COMP 6452 Blockchain App Architecture

T1, 2019

Assignment 2

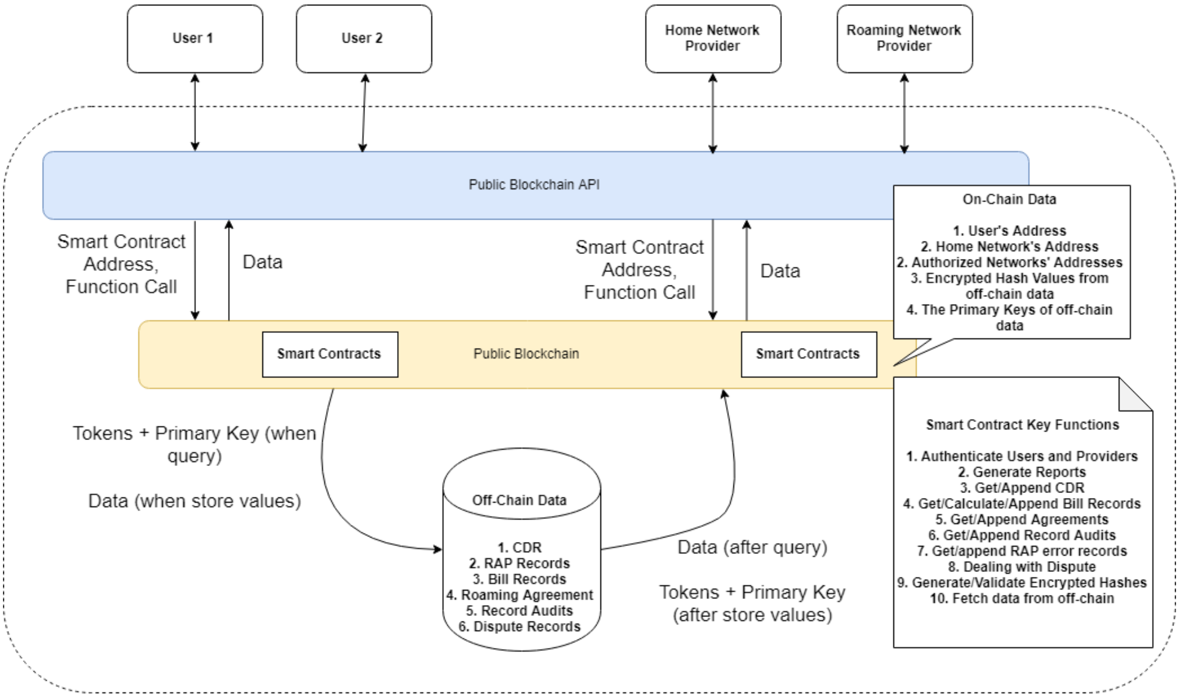
Zhou JIANG

z5146092

School of Computer Science and Engineering

UNSW Sydney

1. Public Blockchain:


User 1
User 2
Home Network Provider
Roaming Network Provider
Public Blockchain API
Smart Contract Address, Function Call
Data
Smart Contract Address, Function Call
Data
On-Chain Data
1. User's Address
2. Home Network's Address
2. Authorized Networks' Addresses
3. Encrypted Hash Values from off-chain data
4. The Primary Keys of off-chain data
Smart Contracts
Public Blockchain
Smart Contracts
Tokens + Primary Key (when query)
Data (when store values)
Off-Chain Data
1. CDR
2. RAP Records
3. Bill Records
4. Roaming Agreement
5. Record Audits
6. Dispute Records
Data (after query)
Tokens + Primary Key (after store values)
Smart Contract Key Functions
1. Authenticate Users and Providers
2. Generate Reports
3. Get/Append CDR
4. Get/Calculate/Append Bill Records
5. Get/Append Agreements
6. Get/Append Record Audits
7. Get/append RAP error records
8. Dealing with Dispute
9. Generate/Validate Encrypted Hashes
10. Fetch data from off-chain

Smart Contract Key Functions

TAP and RAP are in use to exchange information and record errors

- **Authenticate users (customers) and network providers**. Note that a certain identification can perform a certain range of functions in a smart contract. See in " On-Chain Data" section.
- **Generate reports based on CDR, bill records and agreements**
- **Get/append CDR** base on TAP
- **Get/calculate/append bill records** base on TAP
- **Get/change agreements**. An agreement is subject to change once it is expired or terminated. Authentications of relative roaming networks are also changed.
- **Get/append record audits**
- **Get/append error records** based on RAP
- **Dealing with dispute**, including post proposals, agree or disagree, get or append the dispute details, and generating a summary once dispute resolved
- **Generate/validate encrypted hash values**
- **Fetch data from off-chain**, called by other functions

On-Chain Data:

Smart contracts are in use, by which users and authorized networks can get or append data in this system. A smart contract is deployed by home network provider once users' cellphone joins it.

