zID: z5143964
Name: PeiGuo Guan

Answer:

In order to clearly understand the whole architecture, I list the key point of the whole functions and processes here:
HM: Home mobile network
RM: Roaming mobile network

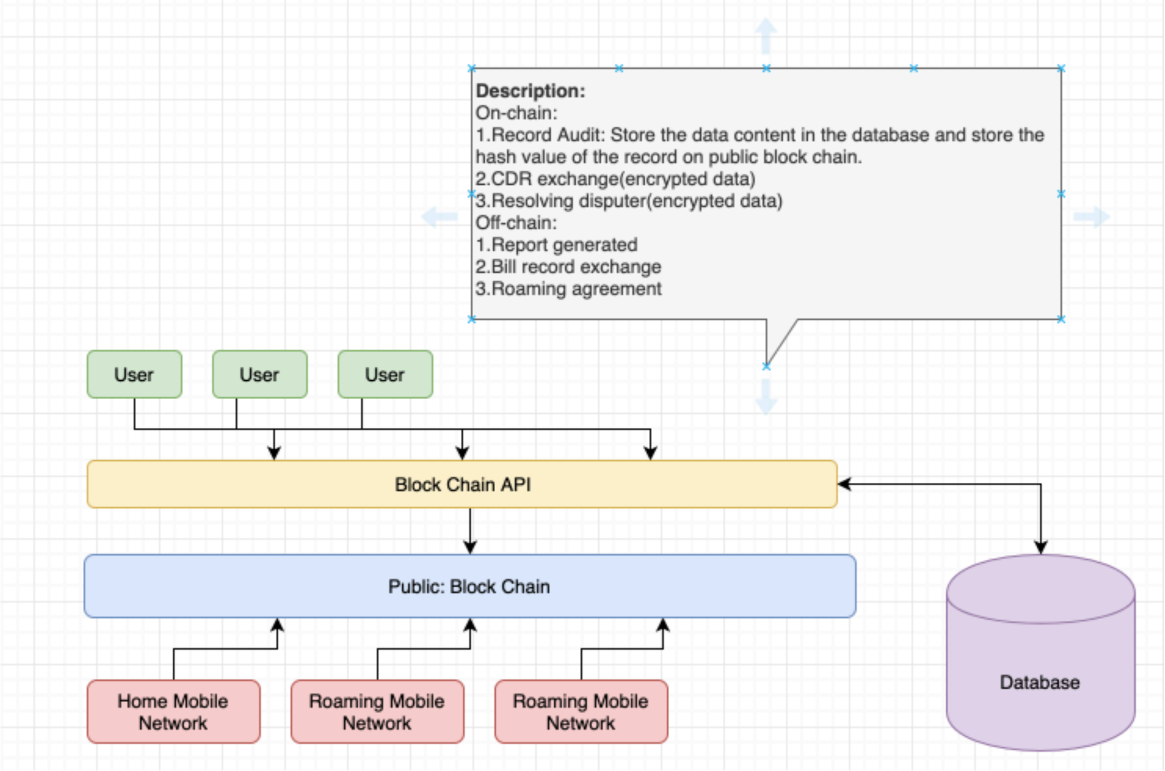
Conventional:

(1) Service provider(HM) makes roaming agreement with another network service provider(RM) if the provider(HM) cannot cover a particular city or country.
(2) CDR is generated based on usage data from switch center. (CDR: Information like date, times, caller, callee, state, code, rate)
(3) Rated CDRs sent to HM and charges based on predefined service. HM and RM partners settle financials monthly based on CDRs reports.
(4) Clearinghouse works as an interface between different RM partners to help them exchange CDRs based on agreements. Clearinghouse receives billing record.
(5) TAP, RAP

Q1:

The blockchain-based method to replace or augment the "Clearing House":

Public blockchain: A public block chain is a permissionless blcokchain, anyone can join the network which means anyone can read and write.



Description:
On-chain:
1.Record Audit: Store the data content in the database and store the hash value of the record on public block chain.
2.CDR exchange(encrypted data)
3.Resolving disputer(encrypted data)
Off-chain:
1.Report generated
2.Bill record exchange
3.Roaming agreement

Description Details:

The record process of users' information should not be on chain, since anyone can read and write it. Although the encrypted data may help to protect the confidentiality, the performance of it will very bad. If we use off chain to storage data, it will cost a lot. So using conventional way is better. By using hash value to generate report and put it on off-chain and exchange between different network.

