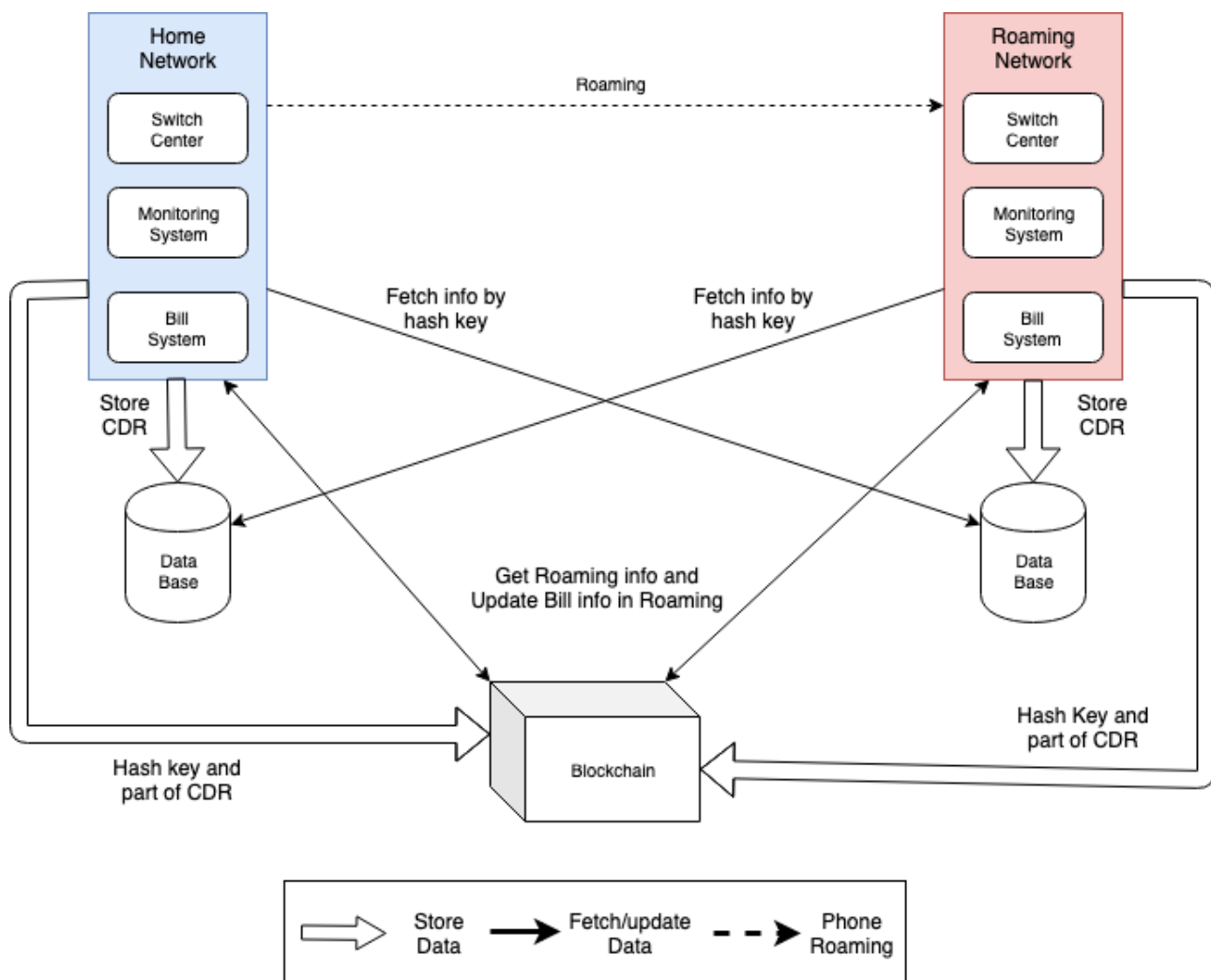


Assignment 2 - Architecture Design and Analysis

Hao Fu - z5102511

1. Design blockchain

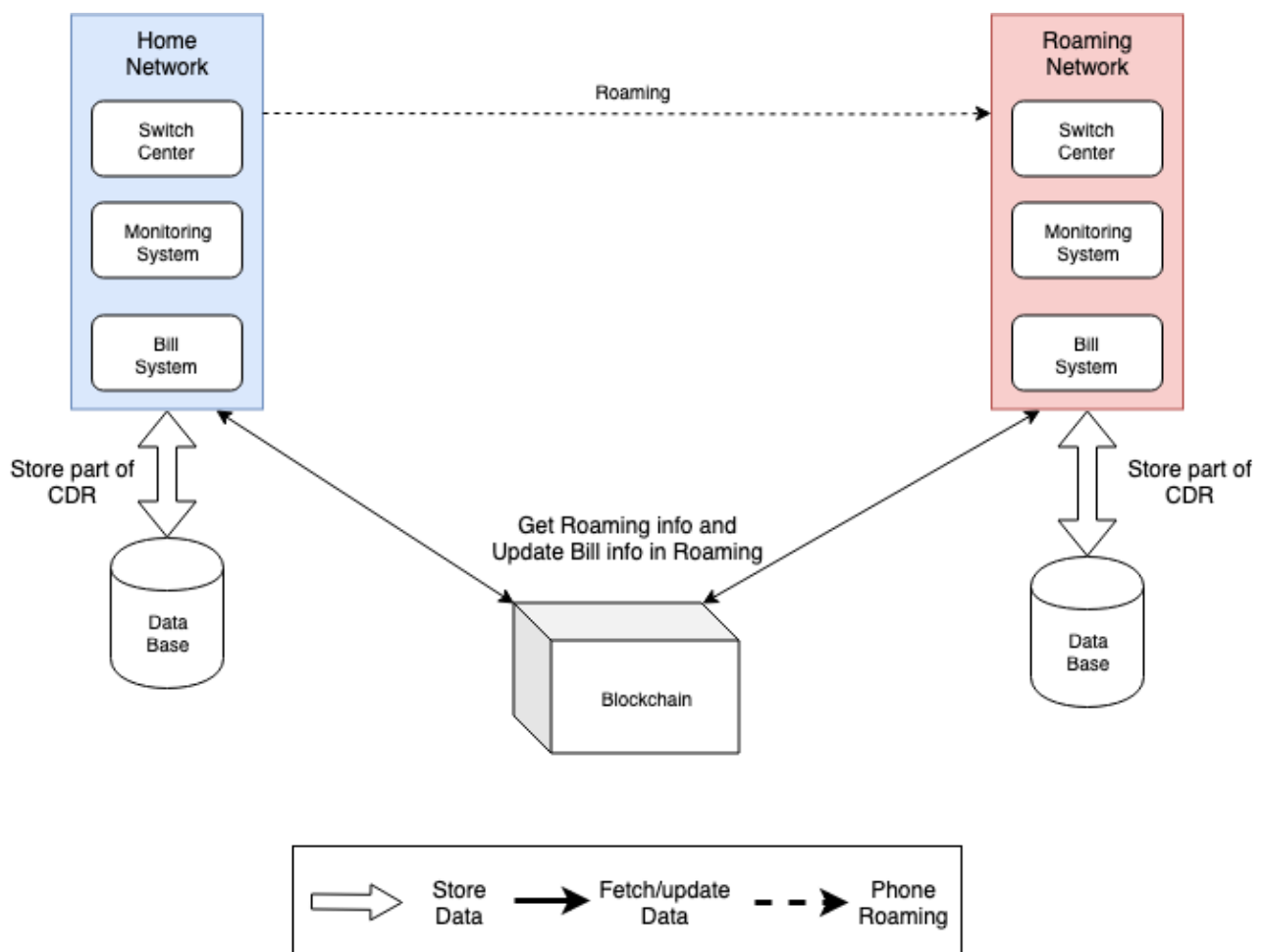
1.1 Public blockchain



For public blockchain to ensure data confidential, we should choose public permission blockchain. We can store the CDR data off-chain in each Network their own database. And put the hash key to the blockchain. The roaming network can fetch the data from home network database with permission. Meanwhile, the number of caller and callee are restricted access for other network. In this way, other network will only able to access the CDR relates with their-self. After the roaming networking got the CDR info, it will calculate bill and update to smart contract on blockchain. Following table show the data storage strategy.

Attributes	On chain	Off chain	Permission
The number of caller		✓	✓
The number of callee		✓	✓
State		✓	
End date		✓	
Times		✓	
Time		✓	
City code		✓	
Country code		✓	
Bill info	✓		
Hash key	✓		

1.2 Private blockchain



As private permission blockchain, we can share more data on the chain and it had better performance such as less latency than public blockchain. But some sensitive data, for example the number of caller and callee, need to store in own database. The remaining data relate with calculating bill info are stored in blockchain. Thus, the roaming can easily calculate the bill info. Following table show the data storage strategy.