- **User's Address** for authentication purpose. A user address should be unique and bound to the phone number.
- **Home Network's Address** for authentication purpose. A network address is also unique that distinctive to other network providers'.

- **Authorized Networks' Addresses** for authentication purpose. When roaming, an authorized (based on agreements) network address is appended automatically by the cellphone. When leaving the roaming network, the address set to be invalid.

The three addresses can meet the NFP 1,2,4 requirements, by which the commercial confidentiality, data privacy and integrity can be ensured.

- **Encrypted Hash Values** for each property from off-chain data.

  To reduce the **latency**, it should have as less as possible data stored on chain, so only the hash values are stored, not the real values.

  Another is for data **integrity**, as the encrypted hash values are irreversible, it can validate the data extracted from off-chain and indicate whether certain off-chain data has been changed.
- **Primary Keys** of data stored in off-chain.

  Although it is possible to search data by its hash values, it is much quicker to search data just by its primary key. Since the Encrypted Hash Values are longer and will results in more steps for decrypting and hash comparing in query. This will further reduce blockchain **latency**.

Off-Chain Data:

Only authorized parties can fetch off-chain data, which requires tokens and primary key. Once matched, the data can be extracted from off-chain database. Off-chain data also have distributed and hot spare servers. These are a way of **data protection**.

In the off-chain database, the CDR, Bill Records, Roaming Agreements, Record Audits and Dispute Resolve Details are stored. As distributed database systems are in use to store up-to-date values, the **low latency**, **sufficient throughput** can be ensured, and would be better than all such data stored on chain.

As reports can be generated by smart contracts based on CDR, Bill Records and Agreements, it can be made on requests and does not need to be stored. The bill records are also calculated by smart contracts. Also, the dispute details (including proposals, agree or disagree records) can be stored in off-data, but details can be deleted once the dispute resolved (just store the summaries generated by the smart contract functions).

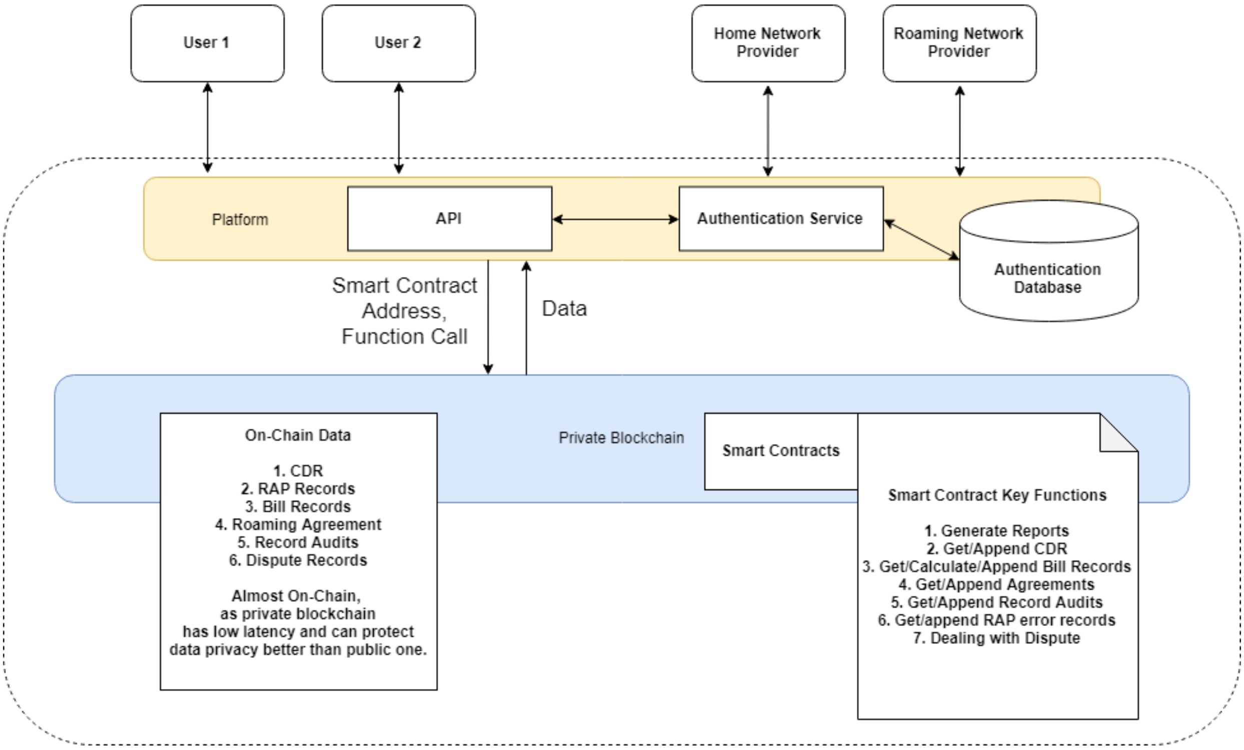
Non-blockchain Components also include:

UI, Client-end apps for users, Client-end apps for network providers

Role:

Blockchain here plays a role of decentralized data exchange and sharing through functions defined in smart contracts. Also, it provides authentication and integrity check functions to meet the NFP requirements.

Private Blockchain:



Authentication Service:

Private blockchain needs authentication service to manage/authorize nodes that can join the blockchain. Every time the API is called, the authentication services response to check the rights. **Note that a certain identification can perform a certain range of tasks in the private blockchain.**

This authentication services have such key functions:

- Authorize a user linking to a home network provider once the user joins.
- Authorize a roaming network provider linking to a home network provider based on agreements.
- Authorize a roaming network provider right to a user if the user is roaming to.
- Revoke a roaming network provider's right to a user if the user leaves it. This is for better **data protection**.
- Authenticate if a user, a home network provider or a roaming network provider has right to query or manipulate certain data.

The Authentication Service meets the NFP 1,2,4 requirements, by which the commercial confidentiality, data privacy and integrity can be ensured.

On-Chain Data:

Smart contracts are in use. Exchange information formats are abided by TAP and RAP. As it is a private blockchain, the transaction **latency** is low. Therefore, all **necessary** data can store on chain, excluding the report, as it can be generated based on other data by smart contracts. The bill records are also calculated by smart contracts based on CDR and agreements. The dispute details always show the latest state (including resolved or not and the summary). Apart from following and authentication, the smart contract has similar key functions to the public ones (see "Smart Contract Key Functions" section).

Off-Chain Data:

No. As private blockchain can ensure quick data transfer, and the immutability can be

Non-blockchain Components also include:

UI, Client-end apps for users, Client-end apps for network providers

Role:

Blockchain here plays a role of partly-decentralized data storage, exchange and sharing through functions defined in smart contracts.

2. ATAM Quality Attribute Utility Spreadsheet

Spreadsheet 1:

Public Blockchain	1	Name	Sufficient throughput for accounting reconciliation
		Description	10000 concurrent requests to handler on hourly basis
		Attribute	Performance
		Environment	Normal Operations
		Stimulus	Hourly accounting clearing triggered
		Response	Systems automatically redirect requests to spare servers by load-balancer
		Reasoning why architecture deals with the risk	
		Distributed servers have abilities to handle massive concurrent workload, sharing the request pressures together.	
Public Blockchain	2	Name	Unauthorized total customer lists fetching attempt
		Description	A network tries to fetch total customer lists from another network
		Attribute	Confidentiality
		Environment	Normal Operations
		Stimulus	A network calls smart contract GetTotalList function
		Response	Systems automatically refuse this unauthorized attempt
		Reasoning why architecture deals with the risk	
		Smart contracts have authentication mechanism that will check if request origin address is allowed to do such task (Total customer lists are not exposed to others).	
Public Blockchain	3	Name	Unauthorized network attempts to fetch users' data
		Description	Another network tries to fetch 1000 users' data that is not shared to it
		Attribute	Privacy
		Environment	Normal Operations
		Stimulus	An unauthorized network calls smart contract GetUserData function

		Response	Systems automatically refuse this unauthorized attempt
		Reasoning why architecture deals with the risk	
		Smart contracts have authentication mechanism that will check if request origin address is part of authorized addresses.	
Public Blockchain	4	Name	A user tries to get another user’s data
		Description	User attempts to obtain detailed CDRs from another user’s data
		Attribute	Privacy
		Environment	Normal Operations
		Stimulus	A user calls smart contract GetUserData function that is not belongs to him/her.
		Response	Systems automatically refuse this unauthorized attempt.
		Reasoning why architecture deals with the risk	
		Smart contracts have authentication mechanism that will check if request origin address is the user’s address (Other users cannot get your data).	
Public Blockchain	5	Name	Unauthorized transaction by another network
		Description	A network attempts to append 5 records roaming data on a user that is not roaming to
		Attribute	Integrity
		Environment	Normal Operations
		Stimulus	When an unauthorized network calls smart contracts function
		Response	Systems automatically refuse the requests
		Reasoning why architecture deals with the risk	
		Smart contracts have authentication mechanism that will check if request origin address is part of authorized addresses (Transaction only appends if the user is roaming to).	
Public Blockchain	6	Name	Roaming agreement changed
		Description	A home network terminates roaming agreement with a remote network
		Attribute	Privacy
		Environment	Normal Operations
		Stimulus	Home network calls smart contracts function to change the agreement
		Response	Systems automatically revoke rights of this roaming network, stopping sharing users’ data
		Reasoning why architecture deals with the risk	
		Smart contracts delete the roaming network address when agreements terminated. From this time, the previous roaming network has no right to get the users’ data.	