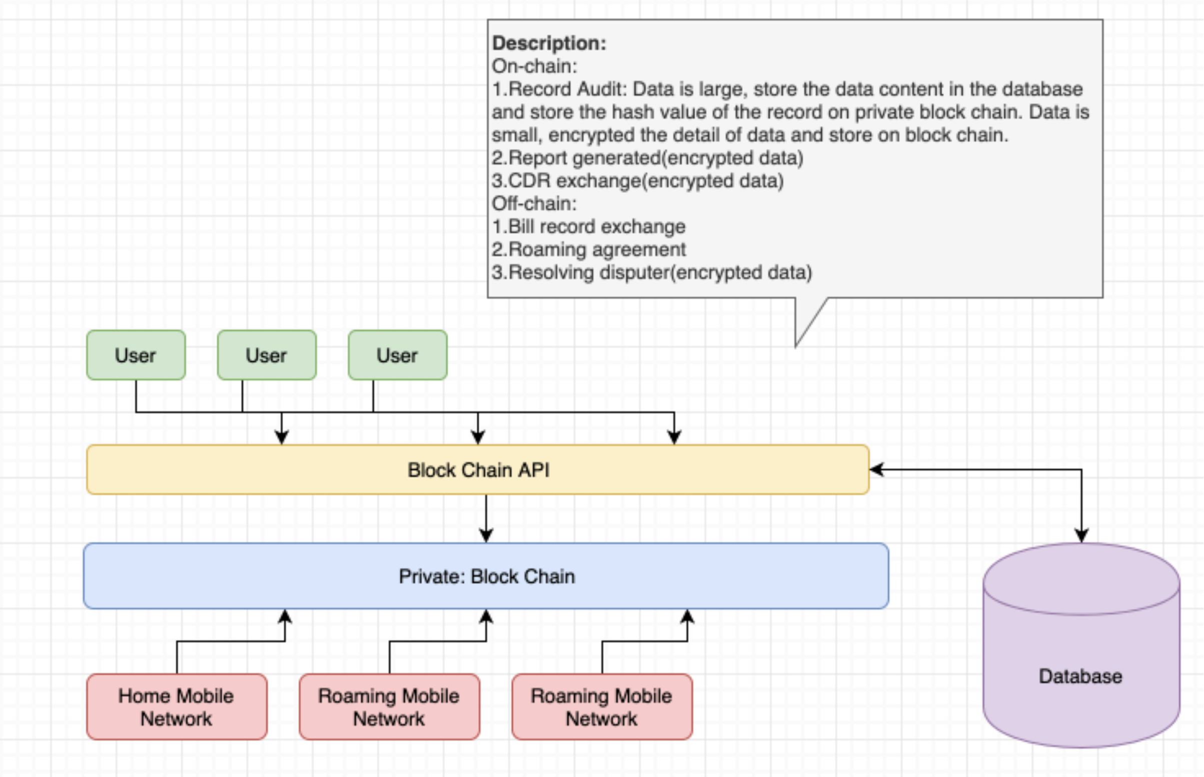
The bill record exchange can use off-chain, since the way of the transaction is more security and it won't public broadcast to the public. In case of on-chain transactions, it is possible to partially derive a participant's identity by studying transaction patterns.

Roaming agreement setup in off-chain, since transfer agreements between 2 parties and it is authorized by third party guarantor.

If the CDR data size is huge, we can use conventional way to exchange data, but this cannot make sure the immutability of data. And if the data size is small, we can think of using on-chain by encrypting the detail of data, decrypted by the private key so as to guarantee the data immutability, integrity and confidentiality.

Since it is public block chain, resolving dispute is the issue between the providers, it can use off-chain to solve the dispute it is security and have more confidentiality.

Private blockchain: A private block chain is a permissioned block chain. In this case, only the home mobile network and the roaming mobile network which the customers currently in are permissioned.



Description:
On-chain:
1.Record Audit: Data is large, store the data content in the database and store the hash value of the record on private block chain. Data is small, encrypted the detail of data and store on block chain.
2.Report generated(encrypted data)
3.CDR exchange(encrypted data)
Off-chain:
1.Bill record exchange
2.Roaming agreement
3.Resolving disputer(encrypted data)

Description Details:

The private block provides more security and confidentiality.

If the data is not that big than we can use on-chain block chain with encrypted the detail like customer list and total number to store the data, since the data should be immutable and confidential and in private block, only the permitted network can join the block chain. Using hash value to generate report of users' information, we can use report generated link number to locate the complete information, so we can put the report number on-chain with encrypted data, only the one who has private key has right to read and write the data.

The bill record exchange can use off-chain based on the CDR information, since the way of the transaction is confidential and the bill is between two parties.

Roaming agreement setup in off-chain, since transfer agreements between 2 parties and it is authorized by third party guarantor.

If the CDR data size is huge, we can use conventional way to exchange data, but if the data size is small, we can think of using on-chain by encrypting detail data, so as to guarantee the data immutability, integrity and confidentiality.

Since it is in private block chain, resolving dispute is the issue between the providers, it can use on-chain block chain to solve the dispute, and only the participants have right to read it so that the history can be recorded and approved.