Attributes	On chain	Off chain
The number of caller		✓
The number of callee		✓
State	✓	
End date	✓	
Times	✓	
Time	✓	
City code	✓	
Country code	✓	
Bill info	✓	
Hash key	✓	

2. ATAM

2.1 Public blockchain

Confidentiality	Network business info	(H, M) Network will not reveal their info, for example total number of customer, to other network.
	Network roaming info	(M,M) Network will not show the roaming info of other network to target network.
Privacy	User personal info	(H, L) Network should keep user personal info private. Other network should able to access minimal user data to finish the roaming.
	User roaming record	(M, L) User roaming record should only share to target roaming network.
Throughput	Handle Peak Transaction	(H,H) Network should hold 1000 roaming per seconds
		(L, M) Every roaming should be finished in 5 seconds.

Integrity	Bad Network connection	(M, M) When a network issue occur, the data should be resubmit after the network is recovery.
	Authorisation Read/Write	(M, L) For local database, it need Authorisation network to read the data and only self can write the data to database.

2.2 Private blockchain

Confidentiality	Private Database	(H, M) Only data relate with calculating will be share in blockchain, others will be store in Database.
	Data linking	(M,M) Transaction in blockchain should be linked with local database.
Privacy	Minimal personal info	(L, L) Some user info will be store on chain.
	User roaming record	(M, L) User roaming record should only share to target roaming network.
Throughput	High request sending in a short time.	(H,H) Network should hold 5000 roaming per seconds
		(L, M) Every roaming should be finished in 2 seconds.
Integrity	Local data modify	(M, M) The data store in local database could be modify or deleted.
	Authorisation Read/Write	(M, L) For local database, it need Authorisation network to read the data and only self can write the data to database.

2.2 Scenario

2.2.1 SCENARIO - 1

Name	High peak transaction
Description	There are more than 1000 request are happened on the same time.
Attribute	Performance - capacity
Environment	Special event such as new year night.
Stimulus	It might will increase the system capacity and handle the data more efficient.
Response	Blockchain should handle any request no more than 3 seconds.
Reason	In some period, customer might roam quite often. For example, the Christmas Eve or new year night. They might have a roaming call at same time.

2.2.2 SCENARIO - 2

Name	Local data is modified in database
Description	Those data which store off-chain could be modify or deleted.
Attribute	Availability - Data transparency
Environment	Normal operation.
Stimulus	It could add monitor to detect any modify in database.
Response	Detecting modify and delete data on database, and report it to blockchain.
Reason	As a trust authority , it need guarantee the data is immutable and reliable. The Network might want modify some transaction detail in their own database.

2.2.3 SCENARIO - 3

Name	Other network.access forbidden data
Description	Other network might enable access all the data in local database.
Attribute	Security - Confidential
Environment	.Normal operation.
Stimulus	Increase security in the network system.
Response	The operation on database should be denied. Other network should only allow to access the data relate with own network
Reason	Other network might want to access some business info in the network. They may try to access other data on the database.

2.2.3 SCENARIO - 4

Name	Bad network connection
Description	When the Network is poor, the transaction might can not complete.
Attribute	Reliability
Environment	Poor network connection.
Stimulus	Make the whole system more robust.
Response	It need wait until the network recovery then resubmit the request.
Reason	Due to physical issues, the network might be unstable or going down during the transaction.

2.2.5 SCENARIO - 5

Name	Other network could access user data in other network.
Description	Those transaction on chain contain user info, other network might able to get user info.
Attribute	Security - Privacy
Environment	No permission operation.
Stimulus	To secure and guard user privacy.
Response	Denied these user data access request which do not have the permission.
Reason	Other network need user info in other network to promote their products.

2.2.6 SCENARIO - 6

Name	Matching transaction with local data base
Description	Each transaction put on chain had a hash key to match off-chain data.
Attribute	Availability
Environment	Normal operation.
Stimulus	Increase data reliability
Response	Error report and invalid transaction.
Reason	The local database is lost, amount of transaction can not match in database.

3. Discussion

In conclusion, the private blockchain with conventional database is the most suitable structure. Comparing to conventional technology, private blockchain have better confidentiality and data transparency. Using conventional database, the record can be modified and deleted. These data should be immutable as a trusted authority. Moreover, blockchain can provide privacy for customer data. All the transaction are store on-chain which is immutable and offer better availability.

As for public blockchain, the private blockchain have a better performance. Because it can contain more data on chain instead of fetching from other network database. Instead of store hash key on-chain, it can avoid fetching data from other network database. In this way, it has less latency and larger throughput. But more data on chain means it have higher cost.