
System Model (Class Diagram) Document

제 WeekdaysIdea 조

조원 : 201502094 이재호

201704146 박지은

지도교수: 원유재 (서명)

Document Revision History

REV#	DATE	AFFECTED SECTION	AUTHOR
1	2020/05/06	Introduction, Class Diagram	이재호, 박지은
2	2020/05/09	USE CASE와 CLASS 간의 관계, CLASS 명세	이재호, 박지은

Table of Contents

1. INTRODUCTION	6
1.1. OBJECTIVE	6
2. CLASS DIAGRAM	7
3. USE CASE와 CLASS 간의 관계	8
3.1. UC: 시스템 모니터링	8
4. CLASS 명세	13

List of Figure

FIGURE 1 – SYSTEM CLASS DIAGRAM.....	7
--------------------------------------	---

1. Introduction

1.1. Objective

이 문서는 블록체인을 이용한 수목 관리 시스템의 시스템 모델 (클래스 다이어그램)에 대한 내용을 기술하고 있다. 시스템 차원의 클래스 다이어그램과 각 클래스에 대한 명세를 포함한다.

2. Class Diagram

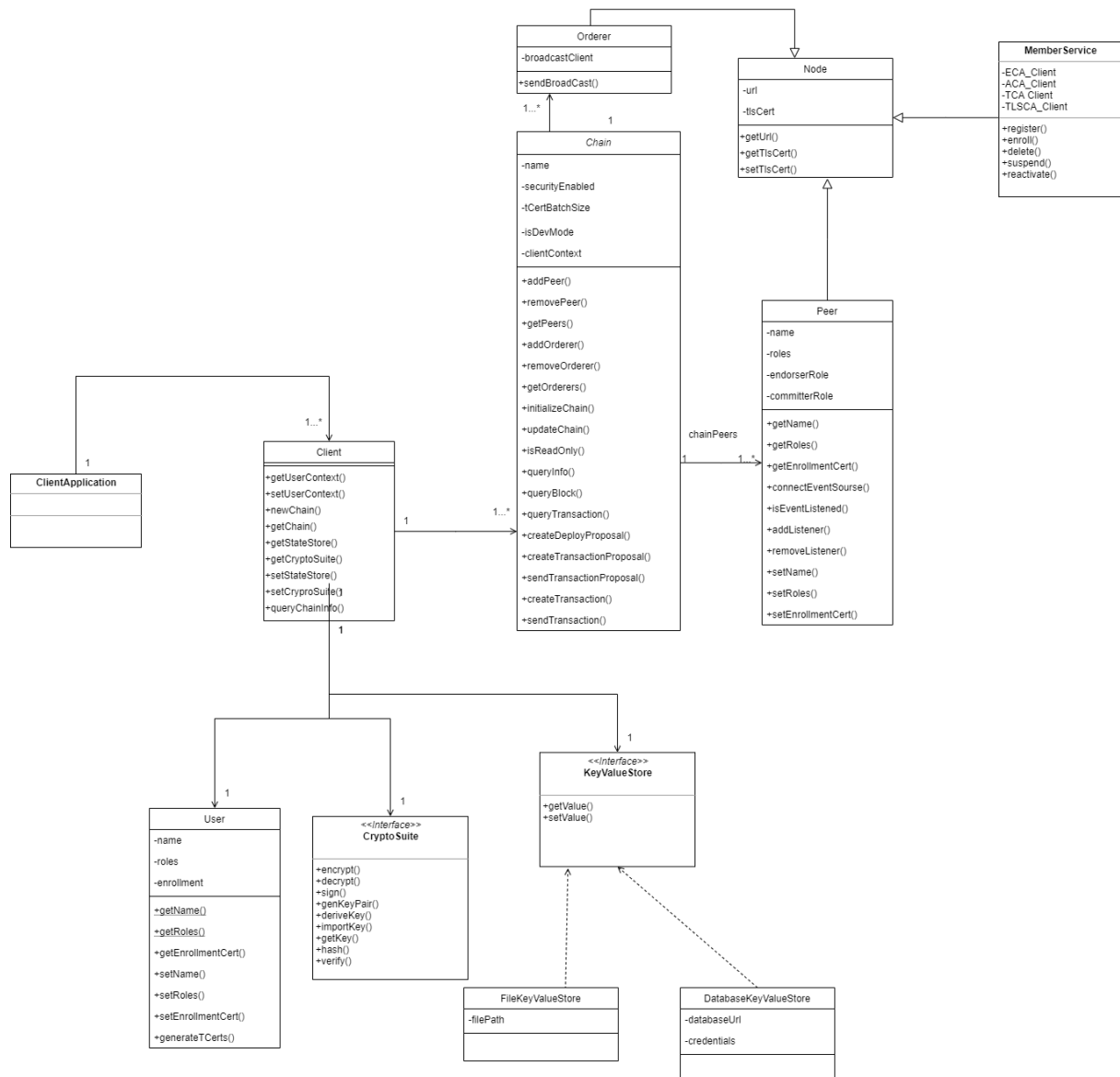
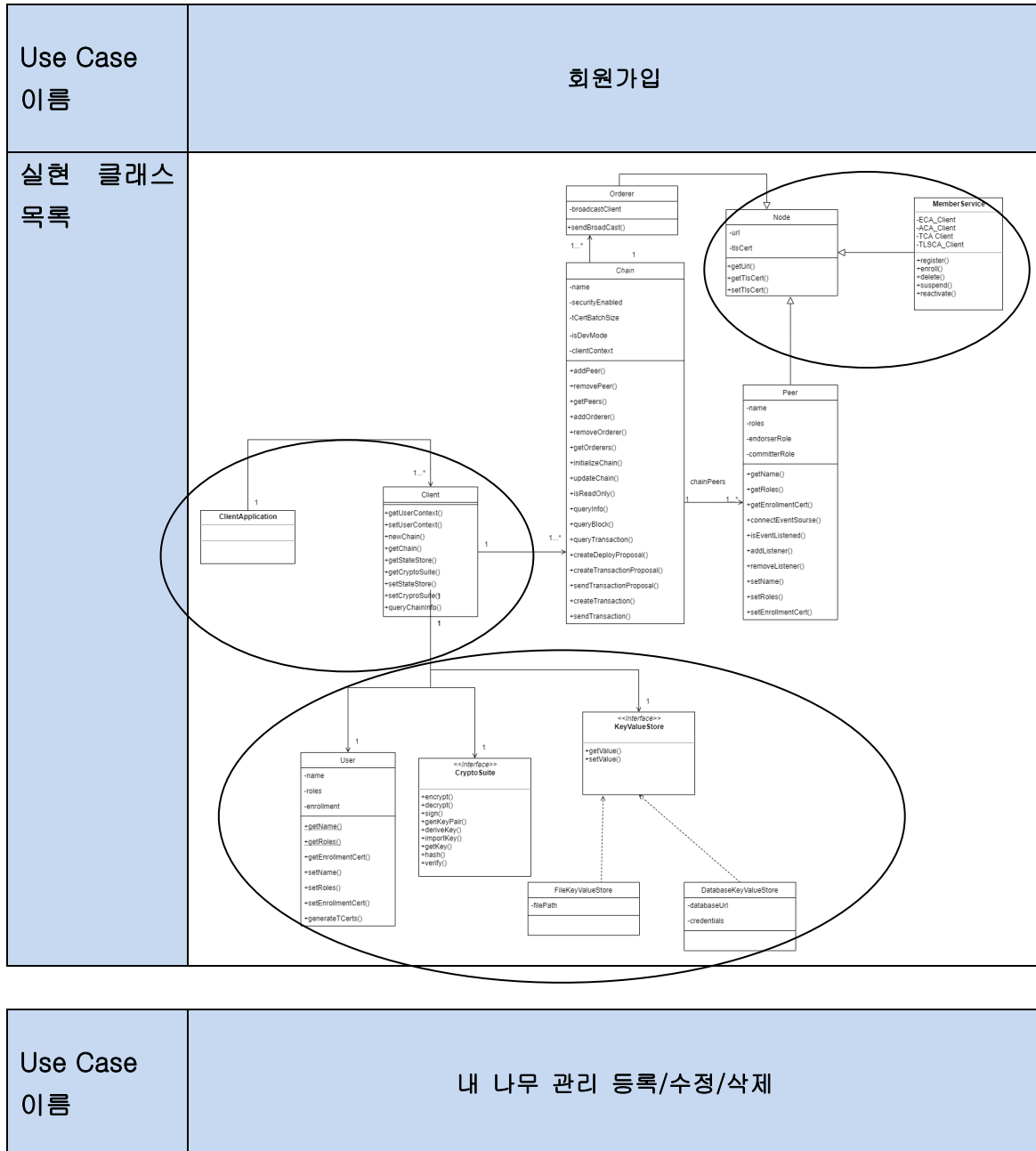
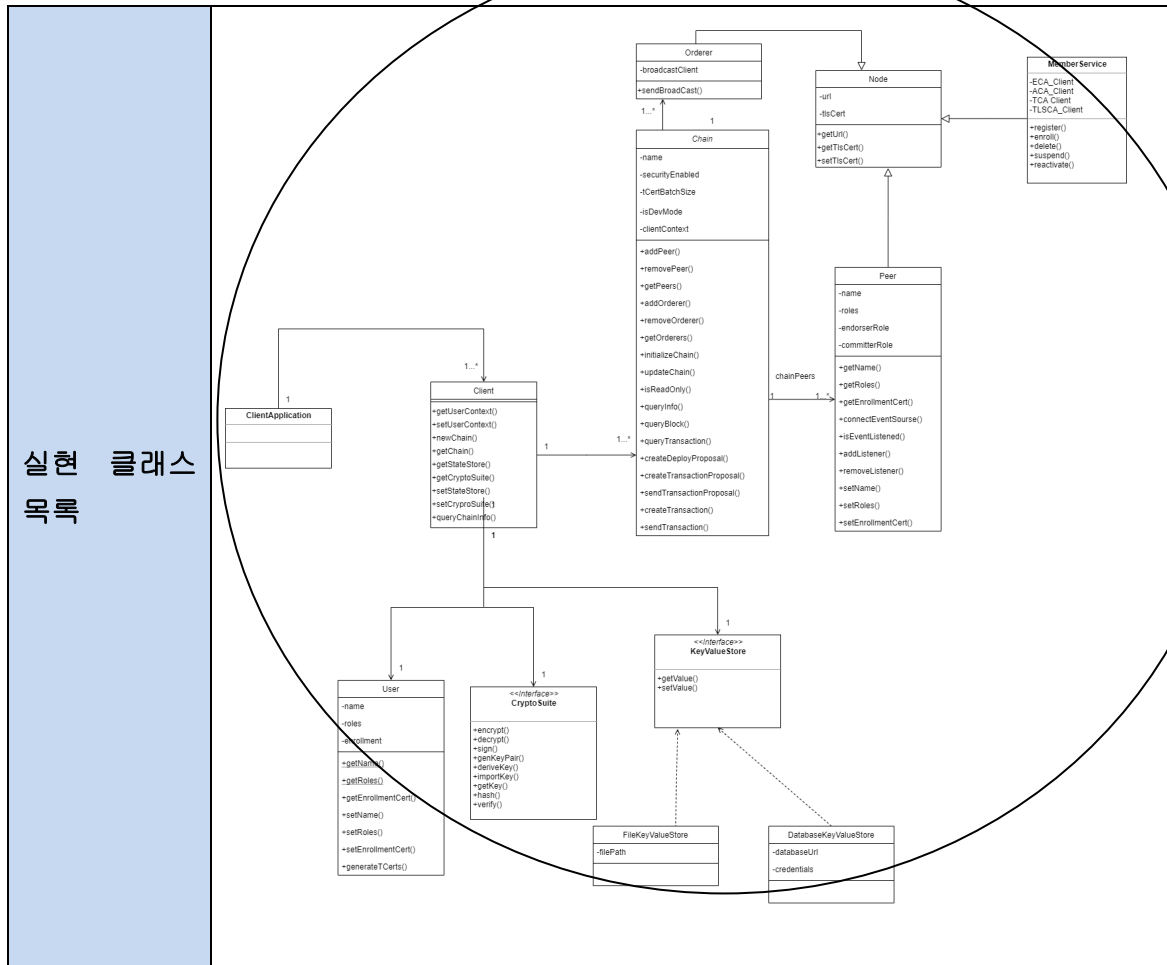


