Distributed Ledger WG Call Notes

23 Jan 2018

# Attendees

* Nick Stavros
* Bobbin Teegarden
* Dan Webb
* Mike Bennett
* Rob Nehmer
* Pete Rivett

# Session Notes

## DIDO

See recently posted material (Doc and slides) at:

<https://ln.sync.com/dl/628e6b6b0/ytefgkve-4u272dta-kwvtknbv-tp8rzvst>

Verified: this link works for anyone without needing an account log-in

Nick: the main changes since the last version are reflected in Slide 20.

## Exchange

(on slide 20)

Discussion on what is meant by Exchange here. The meaning seems to be teetering between something that lets you technical exchange data from one node, network, community etc. to another, and something where you buy and sell crypto-currencies from different communities, like Coindesk. Or both? Or some abstractiojn of which these are both intended to be a common kind?

Picked up last weeks conversation about the nature of a crypto-currency exchange.

Crypto exchange = Broker + Wallet + custodian + Portfolio

(see last week notes)

### Portfolio

Need to look at some portfolio standards.

A Pf has a base ccy, one or more currencies, holdings.

### Wallets

Some are 1 ccy, some can hold multiple ccys.

If multiple, these are only ones on the same network and community.

### Exchange

Focusing in on the meaning of Exchange in light of what we know of wallets, portfolios, etc.

There is no way of keeping the coins from different networks in the same place.

That goes away if the exchange exists in one network. For multiple networks in the same community e.g. Ethereum, these can be exchanged. e.g. airmiles an ETH in the same network. That would be an exchange in one sense of the word - physically exchanging things in the same network.

Meanwhile a cryptocurrency exchange like Coindesk trades across networks and communities.

The more nodes in a network, the more secure.

Could then end up with a catalog of things you could exchange on that network.

Examples of e.g. transferring airmiles from different groups of airmile providers. Need rules that are set up, and the exchange (in this sense) would have to deal with those rules

FIBO or an extension of it could play a role in describing those rules?

## Ontology of distributed ledger applications.

Can we start to build out an ontology of the DLT concepts themselves?

### Concepts:

Secure messaging

Wallets

Transactions

Exchange

### Semantics:

Exchange

 - inter-network exchange

 - intra network exchange

 - etc.

### What to Do?

How to model these?

How to progress an ontology of this?

## Actions

* Finalize the DIDO paper in March. Publish through the OMG.
* Then in June do a rough copy of the ontology
* This can be a half day workshop of FDTF

### Whether to do as FDTF

BUT is it financial specific? No.

#### Discussion

Concepts are not specific to finance, e.g. supply chain. Would define "exchange" differently.

Most of what we said about "exchange" at the beginning is not at all specific to finance whereas crypto currency exchanges would be.

Exchanging things of value e.g. wheat, money, are all financial and are the same kind of things - see e.g. REA ontology for transactions.

Exchanging IoT stuff or other supply chain etc. tokens might not be.

Exchanging information about other non repudiable records need not be financial at all.

We did not come to a conclusion about whether this proposed workshop should or could be hosted by the FDTF. We agreed that it is not exclusively financial.

### Ontology Positioning

What we are trying to do with the ontology: PIM. What about CIM?

* PSM platform specific
* PIM Platform independent model
* CIM Computationally independent model

For an ontology we would have to start with the most general definitions of e.g. non repudiable records content, before specializing down into not only kinds of money, but kinds of thing that can be exchanged for money (per our earlier conversations), all as specializations of this.

## Some Terms and Explanations

### Taxonomy

* Taxonomy in its broadest sense covers a range of relationship types, of which the one we use for ontologies is the generic (“is a”) relation
* A taxonomy is not necessarily a tree structure
	+ that is, there may be multiple inheritance whereas tree implies single inheritance

### Ontology

**Ontology:** Taxonomy of concepts and their differentiae

MB explains the basic analysis required to come up with an ontology:

* Define a taxonomy of concepts
	+ Specifically a “Generic” i.e. taxonomy with generalization relations
* Understand the real world features that differentiate one category of thing from another (the differentiae)
* Consider these in terms of what real things they are expressed in terms of
* Consider data surrogates for most of those thing (most truth makers are not natively made of data though some are)
* Express these as formal properties in a language like OWL

Note that some differentiae are natively data, some are amenable to data surrogates use and some are not data-like at all e.g. legal and social construct underpinnings of things (truth-makers). Sometimes these end up being written verbally first then we think about whether or how to formalize the differentiae.

That's ontology (in the CIM) sense in general.

Then how to apply that to DLTs.

## DIDO Naming

It turns out the name DIDO is not set in stone and so in discussing the name for something here, we are not simply discussing the name for the ontology but a possible alternative name for DIDO itself.

DIDO – D = "Data"

This is part of where data comes in.

What to call it?

DLA - Distributed Ledger Architecture.

But "Ledger" gets misunderstood.

Distributed Integrated Objects (Immutable); therefore

Distributed Immutable Integrated Objects

Distributed Immutable Objects.

 - the rest is detail

But Objects <> object per CORBA.

What about Things?

Distributed Immutable Things

They are really distributed immutable records (of things).

The use of “record” was disputed.

See https://www.google.co.uk/search?q=definition+of+record&rlz=1C1CHBF\_en-GBGB705GB706&oq=definition+of+record&aqs=chrome..69i57j0l5.3220j1j8&sourceid=chrome&ie=UTF-8

Record (noun) (1): "a thing constituting a piece of evidence about the past, especially an account kept in writing or some other permanent form."

### Resolutions

* Use this definition and put it in the paper.
* Put all definitions in the paper e.g. Taxonomy.

So proposal is “Distributed Immutable Records”

(still disputed)

**The ask:** think about what we should call this

Where "this" = replace what DIDO is a placeholder for.

Then if this is XXXX when we would also have an "XXXX Ontology".

## Other things

Nick will re-read and re-organize the document.

Andrew Watson has volunteered to help us.

### The ask on DIDO Doc

There are 2 parts:

1. describes the architecture
2. (part 3) takes those description elements and looks for standards or each of those components.

**Wallets:** e.g. ERC20 on Ethereum. Still to be added to Part 3 (2 above).

## HOMEWORK

1. What will we name the thing that is currently called DIDO?
2. Try and get Hashgraph folks to talk to us.
	1. Get them to confirm whether the proposed architecture if generalized suitably to also describe Hashgraph.