2016-11 (November 2016) Meetings

This page records the Discussion Group's meeting notes for November 2016. We meet **Tuesdays** at 7:30am PT / 10:30am ET / 3:30pm UK / 4:30pm CET and **Thursdays** at 11am PT / 2pm ET / 7pm UK / 8pm CET for 60 minutes. US times are normative during daylight saving time changes. We use Kantara Line A (US +1-805-309-2350, Skype +99051000000481, international options, web interface, more info, code 4022737) and http://join.me/findthomas for screen sharing. See the DG calendar for our full meeting schedule. Previous meeting minutes are here: July, August, September, October.

Tuesday, November 29

Agenda:

- Discuss end-stage recommendations

Attending: Thomas, Eve, John W, Eve, John M, Jim

Next steps: What would a follow-on group work on? DG or WG? You'd normally expect a WG to deliver technical specs. Existing group (such as the IRM WG) or new group?

Blockchain has a challenge in that the "center is floating" but it still has one (a silo?). While the name of smart contracts is odd, the concept of joining identities in a legal sense to the code is valuable.

Jim suggests that if we have an identity (that is, start from the identity-centric view), then we necessarily have semantics. The legal layer of transactional semantics is "prose" (as R3 calls it), which allows incomplete statements that can gain clarity and interpretation over time. "Code", on the other hand, must be complete in some sense immediately (modulo machine learning inference stuff). We're saying "an identity" meaning a single digital identity; all identities meet in the meat! (See this...) In legal-land, think of "persons".

```
(sync (relationship (identity (person (meat)))))

-----------------------------------------------

(sync (identities (relationship)))
```

(See the much nicer diagram JohnW sent to the list!)

Do we think the lowest-hanging fruit around our recommendations would be around the identity/smart contracts elements? Could the relationship elements be captured in a smart contract itself? The incompleteness of any contract means there are assumptions that lean on a legal framework. ("Can smart contracts be legally binding contracts?" In short, yes, if you reference both prose and code.)

Use cases that are real for many today:

- Smart home
    - Entities with identities, and their identities
        - Homeowner (primary), family member, AirBnB renters
        - Smart home devices
    - Contract conditions
        - Renters contracted through AirBnB are allowed to access the specified functions of the smart home devices, and only for a limited time
        - Family members can access the specified functions of the smart home devices until access is revoked
- Medical/telematics
    - Entities with identities, and their identities
        - Patient (primary), doctors, nurses (care team), administrative staff
        - Insulin pump, other devices
    - Contract conditions
        - Whoever is a member of the care team can control and access the insulin pump settings
            - Substitute nurses etc.
- Proxy powers
    - Entities with identities, and their identities
        - Mother, toddler, nanny
    - Contract conditions
        - The nanny can legally pick up the toddler from daycare and drive him around town

Looking at PSD2, the bank account is becoming the fundamental unit of identity. Actually, it sort of always was. The notion of an "identity account" came from more monetary notions of accounts.

Proposal: Add identity to the prose+code recommendations already extant for smart contracts. Jim sent this link to a CommonAccord contract.

AI: Jim: Send the Norton Rose paper to the list so we can bash it.

Thursday, November 17

Agenda:

- After BSC-DG: what would be the next steps after BSC-DG? (Working Group?)
- Report writing – look at items that need text.

Attending: Scott S.,Kathleen, Susan, Thomas,

Scott: Kantara should consider Governance for blockchain in the healthcare space; Kantara should look to developing new Trust Framework, that is distinct from the existing Identity Trust Framework (such as FICAM).

Kathleen: In many healthcare communities, FICAM is still used. But there is oppt to move forward the federation authorization that are healthcare specific (as FICAM does not sufficiently cover this). May get strong support from Fed gov agenccies. But need to get to the point that it would be adopted. Also fits wioth other Kantara WG.

Scott: yes agree, there is place for identity federarion framework (e.g. FICAM). Kathleen: there is drive from HSS to ensure patient access is hoinored and empoered. But if a provider wants to tal to Fed Agencies they have to speak FICAM. But need balance of these approaches.

Scott: don;t need to be about identity assurance (e.g. diamond trade example). Paper-based , human intensive, etc. But it still relied on a human-based certification. Kimberley process certification. Paper certificates are the wek link, as they have been forged. So a governnace scheme should be akin to the Kimberley process, but move away from the weak link and use consent management.

Thomas: could Kantara produce an "architecture" specification, atop which we could builtd a governance trust framework.

Scott: yes it would be part of the governance.