Figure 1 – System Class Diagram

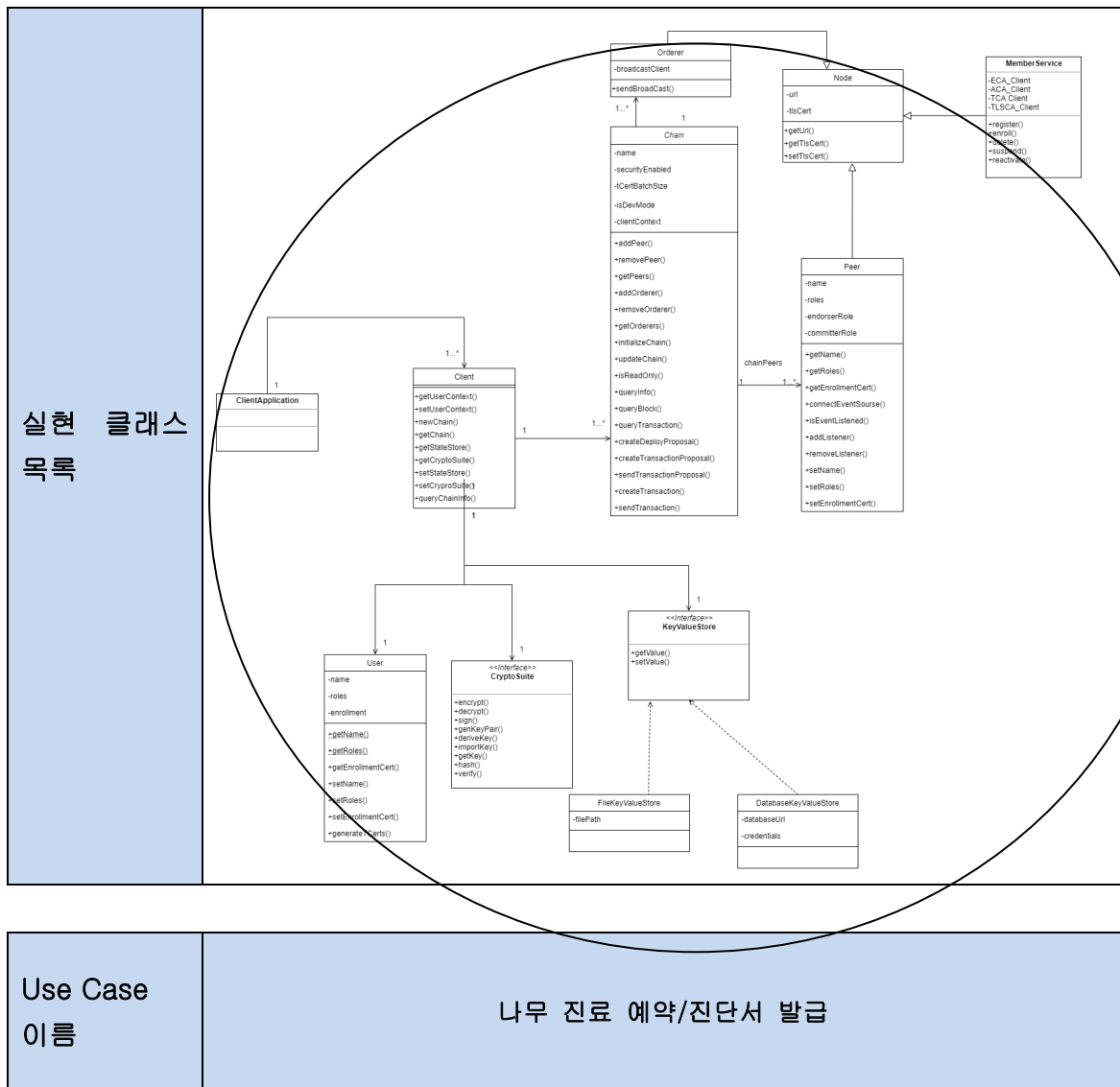
3. Use Case와 Class 간의 관계

3.1. UC: 시스템 모니터링

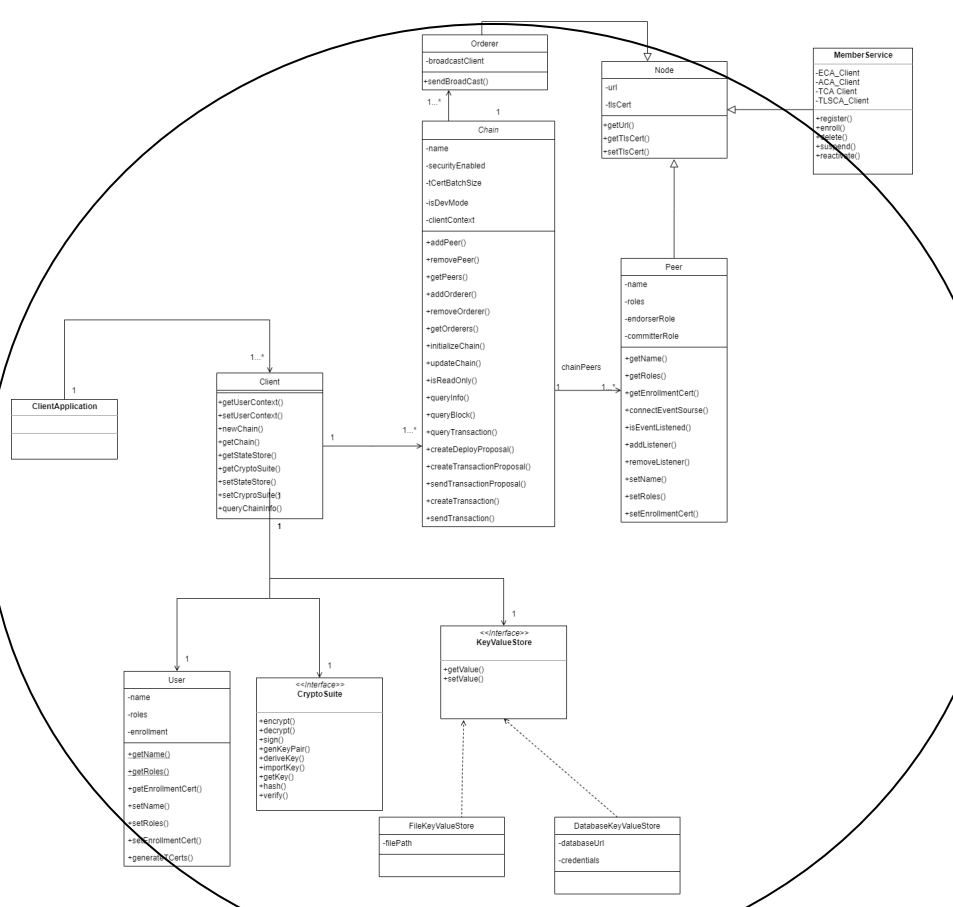


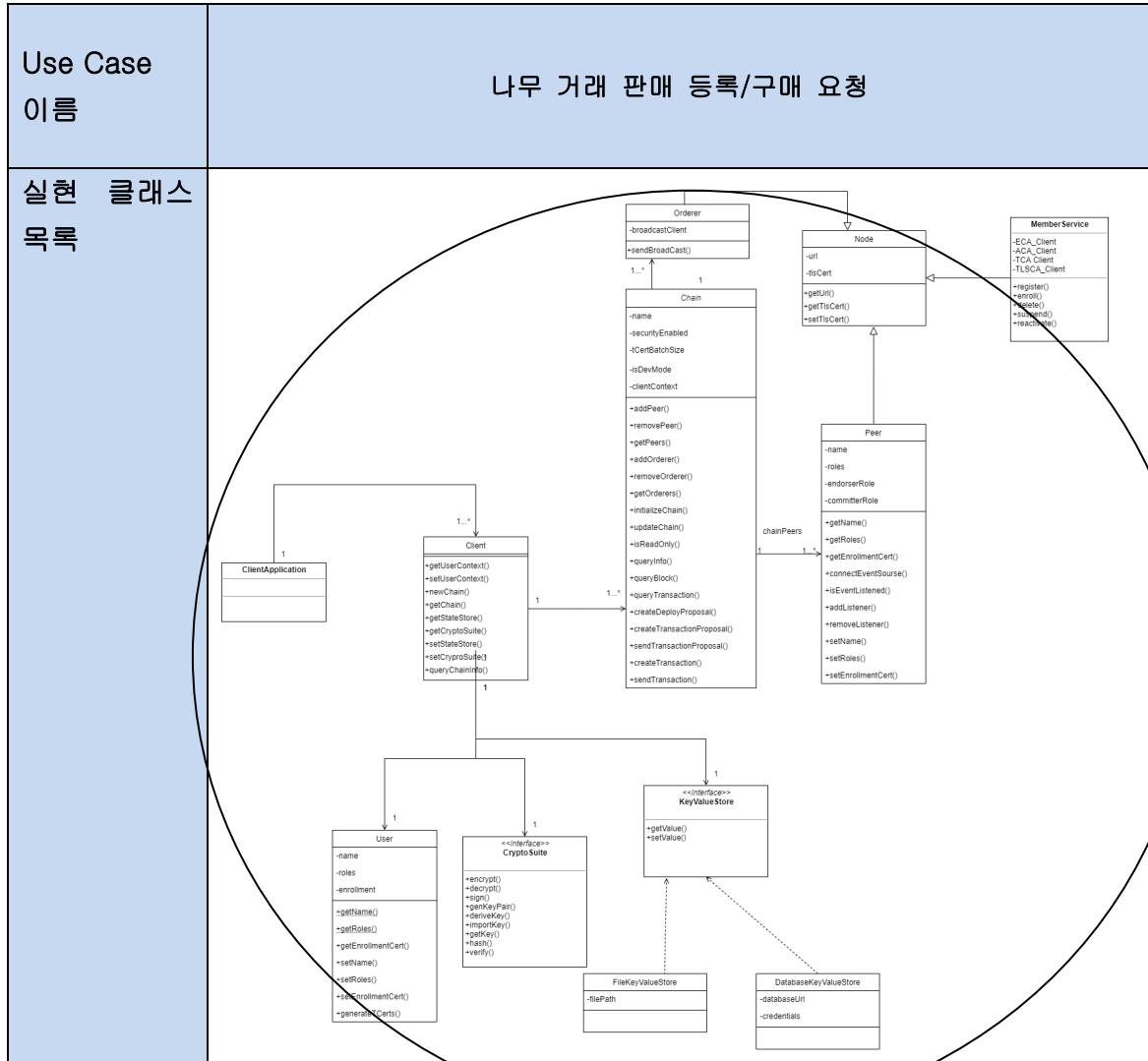


Use Case 이름	나무 정보 조회
-------------	----------



실현
목록





