R3, JP Morgan and Hyperledger compete in MAS blockchain beauty contest. And the winner is ...

The process of 're-imagining' Singapore's interbank RTGS system using blockchain involved R3 Corda, JP Morgan Quorum and Hyperledger Fabric.

By Ian Allison

Updated November 17, 2017 14:51 GMT

The Monetary Authority of Singapore (MAS) and a group of banks in the region have compared enterprise blockchain big hitters – R3 Corda, JP Morgan Quorum and Hyperledger Fabric – in a process of "re-imagining" the interbank RTGS system using blockchain-type technology.

Blockchain is the umbrella term for technology derived from the decentralised cryptocurrency Bitcoin. In a permissioned, enterprise setting this generally means distributed ledger databases with shared memory and no single administrator.

Singapore central bank MAS's "Project Ubin Phase 2" also involved Accenture and a consortium of 11 financial institutions in Singapore: Bank of America Merrill Lynch, Citi, Credit Suisse, DBS Bank Ltd, HSBC Limited, JP Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, Singapore Exchange, Standard Chartered Bank and United Overseas Bank.

This is an interesting piece of research. There have been other large-scale financial infrastructure projects involving different blockchain projects, like the re-platforming of the DTCC Trade Information Warehouse, involving IBM, Axoni and R3 for example, but nobody has publicly gone into much detail about the strengths and weaknesses of the technologies

involved.

Given the candour and detail of the report, **IBTimesUK** took the opportunity to ask the organisers (Accenture in this case), hand on heart, which of the three worked best, and which was the most problematic. Nobody was willing to be quite that frank, however.

It could be said Ubin Phase 2 boiled down to a trade-off between three key factors: privacy, performance and resiliency. Before looking at the exceptional scenarios the test threw at each DLT, it's worth mentioning the key design differences between the three technologies.

R3's Corda is technically not a blockchain; what that statement alludes to is the fact that the system does not broadcast transaction data to all the participating nodes, the way blockchains tend to do. The reason for this is to preserve the absolute privacy of those transactions.

The reputed downside of this is that if data is only shared by two counterparties, and possibly a regulator, the whole system lacks the resiliency of a full broadcast blockchain, and would arguably be lacking when it comes to disaster recovery scenarios and the like.

JP Morgan Quorum is an adaptation of Ethereum made palatable to banks with a 'belt and braces' approach to privacy. Quorum's privacy engine, Constellation, works by allowing smart contracts to be encrypted and distributed to only those directly involved in a transaction. A digital fingerprint of the encrypted smart contract is published to the blockchain and shared among everyone, so all can verify the integrity of the whole system.

In addition, Quorum uses an implementation of Zcash's zero-knowledge proofs cryptography (where the proofs themselves are visible to everybody but what's being proved is invisible). The Zero Knowledge Settlement Layer when applied to Quorum augments the existing Constellation engine to allow cryptographically private settlement of digital assets.

Zero knowledge proofs are without doubt a powerful and exciting candidate for a privacy technology to be integrated into blockchain, but currently have a downside in terms of their computational burden.

Hyperledger Fabric uses a modular architecture intended to allow for pluggable parts to suit a range of multifaceted applications and use cases from finance to shipping and healthcare. It's

foremost an open and general purpose protocol backed by a large consortium of players including giants like IBM.

Fabric 1.0 deals with the problem of data privacy by offering the capability to create channels, enabling a gathering of participants to share a ledger of transactions that are only privy to these participants.

In other words, Fabric preserves the veracity and the integrity benefits of writing things to a chain, but rather than having one blockchain where everyone sees everything, there are lots of different ones where each participant in the channel can see everything in the channel, but nobody else can.

Critics of this design say it works fine in scenarios where you know that the data you are collaborating on will only ever be between that fixed set, but will struggle if other parties were to be brought in on some deal or other. Potential solutions, such as arranging for assets to cancelled in one channel and reissued somewhere else, would probably be rather cumbersome.

So on to the main event. Project Ubin considered how each DLT would deal with gridlock, where payments cannot be settled unilaterally, or where the result is negative net liquidity across the participants and it is not possible to resolve unless additional liquidity is injected to the system – all situations where privacy is paramount.

In terms of privacy, Corda's Confidential Identities transaction amounts were required to enable the "planning" phase of gridlock resolution algorithm. This could lead to privacy concerns in the small prototype of 11 consortium banks, but for a larger payment network, such as the MAS with 63 banks averaging 6,000 transactions, this mapping would be more complex.

In terms of performance and scale, the UTXO model's lineage chain could be "long and heavy", especially after a long duration and many cycles of transactions. In every transaction, each of the Corda nodes will 'walk the chain' to verify each input was generated in a sequence of valid transactions, validating the authenticity of the chain. This can be easily overcome with implementing an expiry to the digital assets. In other words the pledged funds will need to be recycled after a period of time.

Corda performed admirably in a case where transaction(s) were injected into the network during gridlock resolution. Corda can process new payments while gridlock is running, stated the report, while any obligation that is used during a gridlock resolution can be cancelled, or reprioritised without disruption.

Hyperledger Fabric's channels performed adequately in the prototype in terms of privacy. It was in scalability and performance that the design became rather complex to manage.

One key trade-off in the Hyperledger Fabric workstream design is the number of channels required to guarantee high levels of privacy, while achieving gridlock resolution, said the report. Hence cross-channel communication (e.g. movement of funds from one bilateral channel to another) becomes a vital part of the design. At this point, cross-chain interaction is still not supported and is being planned for future platform release.

As a privacy solution, Quorum's Constellation sends the transaction payload only to the involved participants and the rest of the network can only see a hash of the encrypted payload. The key benefit of propagating these hashes to all participants is one of security and resiliency. Should a party to a private transaction require validation of the existence of that transaction at some point in the future, they can confirm this with the rest of the network by comparing it to the hashes that the network holds, thereby not needing to trust the information held at the counterparty.

Perhaps unsurprisingly, scale and performance remains the trade-off, for the time being. It was observed that the current ZKP generation process takes approximately four seconds to generate with a total transaction processing time of five seconds for a fund transfer. There is currently research and development work underway to improve the performance of ZKP algorithms. These include plans to increase proof generation and validation speed and lower the memory