Distributed Ledgers WG Call Notes

13 Feb 2018

# Attendees

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

# Summary

Reviewed the IR Swaps Process model

Considered what is or may be posted to some Block

* This includes things with a date value
* These may include other complex types or relations e.g. currency amount (the IR Swaps example is USD/USD not cryptocurrency)
* More typically and e.g. in Crypto, only a simple data element e.g. integer is posted
* Are there arrangements in existing SmartContracts / scripts etc. for posting complex data?
* What about data where a given element is updated or increment over time?
* Separately, there also needs to be some arrangements for pedigree, provenance and similar metadata for data posted to the Block in some cases

**Actions:**

* Clean up the IR Swaps process diagram to show contract initiation and terms
* Remove the assumption of what goes on a block and what does not, to revert to a purely conceptual model

# Notes

## DIDO Name

Nick Remind people to vote on the DIDO name change. Thanks

## Microsoft Article – Distributed Identity

<https://cloudblogs.microsoft.com/enterprisemobility/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/>

Nick This is a great example of WHY you can't use SW based Software Contracts. Only UML/SYSML/BPMN etc can express this that a human can understand

### Microservices

Nick I think the microservices would be an attribute of one of the conceptual blocks

We needed to define something like microservices for the things that get posted to, read from, updated on the block.

MB: The microservices are a drill in from the conceptual model, as they are implementation related. These would be done differently in different architectures and implementations.

## Distributed Data (Block) Records Issues

Explored several similar but related issues:

* Relationships of records to other records
* Complex data requirements (dates, qualifying properties like currency)
* Provenance and pedigree metadata

What is the complexity of some item of data that is posted to the block? Include pedigree and provenance.

### Record to Record Relationships

Need some clarity on when a record is updated and when it is a new record e.g. accrued amount this quarter v last quarter. Needs the date to disambiguate. Most of these are in the CRUD stuff.

Mike Bennett There are also calculations: floating rate calc, fixed amount calculated, floating amount calculate. So we need another layer of detail in this (concept) model. The rates etc. are in the terms sheet for the contract.

At any given time in the life of the contract, the contract has specific values for the floating rate, the accrued amount on the fixed leg, the accrued amount on the floating leg.

Mike Bennett Also the margin posted against these accrued amounts each day.

Nick Perhaps we need to think that the concept of a DIDO Object must include Date/Time spans and if it is fixed or floats

So the netting needs to be calculated every day (for margining) as well as at the end of the payment period for payment of the netted amount.

We still need to add the process ahead of the contract being agreed.

### Pedigree and Provenance

Pedigree and provenance are a similar but separate question from other qualifying data terms like currency, date and currency.

All data that is used must have associated with it pedigree and provenance at a minimum.

What does that look like?

Nick Pedigree and Provenance of each data (i.e., context) needs to be associated with each contract.

Nick How important the pedigree and provenance have is associated with the time it takes to execute

Mike Bennett Blockchain out of the box gives you pedigree and provenance of a simple (unqualified) data record e.g. a string or a number. It never deletes the data, so there is your pedigree right there.

So is there a problem?

### Temporality

Third thing needed is the life expectancy of the data.

There is a kind of object that is posted to the block. There is a temporality to every piece of data.

So the piece of data has a current date, also a date it expires.

### Complex Data Records

Can we post a whole object to a block, as distinct from a simple numeric or textual record?

A simple object is just an integer. A more complex object is qualified.

Initiation of contract would have you go through each of the items that are required and determine the appropriate context for each of these data items (objects).

Include time, date possibly even geo stuff.

Deus ex Machina - something outside changing the figures etc. versus totally autonomous (process happens inside the block architecture), and anything in between.

Every piece of data needs to have contextual characteristics, which have to be set up up front. So this is a consideration for the design of the Smart Contract. e.g. open ended, market values etc.

### Existing Support?

Do the (all the / any of the) current blocks support the posting of complex objects?

Ethereum talk in terms of oracles, these being places you go to for various figures. In Ethereum, our terms sheet / contract terms would be in such an oracle. In IOTA it might be on the Block itself.

NS suggests identifying a base type that all attributes are derived from (context).

What is currently supported on most block architectures?

* Typically a number (or text or other data type).
* For example fixed amount payable is a monetary amount, qualified by a currency.

Microsoft identifiers (see blog post) all the data is stored off block so presumably only the unique ID string is on the Block.

On Ethereum you can post a complex structure.

Mike Bennett Is this the case for all of them?

Not clear, we would have to check on a case by case basis. e.g. assume that IOTA can handle complex objects.