Conference Call Notes 09 August 2016

MB sums up 26 July actions

Subhankar: Some of the future things will depend significantly on the technology of choice. The kind f smart contrat we can write today i ne.g Ethereum - some of the sophistication of that is not feasible in Hyperleger.

These use different undrlying somethings - Go and Soliditidy respectivey. The reqiurements to store data for smart contrats is very difficult i Solidity. The core architectureis significanty lightweight.

Core point: would make sense to do 2 poCs - one on Ethereum and one on Hyperledger

Then test out the construct and compare and contrast.

Then a few other SC related start-ups coming. These 2 should be sufficient.

This tech choice will drive some of the design considerations for some time in the future.

Comments?

MB agrees doing something on >1 platform wil help illustrate the distinction between conceptual and physical model concepts.

See Barclays implementation example - on Vimeo.

http://r3cev.com/projects/

Ken Traub: Uses the R3 “Blockchain” system which is not really blockchain. Illustrates the template idea we talked about.

SS: At some point down the line we have to consider where is the contract stored ie. the language of the contract - consider whether this is stored distributed or centralized; whether you want to store a hash of the contract and capture some data points. Would not want to store the entire legal language of the contract.

Fiancial community needing to come with some norm about the answers to the above - where you store the contract and where you store the business logic and the data and where you execute the business logic.

Do they aspire to standards? Probably

How many things that look like standards are emerging right now?

- hard to tell, lots of things that look like standards

But de facto standards, would tend to have consortia behind them.

Likely to see stds emerging from FI consortia.

Also Hyperledger (not finance specifically) - more technical focused

Something also happening in E3C but likely not financial.

W3C likely focused on the patterns, conceptual and architecture?

Probably use of BC focused on digital publishing.

As with all W3C events there is an extensive archive - there was a thing over 2 days recently. Can look that up.

This also relates to the emergence of architecture for Internet of Things.

See also IBM - worked in IoT apps for Blockchain already!

Uses the notion of Things (smart devices) that might have many different aplications. Public ledgers might mediate these things so that no one company would need to retain ownership of the thing. Probably not closely related to FiServ related ontology stuff. More like messaging systems among things on the Web.

The word Blockchain is starting to be applied to anythign that involves sharing data between 2 or more parties. R3 is a good example, really just peer to peer messaging. Really just about replication across multiple servers.

So again a lot of this is reinventing existing stuff, as we saw with XML.

Whereas with XML we had messaging with data; here we have the concept of groupings of data.

A good context would be finance.

What would it take to do a PoC for ethereum and a PoC for Hyperledger? With common semantics

PR: Starting point: some semantic representation of the features of such things that can the be realized in each platform.

So we start there.

Pick one of the prevalent Ethereum or R3 things.

However there is very little publiic about R3 that we could draw upn.

Take that and identify what we could abstract up to the model as Pete suggests above.

Action 1: watch the video (link above0.

Can we do a conceptual model of the video alone.

CB: Out there, includign R3, they are marching across different asset classes, trying to represent them in some kind of standard ontology e.g. ISDA for Swaps. They are then trying to test out the quarter “Blockchain” to see how the messages, communications and state changes of that asset move between the constituents. They are doing this now for:

Swaps Commericla paper Syndicated loans

not doing this in isolation there are other platforms e.g. Digital Asset Holdings who are running down the same path. THere are differences between these e.g. DAH thinks more of the info should be controlled by internal parties whereas Quarter seems to want to express the complete asset in the Blockchain.

This is where EDM Council has a potential role. Not the only construct to describe an asset (Identity being another, notable requiremet). There are others working at a higher meta layer. So FIBO describes the asset at a detailed level. It is silent on risk calcuations and cash flow calculations.

These need to be calculated in a standardized way on the fly. For example VAR calculation. Cashflow for DCF calculation.

So there is a process component to this.

Is there already a standard way of doing cashflows and things?

There is ACTUS and the upcoming OMG discussions on possible standard for cashflows standardization.

All regulators have named fields on which to base the VAR calculation but is there a certified proven way in which to standardize the calculations themselves?

CB: The Contract metaphor is a bit limiting. The power is where the contract starts interacting in the financial or healthcare ecosystem. CB models this by defining each contract as a microservice which interacts with both Blockchain and off blockchain infrastructures.

One of the issues of talking of smart contracts in an actual blockchain. because it's decentralizzed these cannot trigger activities in th real world. they can trigger payments only in cyptocurrencies.

What the contract part can do is memorialize the contract details.

Things like R3 have more flexibility to build in the execution part of things. Is this what CB is seeing?