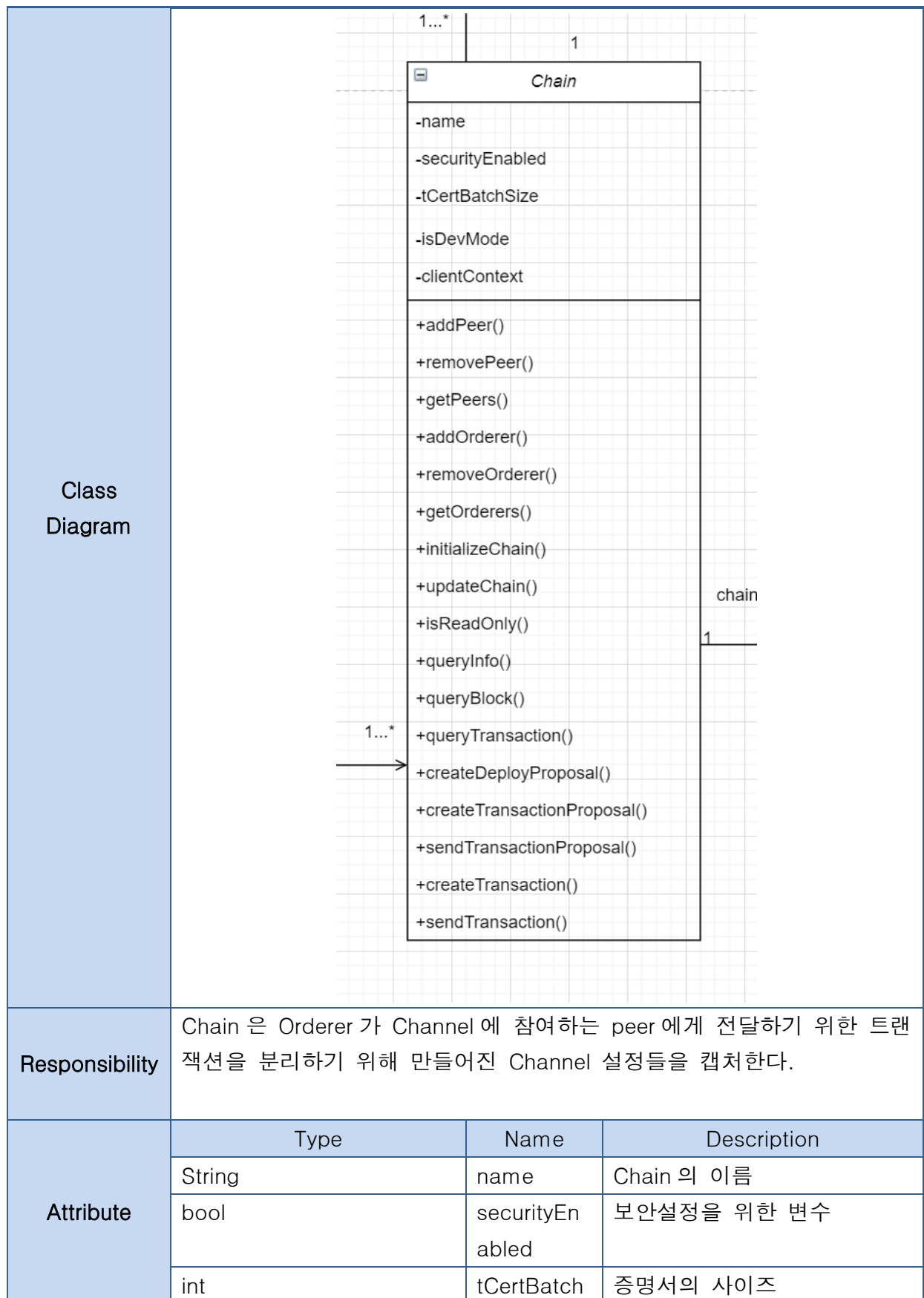
4. Class 명세

[Client]				
Class Diagram	<pre> classDiagram class Client { +getUserContext() +setUserContext() +newChain() +getChain() +getStateStore() +getCryptoSuite() +setStateStore() +setCryptoSuite() +queryChainInfo() } Client "1..*" --> Client </pre>			
	<p>Class Diagram</p>			
Responsibility	<p>사용자의 웹 어플리케이션과 상호작용을 하기 위한 핸들러. 블록체인 네트워크 상의 다른 노드들과의 상호작용 또한 핸들링한다. (채널들을 대표하는) 체인 객체들을 보유할 수 있다.</p>			
Attribute	Type	Name	Description	
	—	—	—	
Operation	Return Type	Method Name	Parameter Type	Parameter Name