Spreadsheet 2:

Private Blockchain	1	Name	Sufficient throughput for accounting reconciliation
		Description	1000 concurrent requests to handler on hourly basis
		Attribute	Performance
		Environment	Normal Operations
		Stimulus	Hourly accounting clearing triggered
		Response	Systems response concurrent requests smoothly
		Reasoning why architecture deals with the risk	
		As private blockchain has less joined parties (compared to the public ones, as it is permissioned) and less time for transaction validation, a sufficient throughput can be guaranteed	
Private Blockchain	2	Name	Unauthorized total customer lists fetching attempt
		Description	A network tries to fetch total customer lists from another network
		Attribute	Confidentiality
		Environment	Normal Operations
		Stimulus	A network calls API to fetch total customer lists
		Response	The authentication services automatically refuse this unauthorized attempt
		Reasoning why architecture deals with the risk	
		When calling API, the API will communicate with authentication services which will check if request origin address is allowed to do such task (Total customer lists are not exposed to others).	
Private Blockchain	3	Name	Unauthorized network attempts to fetch users' data
		Description	Another network tries to fetch 500 users' data that is not shared to it
		Attribute	Privacy
		Environment	Normal Operations
		Stimulus	An unauthorized network calls API to get users' data
		Response	The authentication services automatically refuse this unauthorized attempt
		Reasoning why architecture deals with the risk	
		Authentication services will check if request origin address is allowed to do such task (Not allowing to get users' data if users not roaming to).	
Private Blockchain	4	Name	A user tries to get another user's data
		Description	User attempts to obtain detailed CDRs from another user's data
		Attribute	Privacy
		Environment	Normal Operations
		Stimulus	A user calls API to get another user's data
		Response	The authentication services automatically refuse this

			unauthorized attempt
		Reasoning why architecture deals with the risk	
		Authentication services will check if request origin address is allowed to do such task (Other users cannot get your data).	
Private Blockchain	5	Name	Unauthorized transaction by another network
		Description	A network attempts to append 5 records roaming data on a user that is not roaming to
		Attribute	Integrity
		Environment	Normal Operations
		Stimulus	An unauthorized network calls API to append CDRs to a user's data
		Response	The authentication services automatically refuse this unauthorized attempt
		Reasoning why architecture deals with the risk	
		Authentication services will check if request origin address is allowed to do such task (Transaction only appends if the user is roaming to).	
Private Blockchain	6	Name	Roaming agreement changed
		Description	A home network terminates roaming agreement with a remote network
		Attribute	Privacy
		Environment	Normal Operations
		Stimulus	Home network calls API to change the agreement
		Response	The authentication services automatically revoke rights of this roaming network, stopping sharing users' data
		Reasoning why architecture deals with the risk	
		Authentication services will delete the roaming network address when agreements terminated. From this time, the previous roaming network has no right to get the users' data.	

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

A private blockchain would be better.

- Conventional technology can have comparatively low latency if distributed servers are in use. However, it is fully-centralized and not transparency. In this project, a fully-centralized database may not be trustworthy enough as the conventional databases are not immutable that the data can be modified.
- Public blockchain is transparent and fully-decentralized that everyone can join as a node. All the authentication relies on the robustness of smart contracts, which can have security or privacy issues. On the other hand, as public blockchain need low latency in the real-time transactions, that means some data may store off-chain, which is also a trust issue.

- Private blockchain is transparent, partly-decentralized and guarantees much quick transactions than public blockchain (low latency). A trusted third-party offers authentication service that will be more robust than authentication functions in smart contracts. Then only authorized nodes can join the blockchain. Moreover, as all necessary data is on chain with immutability, it could not be modified arbitrarily.

  Thus, private blockchain is transparent and trustworthy than conventional technology, also quicker and more secure than public blockchain. As a result, a private blockchain would be better.