Q2:

Public Block Chain Scenario:

1.

Name	The confidentiality of users' information
Description	Commercial confidentiality for telecommunication companies
Attribute	Confidentiality
Environment	Normal Operation
Stimulus	Other Network node in public block chain wants to read and write the data
Response	They have not right to change the data
Reason	The data is encrypted and the one who has private key has right to decrypted the data and get the hash value to locate the data.

2.

Name	Limitation of data shared
Description	Commercial confidentiality for telecommunication companies
Attribute	Privacy
Environment	Normal Operation
Stimulus	The roaming network tries to get the complete information of customer lists
Response	The data is unavailable for those roaming network service
Reason	The data shared to the other network is the least, and some of the important data like customer lists are encrypted.

3.

Name	Overload data response
Description	Throughput for accounting reconciliation
Attribute	Performance
Environment	High load
Stimulus	Lots of customers roaming and request in the same time
Response	System has a load balancer to deal with concurrent processing.
Reason	The data is stored in database in a conventional way, and the encrypted index URL is generated in block chain.

4.

Name	Integrity for accounting reconciliation
Description	Transactions only for those by authorized network.
Attribute	Integrity
Environment	Normal operation.
Stimulus	Some node tries to join and change data
Response	The node can join the chain successfully, but it is unavailable to change the data.
Reason	The data has been encrypted, and the hash value can check the content has been changed or not.

5.

Name	Latency response
Description	System builds up agreement within 250ms after user send the request
Attribute	Performance
Environment	Normal operations
Stimulus	Lots of Customers using the phone call in different country.
Response	Systems process the request and build up the agreement with other network service.
Reason	Different Network builds agreements in off-chain which is fast and security.

6.

Name	Information confidentiality.
Description	It is possible to partially derive a participant's identity by studying transaction patterns.
Attribute	Confidentiality
Environment	Normal operation
Stimulus	Some node is studying transaction patterns to derive a participant's identity
Response	Failure
Reason	The information is encrypted and only the one who has private key can get access to the data, and the off-chain data is more security.

Private Block Chain Scenario:

1.

Name	The confidentiality of users’ information
Description	Commercial confidentiality for telecommunication companies
Attribute	Confidentiality
Environment	Normal Operation
Stimulus	Other Network node in block chain wants to read and write the data
Response	They are not access to the private
Reason	The private block chain is permissionless, only the one who gets involved in the private chain has chance to read and write the data.

2.

Name	Limitation of data shared
Description	Commercial confidentiality for telecommunication companies
Attribute	Privacy
Environment	Normal Operation
Stimulus	The roaming network tries to get the complete information of customer lists
Response	The data is unavailable for those roaming network service
Reason	Same as the public chain, the data shared to the other network is the least, and some of the important data like customer lists are encrypted.

3.

Name	Overload data response
Description	Throughput for accounting reconciliation
Attribute	Performance
Environment	High load
Stimulus	Lots of customers roaming and request in the same time
Response	System has a load balancer to deal with concurrent processing.

Reason	The data is stored in database in a conventional way, and the encrypted index URL is generated in block chain on chain.

4.

Name	Integrity for accounting reconciliation
Description	Transactions only for those by authorized network.
Attribute	Integrity
Environment	Normal operation.
Stimulus	Some node tries to join and change data
Response	The node cannot join the chain.
Reason	It is private block chain and the data has been encrypted. The hash value can check the content integrity.

5.

Name	Latency response
Description	System builds up agreement within 250ms after user send the request
Attribute	Performance
Environment	Normal operations
Stimulus	Lots of Customers using the phone call in different country.
Response	Systems process the request and build up the agreement with other network service.
Reason	Different Network builds agreement in off-chain which is fast and security.

6.

Name	Information confidentiality.
Description	It is possible to partially derive a participant’s identity by studying transaction patterns.
Attribute	Confidentiality
Environment	Normal operation
Stimulus	Some node is studying transaction patterns to derive a participant’s identity
Response	Failure

Reason	In private block chain, the participants are all authorized by third party and the information is encrypted and only the one who has private key can get access to the data, and the off-chain data is more security.

Q3:

In my opinion, using private block chain is better, since the home mobile network and roaming mobile network is like partners and some of the transactions and agreement would be more security by using private block chain. Compared with public block chain, lots it has permissionless mechanism, so when the data broadcast to the public, the one without authorized or certification cannot read and write, it guarantees the security, confidentiality and privacy. It also saves the bits size to some degree without encryption. Most importantly, it saves the property of block chain like immutability, safety, and so on compared with conventional way.

However, all of this assumption is based on the data size is not large. If we need to transfer and process big data, conventional way is better, since the performance of the block chain is pretty bad like the latency, throughput, the cost and son on.