1st

I think the Receipt Timestamp will become important and that we need to say more about it.

Implementers should provide the Receipt Timestamp to the sender when the txn is deemed received by the receiver. In the default data exchange method of EDM, per our new standard 6.3.xx, the Receipt Timestamp is provided back to the sender before the transmission of the data is ended. I recognize that implementers may choose other methods, but we need to make it clear that both parties should know what the Receipt Timestamp is as soon as possible during the information exchange.

2nd

Scenario E, Step 3 brings up an interesting issue.

I send the initial TC at 1PM on Tuesday

At 1 PM on Wednesday I send a Revised TC.

Does the Confirm Deadline clock now begin at 1PM on Wednesday or at 1PM on Tuesday. I believe it begins at 1PM on Wednesday since that is when the latest valid TC was sent. Either option creates an opportunity for gaming the system.

If I use the 1PM on Tuesday as the baseline, I could send you intentionally incomplete or bad data in the initial file so that I have an opportunity to line up some counter/secondary deal before the confirm is real.

If I use the 1PM on Wednesday as the baseline, I could cause continued delays in the confirmation accepted state by sending revisions and continually pushing out the effective date. This would allow me to game the system in another way.

You fell victim to one of the classic blunders! The most famous is "Never get involved in a land war in Asia," but only slightly less well known is this: "Never go in against a Sicilian when *death* is on the line!"  (Princess Bride)

3rd

Under Revised Transaction Confirmation I think we need to say something about the fact that the Confirming Party may assign a new confirmation number to the txn when revising. If this is the case, they should send the original (or previous) conf number in the Prior Transaction Confirmation Number field of the Tracking Data

4th

I think we need a standard that addresses the sharing/exposure of the data exchanged between the two parties. Any single party may elect for their service provider to provide their own proprietary side of the transaction but they can not disclose their counterparty or anything that would lead to identification of their counterparty. This was discussed a lot at the beginning of this request, that in block chain, a lot of information can be viewed. There is also the option for closed and/or private block chain.

Unless I as a seller elect to make it public that I am selling gas at a location, none of my information, including my identifier, should be publicly viewable by anyone else using the block chain technology or the service provider or any other subscriber. This should not create an opportunity for selling of data by a service provider or selling of data analytics unless I agree to be part of that information sharing. This has been mentioned on multiple occasions as an opportunity and I as a seller need the option to opt-out of being part of such information sharing. It could be that, if I elect to do these txns using Service X then, when I sign the agreement with Service X I agree to their use/share/analysis of my information. But that exposure needs to be made clear and the default position should be no exposure.