Blockchain PSIG Call Notes

01 October 2020

# Attendees

* Neil Aeschliman
* Robert Stavros (Jackrabbit, 569992)
* Mike Bennett
* Bobbin Teegarden
* Ian Stavros (Jackrabbit - 643024)
* Frederic
* Rob Nehmer
* Rencher, Robert J

# Agenda

* IOTA Updates
* RFI for Crypto IDs

# Meeting Notes

## IOTA Updates

### 3 day meeting (summit) this week

MB presentation on standards and presentation

### Other presentations of interest

#### Yesterday – Supply Chains

With Trade Mark East Africa (TMEA)

**Key features**

* Supply Chain / Demand Chain
* Integration issue
* Data Residency issues.
* Private Tangle

Implications for IOTA Protocol Standard (RFC)

* Will need to support private tangles
* Will need to know if these use or require Coordinator under IOTA vs
* RFC will include conformance points for this kind of implemetation

**Features to look for on this:**

Neighbor Node Discovery IOTA v1 was manual / social networking.

IP at the moment.

IOTA v2 (Coordicide version) has autopeering (node discovery and connection is done automatically).

IOTA v2 Submission needs to support Private Tangles

### Aside

Need to be able to support PTs as you would never get the level of testing that is needed for some business use cases.

Testing – there is the Testnet. Nothing goes onto Mainnet (production environment) until it has been tested.

But don’t want to release potentially hostile things onto that.

For later tests of IOTA v2 stuff, we will have incentivized Testnet. Bug bounties etc.

### Private Tangle

Business use case for non repudiation etc. – may often be use case that requires a self-contained network of known trusted participants. This is a trust network.

All done manually. Asked about SLAs – they don’t really have these formally (too many unknowns on the circumstances of a particular node). Given a Distributed Ledger (DLT) is resilient to such variables

They are on IOTA 1 or 1.5 (Chrysalis).

Chrysalis is IOTA 1.5 on current Mainnet – started introducing some of the new Coordicide.

Coordicide – formal specs just out of Research. So IOTA 1.5 has some of those features but written before those were really documented.

Private Tangle (PT): Needs a coordinator.

So

IOTA v2 spec will have conformance points for the things that PTs need:

* Coordinator
* Manual node discovery

Autopeering – seems to have some relation with Mana.

Private Tangle scenarios

* Data residency – geographical context limitation
* Business use case context

Business use case context – also the option of Streams.

### IOTA Access

Just released.

Potential standard.

Protocol description – seems to be suitably separated for a potential standard.

So

We would to do an RFP if we were going to an IOTA Access submission.

**Use case:** IoT / device (e.g. cars) access control.

Gives a means to control who has specific privileges or capabilities wrt to a given device.

Must rely upon – some kind of identity

IOTA Selv – DID implementation

(NOT Ephemeral DID)

**Discussion:** Access would work well with Ephemeral DID – can define the context as being the rules for when someone can access or do certain things with a given device.

Find link:

#### Conclusions

Think about RFP for what Access does

And maybe link to the Ephemeral SSID idea.

### Questions

#### Via chat

BT: I hope the 'private networks' are like blockchain containers?  Would be interesting and has some market 'recognition'

#### What are Blockchain Containers?

BT:

Container concept for M2M and containers that give a private context on the Internet – so you are assured of your security, visibility. Blockchain is an instance of that.

Blockchain – little WANs within the LAN. Containers are the system architecture for that kind of privacy. Like Dockers. Gives a private environment. This might be more of a metaphor.

<https://www.networkworld.com/article/3529384/essential-things-to-know-about-container-networking.html>

#### Discussion

May be useful as a marketing term for private tangles. May want to imitate that. Can then call it a distributed container.

May relate to a thing called Sharding. Shard might be the same idea as Distributed Container.

Note: Sharding in the sense used in IOTA Might or might mean the same thing as sharding term from many years ago. Push and pop from back in the day.

MB: I think it is more like network shear in IRC. But conscious.

IOTA v3 will probably need to be a new RFP. Likely to be non backwardly compatible. This is the one that will support:

* Sharding
* Non IP networking

Q: Sharding – is it done to manage the network (deliberate) due to network traffic with the idea to recombine when capacity allows? (MB: that’s my understanding)

Like a fork – discussion forks between 2 groups of participants.

Seems to be part of the technical architecture.

To post you select 2 things; who do ask to do that (algorithm); based on who you were communicating with locally. Efficiency. This is where Autopeering comes in.

Q: When does a shard become a Private Tangle?

Coordinator was so that the network was not overwhelmed. If you trust the people you peer with.

When do have trust and when you don’t – need to ensure this is covered in the spec (IOTA v3; what about IOTA v2?)

Can have gateways between Private Tangle and the Mainnet and so move currency.

Alternative? To have a PT with a private token that is not exchangeable for monetary value anywhere.

Digital currency: What about private tangle tokens as a self-contained, non-exchangeable (like microcurrencies)

One of the new things in IOTA v2 is UTxO. This supports ‘colored tokens’.

## Conclusion

These are things to keep an eye on with the IOTA RFC

* Think about business scenarios
* Requirements for specific conformance points for specific scenarios

BT: I was going to suggest that when you start describing the complexities of networks of currency vs contracts (messages being the currency), it would be nice to have a micro-ontology of who can do what to whom...

This is one possible outcome of the Interoperability RFI was to do an ontology of these core concepts. Add today’s ones to that.

## Next Week

RFI – Rob to present next week

(assuming Char would not be available that week, for the LETS RFP).

Soon: think about ontology of core Tangle and Blockchain concepts.