		new chain		
	Description	체인 객체를 주어진 이름으로 초기화		
	Return Type	Method Name	Parameter Type	Parameter Name
		get chain		
	Description	world state 저장소로부터 체인 객체 정보를 얻는다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		query_chain_info		
	Description	원하는 Peer 노드의 체인 정보를 탐색한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_state_store		
	Description	여러 어플리케이션 객체의 상태를 데이터베이스를 통해 공유하는데, 이 때, 다양한 저장 방식이 선택하도록 한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_state_store		
	Description	이 client 객체를 사용할 때 상태 저장 객체를 획득한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_crypto_suite		
	Description	CryptoSuite 인터페이스의 객체를 설정한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_crypto_suite		
	Description	이 Client 객체의 사용을 위해 필요한 CryptoSuite 인터페이스의 객체를 얻는다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_user_context		
	Description	이 Client 객체의 security context 로서 User 객체(private key, certificate)를 설정한다. 어플리케이션을 복구해야 하는 경우에도 user context 객체를 사용하여 상태를 복원한		

		다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_user_context		
	Description	권한이 있는 user 객체만 접근할 수 있는 key-value 저장소로부터 key(user 객체의 이름)을 통해 value(User 객체)를 로드한다. 로드된 User 객체의 ECert 는 트랜잭션을 발생시키는데 쓰인다.		

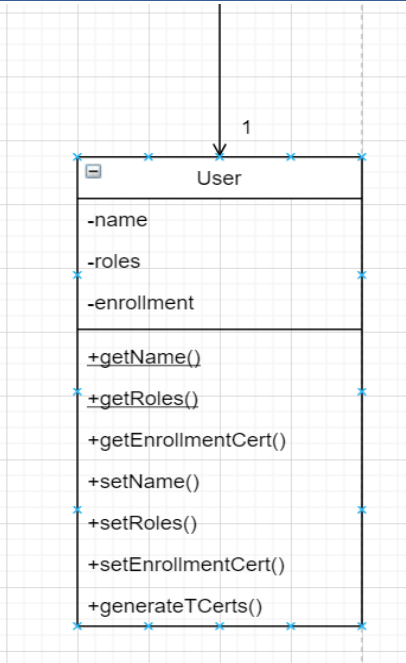
[Chain]



			Size			
	bool		isDevMode	개발 모드 선택을 위한 변수		
	Client[]		clientContext	Chain 에 관여 중인 Client 객체들		
Operation	Return Type	Method Name	Parameter Type	Parameter Name		
		add_peer				
	Description	로컬에서 peer 객체를 chain 객체에 추가한다.				
	Return Type	Method Name	Parameter Type	Parameter Name		
		remove_peer				
	Description	로컬에서 chain 객체로부터 peer 객체를 제거한다.				
	Return Type	Method Name	Parameter Type	Parameter Name		
		get_peers				
	Description	로컬 정보로부터 chain 상의 peer 객체 목록을 얻는다.				
	Return Type	Method Name	Parameter Type	Parameter Name		
		add_orderer				
	Description	로컬에서 chain 객체에 orderer 객체를 추가한다.				
	Return Type	Method Name	Parameter Type	Parameter Name		
		remove_orderer				
	Description	로컬에서 chain 객체로부터 orderer 객체를 제거한다.				
	Return Type	Method Name	Parameter Type	Parameter Name		
		get_orderers				
	Description	로컬 정보로부터 chain 상의 orderer 객체 목록을 얻는다.				
	Return Type	Method Name	Parameter Type	Parameter Name		
		initialize_chain				
	Description	하나의 App 객체가 새 chain 을 만들기 위해 orderer 객체(들)을 호출한다.				
	Return Type	Method Name	Parameter Type	Parameter Name		

		update_chain		
	Description	chain 을 업데이트 하기 위해 orderer 객체(들)을 호출한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		is_readonly		
	Description	chain 상태가 읽기-전용인지 확인한다. (chain 하위의 종료된 channel 은 읽기-전용으로 되어 조회 쿼리만 가능하고 쓰기 트랜잭션 생성이 안된다.)		
	Return Type	Method Name	Parameter Type	Parameter Name
		query_info		
	Description	chain 객체의 상태로부터 height, 알려진 peer 들 등의 정보를 쿼리하여 조회한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		query_block		
	Description	블록 번호를 가지고 블록체인의 블록을 조회하는 쿼리		
	Return Type	Method Name	Parameter Type	Parameter Name
		query_transaction		
	Description	원장을 쿼리하여 조회한다		
	Return Type	Method Name	Parameter Type	Parameter Name
		create_deploy_proposal		
	Description	배포 제안을 생성 : 데이터(체인코드 ID, 체인코드 invocation 스펙 등)를 private key(ECert)로 서명한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		create_transaction_proposal		
	Description	트랜잭션 제안을 생성 : 데이터(체인코드 ID, 체인코드 invocation 스펙 등)를 private key(ECert)로 서명한다.		
	Return Type	Method Name	Parameter Type	Parameter Name

		send_transaction_ proposal		
	Description	생성된 제안을 peer 객체에게 전송한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		create_transaction		
	Description	endorsement 정책에 따라 제안에 대한 응답을 하고, 트랜잭션을 생성한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		send_transaction		
	Description	트랜잭션을 chain 의 orderer 객체(들)에게 전송한다.		