Susan: There is project where Identity Providers platforms will be listed at global level (part of mandate for 2030). UN Goal 16.9: identity for all persons on the globe. So having an architecture would help all these folks to understand what identity and blocklchain, and what they are obtaining. In ID2020 there will be platforms that will be developed, but lacking an architecture that can be understood by non-technical people. So an architecture standard would be one item that a new Working Group can deliver.

Susan: technology is moving so fast that may be now is timely to start developing an architecture. There are already groups/companies creating new platforms.

Scott: Kantara needs to reach out to these organizations. There is an org in Germany that gives study grants. GIZ.de: https://www.giz.de/en/html/index.html

Susan: a false document is a false document, so it would be good if can we use blockchain to minimize this.

Susan: news today is suggesting listing religion and demographic fields. So future solutions must avoid discrimination, bias, etc.

Scott: some patient care data lists relgiion. Kathleen: this is only for pastoral care.

Kathleen: Governance to protect attributes (of a person) being associated with service – would be very useful. How does this apply to (tied to) blockchain governance. eg. ability to anonymize your attributes, with verifiability. Scott will bring some these issues into his Identity Professionals WG.

Susan: how can identity of a person not be used against them, how can blockchain play a role. For example: decentralized platform, not controlled by any specific government. Susan: can;t separate architecture from governance from politics.

Thomas: this is good inoput.

Kathleen: choosing one salient issue would make a WG very relevant. Fed AuthZ touches blockchain, so is relevant.

Thomas: no meetings next week.

Thursday, November 10

Agenda:

- Report writing – look at items that need text.

Attending: Scott Shorter, Matisse, Kathleen, Thomas, Colin, JohnW

Thomas: going through report. Asked about MedRec. Kathleen: we need criteria(s) to understand and organize use-cases like MedRec. Thomas: May be we should ask as to which aspects of blockchain can solve issues in use-case (e.g. MedRec). For example: (i) cost-savings/cost-benefit, (ii) streamlining processes, (iii) visibility, (iv) privacy-preservation, (v) economic benefits in creating new markets; (vi) improve/manage provenance; (vii) improve effluence of establishing trust (e.g. do at runtime); (viii) Improved governance; (ix) Fairness (instead of using "decentralized"); (x) Autonomy.

(SEE: in the report itself there already some listed criteria).

Use these criteria set on use-cases like MedRec and others.

Scott AI: MedRech is one out of 10 use cases (of the 10 winners of ONC). Scott will review and do short writeup. Scot take 5 and Kathleen take 5. There are 2 types of submissions.

Smart Contracts definition (thomas). Describe text that Thomas and Susan are writing. Question: can 1 paper contract map to 10 smaller smart contracts and how to express unity of execution of these as a whole. CommonAccord has this notion in-built, but not sure if same is true in current smart contract. Kathleen: 2 examples from health GPRI/FHIR. Headers can have pointers to CommonAccord or OIDs (e.g. that describe policies and enforceable rules). Using this possibly with XACML.

Kathleen: there might be technologies and techniques (Sovrin, Interledger, etc) and would be good if we could capture and explain what's nice about these.

Thursday, November 3

Agenda:

- Report writing – Sovrin Foundation questionnaire answers discussion

Attending: Eve, Thomas, Kathleen, Scott S, Susan

What's the right way to proceed? We don't have a lot of time to engage in a back-and-forth; we should write in our report whatever our analysis is, and if we have dissenting opinions we can attach those in appendices or whatever.

Let's bubble up the reason for Sovrin's existence. The vision is, of course, familiar, with a new technology being introduced to solve it better than before. In May, Thomas asked Chris Allen "How do you get the counterparty to accept what's being offered?" (In this case, it's a relying party accepting a self-sovereign identity.) Thomas points to a different system that leverages blockchain to provide somewhat similar capability, CONIKS: The individual can generate new key pairs, and there's a ledger that records the history of the key pairs over time. Binding the record to a (say) proofed identity is the exercise left for the reader, so IAM would still be needed. It's a kind of key directory that gives correlatability over time of a set of keys. Maybe this, and Sovrin, and certificate transparency, all are different approaches to the "blockchain identity use case".

Eve temporarily climbed up on a soapbox to rant about identity as, in great part, a function of an individual's relationship with an organization (e.g. vendor or whatever). Thomas points out this is in Chapter 2 of his new book! Thus, many attributes/claims that the organization has to store are unique to that organization, and it's inefficient and pointless for the individual to store them in tamper-proof form anywhere else. Susan points out that "self-sovereign" has grabbed the world's imagination, and a lot of it has to do with consent.

