Provide a short discussion of which solution (using conventional technology, private blockchain, or public blockchain) would be better, and why.

**Brief explanation of each approach:**

**Conventional:**

The conventional architecture suffers from many of the same issues as other centralised systems, being that the clearing house is a single point of failure and must maintain the trust of each of the parties involved. The confidentiality of personal and market sensitive data being handled within this single entity can be considered a security risk. Also, if the internal operations of the clearing house are insufficiently transparent, this can further degrade trust from the participants.

**Private blockchain:**

The private blockchain approach designed in this assignment is essentially a wholesale replacement of the conventional clearing house, with the key features of the clearing house such are payments, CDR transfer, and roaming agreements, replicated on the blockchain. The customer authentication is left off-chain as it was not deemed sufficiently crucial to maintain an immutable history of authorisations to justify the high level of network throughput to deliver near real-time authentication of customers which would be required.

**Public blockchain:**

The public blockchain approach deviated from just replicating the clearing house on-chain due to the higher transparency of on-chain data which it provides. Sending usage information over a public blockchain could lead to issues with commercially sensitive data, as the number of records are linked to a relatively fixed number of mobile network blockchain accounts. At the very least, some information could be inferred from the throughput volumes linked to each account.

For this reason, I leveraged the public nature of the network, and allowed anybody to create a mobile customer (roamer) blockchain account. Anyone can do this, and they can create as many as they want. The account is only useful, however, when it is linked to a real mobile network account with the customers home network, and roaming is authorised by the mobile network provider. Once this is done, the customer has the flexibility to prove this authorisation to any mobile network participating in this blockchain platform and then to sign up for one of their mobile plans. They are then free to use the roaming network services according to the plan entitlements and the charges are forwarded to by the network to the customer's home network. CDR data is sent directly from the authorised users mobile to their home network via web API.

**Which is better?**

The private and public blockchain approaches, if implemented properly are strictly better than the conventional clearing house approach - due to the reasons given in the conventional explanation section. In the architectures which I propose in this assignment, the public blockchain approach is better than the private approach. The benefit of allowing balances owing between counterparties to be netted out with on-chain tokens, reducing the need for financial transactions in real currency is common between the private and public approaches. In the public approach the benefits of the blockchain are most significant for a few reasons:

* Customer value – in the public option we are able to leverage the capability of blockchain technology to give the roaming customer more choice and better value. Instead of negotiating bilateral roaming rates between providers, the customer is able choose the rates based on the available plans.
* Data security – information stored on the blockchain is distributed between many individual customer accounts, rather than grouped under roaming provider accounts. There is no way to identify the home network of a customer account unless the customer requests for a plan and engages in usage on a roaming network. This is needed to enable financial transaction between the counterparty networks.
* Throughput – the public and private approach deal with the issue of data throughput in different ways. The throughput capacity in the private option is higher so more information can be exchanged on-chain. The public blockchain throughput limit (up to 15 transactions per second) would not support the number of transactions required to support a global scale clearing house, so CDR data is shared off-chain. The blockchains is only required for token sharing and authorisation. The benefit of having on-chain CDR exchange is still maintained in that usage data is shared directly from the customer's device over secure http directly with their home network.
* Transparency – transactions can be viewed and validated by a much wider set of agents so the system is much more decentralized, reducing the potential for parties to compromise the integrity of the platform.
* Failure recovery – in the private option, if a blockchain account private key is compromised, commercially sensitive information about their bilateral roaming agreements and rates, and CDR data becomes known to those with access to the key. In the public option, if a network provider’s blockchain account is compromised, only token payment data is revealed. Additionally, if a customer account private key is compromised, only that customer’s data becomes known. In short, the data is much more decentralised in my proposed public blockchain approach.