance. Added this as a heading]

### Smart Contract Governance Issues

2 distinct issues:

* How you get to run a SC
* How you get to change the code in a SC

#### How you change the code.

*(some of this is feedback from the Cloud Security Alliance Blockchain WG presentation)*

Variation even in that: from

* non changeable
* one (named) person can change it
* A define number e.g. 7oo10 people can change it

This relates to consensus:

* Data value consensus (the Blockchain proposition)
* Community of Interest consensus e.g. for changing code

This is why a lot of DLTs are not exactly decentralized even if the architecture itself is.

*[See previous comments on the VMB paper on governance issues in decentralized DLTs, discussed on earlier calls]*

#### DLT Governance Comments

DLT is still in its infancy. We see a lot of theological differences.

Some are legitimate reasons, others are not so much.

### Digital Currency

Also on Digital Currency: as well as ECB, the US Fed also looking into that.

Then the concept of 'sovereign' comes into play e.g. who 'creates' the DC e.g. China, ECB, USA, or the idea of a 'global' currency, as envisioned in the original Bitcoin idea. This was to be a currency that did not have any sovereign.

Digital coinage varies by purpose.

e.g. Dogecoin created as a joke

### Cryptocurrencies

There are now around 3000 crypto currencies. They are easy to create. For instance you can go onto Ethereum with about $10K and create your own. As long as you can shill it you can make money (Ponzi like). No-one to assess the quality of:

* The governance
* The Smart Contract
  + Itself
  + Its governance
* Mechanisms e.g. for the 50% problem

Some don't have a web presence. At least one is just a Telegraph group. If you can shill it they will come.

### Regulatory Governance

Rather like the Wild West or (for banking) the 1920s i.e. prior to the establishment of a central bank.

Anticipate that this will be regulated. Then people can elect to play in an unregulated industry.

Binance – now UK banks no longer let you put money in or out. See

<https://stockhead.com.au/cryptocurrency/crypto-is-volatile-reckons-bank-of-england-binance-cops-another-uk-block/>

But how? E.g. you can't make a thing be regulated but you can identify what is regulated and people get to invest only in those. Comparable to 'Accredited Investors' in US securities trading.

## Definitional Questions (Money etc.)

The above also relates to one of the money questions we looked at before: whether the money is on the exchange or in your own wallet.

### How Addresses / Keys work: Wallet v Exchange

The money is associated with a private key. For exchanges: the private key (for your money) is at the exchange. With a wallet, you have the private key in your own wallet.

[indeed for one definition of the term 'Wallet', the wallet is and only is your private key – not the same meaning as a digital wallet for payments etc. in regular currency]

Is there an equivalent to fractional reserve banking? Not for the private keys. But for the underlying real currency you would use to ship it in and out, there is a definite issue with the fractional relationship between the stated value of the crypto currency, and the corresponding USD amounts available.

This comes back to:

Community of Interest > governance

Not simply governance of the SC but governance of the overall corporate and financial matters.

Hence DIDO RA governance section.

### Supply Chain Governance Issues

Meanwhile in the technology governance side: how do we govern these things in terms of risks in the supply chain.

Compare with the grain silos issue in the 1970s. Fed gov paid them to store the grain. Was able to move the grain from one to another given he knew when they would inspect each thing.

Suppose you identify a firm that has the bolts you need; but there ends up not being enough of the thing i.e. physical things double-count.

Real product can be double counted even if the digital twins are not. Hence governance needs to cover the relationships between the data and the real world truth of the matter.

- need an ontology for that (and a knowledge base)

### Governance Factors / Types

* Crypto currency (economic)
* Technology
* Real world / supply chain etc. (relation of the data to the things; how audited or validated)
  + Operational risk

Without good governance you can't ensure any of those 3.

In all 3 cases:

* Are they aware of a given governance provision?
* Are they implementing that?

See Appendix I and J of the DIDO RA. Cognitive model and governance model. These need to be overlaid to ensure you have complete governance.

### For this group

We could keep a watching brief on all 3 of the above concerns? So far we have been looking at the technical governance.

* Technical – this SIG
* Financial – Finance DTF
* Supply chain – this SIG (part of the interoperability conversations
  + E.g. Boeing

RR: The industry is not mature enough so companies are establishing their own governance policies internally. Key areas:

* DLT
* Manufacturing and information security

Where Manufacturing extends to Supply chain

So the issues for supply chain are of interest to this SIG.

What they do: find a company that is providing the infrastructure and apply the governance to them.

See DIDO RA:

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

## Architecture

### Layers

(from the Cloud Security Alliance Blockchain WG call)

* Ethereum runs some Go code
* Smart Contracts runs on top of that
* Application runs on top of the Smart Contract

We needed to identify the semantics of the layers i.e. what is the meaning one thing being a layer on top another thing. In this example:

* "A runs on top of B" is the meaning of the layering relationship

(how mechanized e.g. APIs, calls, DDS based information interchange etc.)

So that is one kind of layering.

Another is payload inclusion (like IOTA Layers)

NS: A large driver for the layers comes down to the Non-Functional Requirements. For example, maintainability, or Scalability.

Once we understand the layers we can apply these governance principles to them.

The reason for considering things in layers in the first place: goals for the layers.

For example interoperability. Reusability and so on. These may tie back to the NFRs. E.g. device drivers at their own layer. NFRs help us to ensure the layers are correct. NFRs have to be interpreted by the domain people not only the technical e.g. finance meaning of portable, maintainability. Same again for supply chain, consumer products etc.

### Governance

#### Back to Governance again

On the technology governance side:

The relationships between Business (CIM), Logical design, physical implementation

- without good business models, the physical designs:

* Can't be audited (from QA audit as distinct from security audits, which do happen)
* Can't be change-controlled

Need audit of all of the NFRs as well as business requirements. These include:

* Security
* Maintainability
* Reliability
* Etc. (all the NFRs)

Full list at:

<https://www.omgwiki.org/dido/doku.php?id=dido:public:ra:1.4_req:2_nonfunc>

## AoB

### DDS Foundation

Voted to have the user scenarios go public (user experiences). You can now get to these from the web. Link:

<https://www.omgwiki.org/ddsf/doku.php?id=ddsf:public:guidebook:03_user:start>

No login required.

## Next Call: 22 July

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/>