A big concern of Eve's is: When we're talking about autonomous individuals, in the cases of what solutions does Alice have to go get an app from an app store or a browser plugin (thinking of things like "Sovrin clients")? The thinking is that *requiring* users to take an extra step is likely to make a solution fail unless some vertically integrated provider (like Apple or Google) builds it in, or some country forces the solution. A big question is: "What does the consumer want?" Does Alice want to install something?

Sovrin does add a unique multi-stakeholder governance model, which mitigates risk well beyond what Ripple could do beyond its four virtual walls.

We do seem to have gained some consensus here on skepticism about the longstanding aims of the user-centric/self-sovereign movement, which we'll have to capture in our report and share back with the various stakeholders.

Tuesday, November 1

Agenda:

- Report writing – Sovrin Foundation questionnaire answers discussion

Attending: Eve, Thomas, John W, Kathleen, Susan, Jeff S, Andrew, Alex, Adrian

Logistics: Today marks four months out of six in this DG's journey.

Smart contracts vs. legal contracts: How has this difference been articulated? Barclays has written a paper, and we've discussed it some (need for jurisdiction information and formal identification of parties). The MIT event had some discussion as well, with Bart Suichies' comparison table

(was that distributed to the list?). Where does the role of consensus come in? Any delta is relevant to our report-writing, especially as it relates to identity. Scott D has the action to write about legal contracts. Thomas listed four elements: parties (majority have 2), terms of the contract, consensus/verifiability (other parties can independently check whether the terms were executed on), semantic connection between legal prose and machine-readable code.

Do the elements of (machine-readable) access control constitute a machine-readable contract? Lots of machine-readable authorization policy languages either could be (and/or or) easily translated to, or constitute themselves, a near-natural language declarative semantic description. Could they be "taken to court", that is, could they be validated in a way that is traditional for legal contracts?

How does Jim H envision (or actually implement, by now) the connection between the legal contract text in CmA and the smart contract code? What if one half "blows up"? How does the regulatory regime under which the contract operates get identified? Have smart contracts been operating in such a gray zone that they've been trying to set totally separate standards that add a different and possibly even bigger risk? Could civil law standards usefully be created to mitigate this risk?

Thomas and Susan took the assignment to flesh out the Smart Contracts definition and analysis in the report. This section should link to and discuss the CmA connection, and, where it can, talk about parties in their "identity" guise.

Sovrin answers: You can find them in your inbox or in the email archive. See also the paper Thorsten mentioned in email.

Discussion of the "Different approaches being taken in the new solution space, e.g. if other approaches are being taken outside of Sovrin" answer: Adrian attended IIW and the Sovrin-related sessions. Sovrin came across as "one of only four standards-track efforts that are alternatives to federation". You can use the private key you get as part of your identity to sign things. Evernym has basically become Sovrin now, having donated the code to the Foundation. The technical part of the model seems identical to the Blockstack model, and then there's a governance model on top that adds permissioning. The answer in this section talks about other blockchain use cases such as Bitcoin. As for other blockchain *identity* use cases, it appears they have all converged on a single technical answer: Don't put identity information itself on the blockchain (for the usual reasons: security and privacy of PII, latency, bloat); only put pointers on the blockchain; make that pointer model flexible so that that the identity holder can have pseudonyms; identity information is actually stored in a traditional repository of some kind. It's not that IdPs necessarily go away (they're mentioned in the Sovrin FAQ), but they would depend on the Sovrin layer. It's a four-layer model.

Thomas notes that UMA enables a distributed model when it comes to an identity-holder's resources. Eve also notes that OpenID Connect enables distributed and aggregated identity claims in SSO explicitly. Adrian discusses the W3C verifiable claims work as being uncontested as solving the triple-blind concern.

The question is: What, then, is the Sovrin work actually solving, if the current state of the art in identity and federated identity isn't so bad? Is it just that "having IdPs in the world is evil?" (Not that this may not be enough...) For whom is this solution targeted, then? Is the value worth the implementation/deployment cost, and for whom?

AI: Eve: Send her analysis of the triple-blind vulnerability identified by researchers to the list.

AI: Adrian: Send a link to the verifiable claims work to the list.

AI: Thomas and Susan: Work on the Smart Contracts subsection of the Blockchain report section.

Next time: Assemble a final list of comments and questions back for the Sovrin folks to answer, and work on the Sovrin Foundation Case Study report draft section.