SUTD had the privilege of hosting Sai, Lead Developer of Quorum[1] on 26th October 2018. Sai shared on JPM's history with blockchain **and the upcoming challenges facing adoption of the platform. Blockchain adoption was likened to adopting a fundamental paradigm shift to current technology platforms. JPM intends to maintain full decentralisation of the Quorum platform by ensuring that each node within the system is identical. The primary concern of most organisations would be the need for privacy in transactions hence the focus has shifted to increasing the efficiency of generating zero-knowledge proofs of transactions within Quorum nodes.**

JPM began by exploring the feasibility of use cases for blockchain applications. The key benefit of using a blockchain system would be the increased reliability afforded but with the added caveat of needing to preserve confidentiality in the system, ensuring security and remaining decentralised. But first, Quorum started by allowing the use of comparably more efficient consensus algorithms such as RAFT[2] or Istanbul Byzantine Fault Tolerance[3] and a private transaction manager[4] in order to fulfil the fundamental needs of enterprise applications. Constellation was first built using Haskell but the team is currently working on improving Tessera's[5] **transaction manager to increase zero-knowledge proof[6] generation speed.**

Quorum was chosen as a platform to develop a proof-of-concept for Project Ubin[7], successfully completing Phase 2 and demonstrating the decentralisation of key functionalities in the banking process. The EAF-2[8] algorithm utilised by banks for resolving gridlock while ensuring privacy was implemented with zero knowledge proofs through a collaboration with the ZCash[9] team. In 2018, Project Ubin Phase 3 was completed with a proof-of-concept on interchain settlement through hashed timelock contracts[10].

The importance of network effects in building capability within the industry was emphasised. JPM's efforts included spearheading the Ethereum Enterprise Alliance[11] **and the Interbank Information Network[12]. The steep learning curve in adopting blockchain is the result of ensuring that cybersecurity issues and risks are sufficiently addressed and ensuring transaction speeds are sufficiently high for real-world use cases on medium-sized smart contracts.**

To conclude, the session gave us insights into the uses of private blockchains and the key considerations facing their adoption. JPM's key design concerns would be the need to **maintain decentralisation of the network and improving confidentiality of transactions while taking the lead in building industry-wide capability for blockchain technology.**

Relevant readings:

1. **Quorum - https://github.com/jpmorganchase/quorum**
2. **RAFT - https://raft.github.io/**
3. **Istanbul Fault Tolerance - https://media.consensys.net/scaling-consensus-for-enterprise-explaining-the-ibft-algorithm-ba86182ea668**
4. **Private transaction Manager - https://github.com/jpmorganchase/quorum/wiki/Transaction-Processing**
5. **Tessera - https://github.com/jpmorganchase/tessera**
6. **Zero-knowledge proofs - https://eprint.iacr.org/2017/1093.pdf**
7. **Project Ubin - http://www.mas.gov.sg/Singapore-Financial-Centre/Smart-Financial-Centre/Project-Ubin.aspx**
8. **EAF-2 algorithm - https://patents.google.com/patent/US8725609**
9. **ZCash - https://z.cash/**
10. **Hashed timelock contracts - https://github.com/bitcoin/bips/blob/master/bip-0199.mediawiki**
11. **Interbank Information Network - https://www.jpmorgan.com/country/SG/en/detail/1320570135560**
12. **Ethereum Enterprise Alliance - https://entethalliance.org/**