FDTF DLTWG Call

Tuesday 16 Jan

# Attendees

* Inessa Collier
* Bobbin Teegarden
* Mike Bennett
* Dan Webb
* Pete Rivett
* Nick Stavros

# Session Notes

## IOTA

Areas being standardized: API and wire protocol.

One of those is coming to the OMG the other through ETSE (see previous notes). Also the platform is being made available open source via Eclipse. This makes three items in all that make up what IOTA consists of.

Q: Are they looking beyond the platform as well?

## Wallets

On an earlier discussion it was mentioned that there was a de facto wallet standard for some cryptocurrencies, and that in general wallets are not standard – so in order to hold a range of currencies you need more than one wallet. Can anyone remember what the de facto standard was called?

Later: this was ERC20. However this is a standard on one Blockchain system only.

### Discussion

on use of a wallet and whether this is something the industry might standardize.

Suggestion: Wallets - like a portfolio.

Inessa: wallet functions like your bank account to yourself. You decide where who when to send money. Not really portfolio in that sense. Doesn't show you history, P&L as a portfolio would.

NS: should we push the idea? Wallet is useless

IC: no it is not.

In terms of the UX, privacy keys, that's a risk.

Suggestion: Is there a need for better tools to manage the privacy keys etc.

De facto wallet standard?

IC: The wallet doesn't hold the ccy it is an address on a particular blockchain. The ccy is native to that BC. e.g. Bitcoin native to the bitcoin BC; can't transfer something to the Ethereum blockchain .

On the Blockchain network you have an address, anyone can see that address (if it's a transparent blockchin). Can enter any address. i.e. etherscan.io - you can put that there and see what current balance, what tokens.

ERC20 tokens. These are the ones used in Ethereum. People doing ICOs on Ethereum use that.

Wallet is your address. Can't have one wallet on the same blockchain that holds Bitcoin and Ethereum.

Also IOTA - has its own tangle. Also Cardano - Ada currency. Neo and so on. Will also host ICOs and people can issue tokens on that.

Issue of holding and exchanging among themselves.

How these interact.

Blockchain 2.0 (or 3.0 now): the idea is to have interrelation between different blockchains. Polka Dot, Efl and others are finding ways to connect and have different blockchains communicate. So you can't force having different tokens on the same platform. People working on that. Have some way of hosting different tokens on more or less the same platform. Or linked together. Problem exchanging. To sell one and get another you go to an exchange e.g. Ada to Bitcoin. Decentralized exchange?

### Exchanges

Q: How do wallet work in the context of crypto exchanges?

A: They don’t:

Exchanges: the exchange does it for you. The exchange holds the ccy for you and they hold the private keys for the wallets.

Can always transfer out - there is a wallet for each token and you can transfer it from that wallet to another one on that exchange or off exchange.

ERC20 is the de facto standard. It is a standard run by Ethereum.

Are others using ERC20? No but others will use something similar. Handles any coin based from Ethereum.

So this raises the question: is ERC20 or something like it, framed in such a way that the same ‘standard’ component could be implemented on different blockchains (and non blockchain DLTs like IOTA)? How or to what extend would we need to abstract or generalize the stuff that defines the ERC20 standard to have a possible standardization proposal? Or is that an unanswerable question?

Can include whatever is based on Ethereum e.g. air miles or anything else. Any token – see conversation from 2 weeks ago about the potential exchange of things other than currency on a distributed ledger.

In order to move an ERC20 token you need to spend gas (part of Ether, the Ethereum native ccy). Similar to how miners get rewarded with bits of Bitcoin for mining. In Ethereum when a token has to be moved, miners have to be rewarded so they are rewarded in the gas.

## Exchange v Wallet v Community

Wallet is like your account. So you might have a EUR, GBP account similarly you would have the ETH, BTC wallet and so on. Each wallet is like each account.

The wallet on the exchange is not "your" wallet since you don’t hold the private key. So this is more like the brokerage.

So the crypto currency exchange is both the exchange, the broker and the custodian.

Comment: there is no insurance for these.

When you buy something on an exchange, transfer it off the exchange to your own wallet OR to a thing called cold storage? Someone operates that and you end up trusting them.

If it is ERC20 send it to myetherwallet.com i.e. you sent it to the Ether network and you are the only one in possession of your private key but it is hosted virtually.

Cold Storage = hardware wallet. Nanoledger and Trezor. Piece of hardware where you send your tokens and you have to enter a pin to do that. Puts the owner in charge. Like a flash drive.

Coinbase only supports 3.

Also most exchanges don't allow fiat currencies so you have to use Bitcoin, Etherum and Litecoin. Also maybe BitCoin Cash.

Use Coinbase and use your bank account to buy one of the 3 or all three.

Bitfinex is the most professional one.

Binance is also popular.

### Back to Wallet Standards Exploration

What kind of thing is ERC20? Is it like an AI or something? We don't know.

Ethereum doing their own i.e. ERC20

Hyperledger one is being standardized through W3C.

At this point we looked at a page showing ERC20 – seems to be a simple enough list of methods or calls or some such thing.

## Community

This appears to be a separate concept that is being explored in DIDO.

DIDO - looking to firm up the notion of DIDO Communities. White paper to follow.

W3C will control and run the Hyperledger organization? Called... we don't know.

Community in the DIDO sense describes the nature of the organization and how it runs its standardization arrangements e.g. IETF.

DIDO Looking for ways of assessing a community and what standards cover a give community if any. Including procedural standards, voting, notice periods and so on. Constitutional stuff.

Constitution and Quality Assurance systems.

Gaps: evaluation yardstick for what that community is like.

Not the same as network since there may be multiple networks in a given community e.g. different application networks on Ethereum.

Need to get a sense of safeguards, risk factors, organizational trust.

Need to see where the discipline is e.g. ISO 9000 for repeatable auditable process.

Hyperledger TSC.