CB yes, participants, by beign in the network themselves, are allowing themselves to be part of the process. Recent example, was isolated from connecting to particular rails at the banks e.g. access to this or that kind of account. See JPM recent exaple, trading CP across counterparties, trading th CP for Dollar value, among JPM and a group of their clients - so in that context you could open up the acccounts and then there was an execution component.

So some participant decides they can take their order from the BC - then you can view the BC as a means to place some orders.

Specifically JPM were using the Smart Contracts for the execution mechanism - becomes the arbitrator for the state changes So all state changes recorded on the blockchain

Was there code in the BC that can be executed?

Yes.

These are very simple use cases. They are not describing the entire contract. Consider distinction between describing the whole contract versus just identifying the thing.

What a SC really does is simply that when a new txn is added to the ledger then the valid preconditions for that txn to be accepted have been met.

Does this carry the data with it?

It is code that acts on the txn.

Where is the data in the txn? This is different in different models e.g. BitCoin txn is a structure which includes the code for the txn and some fields you would regard as data ie parties.

BT: Does this combine code and data in one chunk?

SB this is not necessarily the case in Ethereum you essentially create - for example you can create for a syndicated bank loan, the code which calculations the interest. In Hyperledger you write and go. These are business logic embedded in the Smart Contract itself. so you want a txn that creates the thing - you create the SC then other things can talk to that (I may have this wrong - MB); in other e.g. Eth or Hyp, there is a 2 step process, you create the smart contract 1st, then others say if thy agree with the SC. IF all agree with the contract, and sign with their private keys, then it become immutable. It can't be changed without them signing it again. Now this thing can't go out and fetch data, but once the data is inserted into it an a message is there, it will calculate interest in the way the logic is written.

KT answer to BT question - this varies from platform to platform. Regardless of whether they are packed together or not the purposes of the SC is that, the system is recording a time ordered series of txns and coming to consensus on that. For each txn to be accepted there are preconditions to be met and things are calculated that are a result of accepting that txn, There are preconditions and consequences of things. Whether the code is sent in to the BC or is already there and implicitly referenced, the outcome is the same. If it executes without failure then that txn is accepted into the ledger.

MB: Is this a fair statement? SS: I would separate between the txn and the Smart Contract. Reason: there could be a SC to which I could send a contract, and that is a valid txn but the SC access control does not allow me to all that function. So the txn is still valid from the perspective of the network (Etherum). So, every interaction with a smart contract is a txn. SC does not validate the txn; the txn is validated by the network and is passed around by the network, SC says this is the method, an the guy who is calling me is authorized to do so, there are parameters he needs to pass. if the parameters are not right the method called will fail. So this is a distinction between txn verification and txn implementation.

A txn is not accepted ont othe ledger unless a smart contrat succeeds. if a txn is not well formed it is rejected eg if syntactically valid. When saying valid talking of more than well formed, it defines conditions for a txn to be accepted onto the ledger.

How does the person putting these things onto the BC know it's valid or not valid?

THat differs between implementations. Bitcoin has a stack which gives the needed structure of the txn . In Eth this is done differently. This differs among networks

BT th BC may be prompting or the next bit of data is needs?

No BCs don't prompt for anything the BC is just a record of completed txns.

SS: To answer this, if anyone else creates a smart contract on e.g Eth or Hyp, and wants me to interact with that I need 2 things: the unique ID of that SC so I can instantiate is before I can call any of its methods. And I need the API structure of that. If I have all that i.e. if I have the full construct, then only can I instantiate and then call that thing.

KT: This applies to Ethereum but not to BitCoin.

BC is not really a platform where people are using SC.

No-one in Finance is likely to be taking the BitCoin protocol and creating a leger. Maybe there are other protocols laid on top of that but purely using BitCoin no-one is doing.

so Ethereum and Hyperledger is where we should focus.

CB: not necessarily; there are orgs working on exactly this. In the BitCoin bockchain.

However where they are doing that they are maing very light use of the SmartContract feature.

Some of the other networks may differ in how the SC is referenced and accessed. What is true across all the implementation is that the system hold and ever growing list of txn and that there is a piece of code that indicates success for a txn and that piece of code is what we call the smart contract.

How hard for us to do a txn in Ethereum or Hyperledger and see how this actually works?

We can just get the code from GitHub and put it on a server e.g. Ubuntu.

- for both?

- easier with Ethereum ,whereas Hyperledger is shipped with some virtual machine, so their hings is wrapped in that which makes it hard to deploy that thing.

Can use AWS. Need to take every step and execute those steps into an Ubuntu server based on AWS.

Can we schedule a demo for this?

Yes. Subhankar will do a demo.