[User]			
Class Diagram	 <pre> classDiagram class User { -name -roles -enrollment +getName() +getRoles() +getEnrollmentCert() +setName() +setRoles() +setEnrollmentCert() +generateTCerts() } </pre>		
	Responsibility	<p>등록 Certificate(ECert), 서명 key 에 의해 등록된 사용자를 대표한다. 등록된 사용자는 체인코드 배포, 트랜잭션(+쿼리)를 수행할 수 있다. User 식별은 App 을 통해 private key(ECert)에 대한 접근을 하여 등록여부를 확인하지만, Peer 식별은 private key(ECert)에는 접근 못하고 서명을 검증하기 위한 certificate 만 가졌다.</p>	
Attribute	Type	Name	Description

	string		name	객체의 이름
	string		roles	객체의 역할
	Object		enrollment	객체의 등록 증명서
Operation	Return Type	Method Name	Parameter Type	Parameter Name
		get_name		
	Description	User 객체의 이름		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_roles		
	Description	User 객체의 역할들(손님, 방청객)		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_enrollment_certificate		
	Description	User 식별을 대표하는 ECert 를 반환		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_name		
	Description	User 이름 설정		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_roles		
	Description	User 역할 설정		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_enrollment_certificate		
	Description	User 등록 certificate 설정		
	Return Type	Method Name	Parameter Type	Parameter Name
		generate_tcerts		
	Description	로컬에서 crypto 로 트랜잭션을 위한 T-Cert 들을 얻는다. 트랜잭션 하나 당 T-Cert 하나가 대응된다.		

[Peer]

<p>Class Diagram</p>	<pre> classDiagram class Peer { -name -roles -endorserRole -committerRole +getName() +getRoles() +getEnrollmentCert() +connectEventSource() +isEventListened() +addListener() +removeListener() +setName() +setRoles() +setEnrollmentCert() } </pre>			
<p>Responsibility</p>	<p>원격의 Peer 노드와 그 네트워크 멤버십을 대표한다. Peer 멤버십은 해당 네트워크 조직 전체를 대표한다. (User 의 ECert 는 유저 개인을 대표한다.)</p>			
<p>Attribute</p>	<p>Type</p>	<p>Name</p>	<p>Description</p>	
	<p>string</p>	<p>name</p>	<p>객체의 이름</p>	
	<p>string</p>	<p>roles</p>	<p>객체의 역할</p>	
	<p>bool</p>	<p>endorserRole</p>	<p>Endorser 역할을 가지는지 나타내는</p>	
	<p>bool</p>	<p>committerRole</p>	<p>Committer 역할을 가지는지 나타내는 변수</p>	
<p>Operation</p>	<p>Return Type</p>	<p>Method Name</p>	<p>Parameter Type</p>	<p>Parameter Name</p>
		<p>connectEventSource</p>		
	<p>Description</p>	<p>모든 Peer 객체는 App 을 위한 이벤트 source 로 여겨질 수 있다. 모든 Peer 객체가 똑같은 이벤트를 공유하기 때문에 App 에서는 chain 상의 한 Peer 만 이벤트 source 로</p>		

		사용해도 된다. 이 메소드는 Peer 객체 하나를 이벤트 source 로 선택하여 App 이 콜백 리턴을 하도록 한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		is_event_listened		
	Description	타겟 Peer 에 주어진 이벤트에 대한 listener 가 최소 한 개라도 있는지 탐색하는 네트워크 call		
	Return Type	Method Name	Parameter Type	Parameter Name
		addListener		
	Description	이벤트 source 에 연결된 peer 객체에게 이벤트 타입에 대한 콜백을 등록한다. 다양한 타입의 이벤트를 수신하면, 다양한 이벤트 콜백을 여러 번에 걸쳐 invoke 해준다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		removeListener		
	Description	이벤트 리스너를 제거한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_name		
	Description	Peer 객체의 이름을 얻는다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_name		
	Description	Peer 객체의 이름과 ID 를 설정한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_roles		
	Description	Peer 가 참여하고 있는 user 객체의 역할을 얻는다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_roles		
	Description	Peer 가 참여하고 있는 user 객체의 역할을 설정한다.		
	Return Type	Method Name	Parameter Type	Parameter Name

		get_enrollment_certificate		
	Description	user 객체 하나의 식별을 위한 ECert 를 반환한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_enrollment_certificate		
	Description	조직을 대표하는 Peer 객체의 cert 를 설정한다.		

[KeyValueStore<<Interface>>]				
Class Diagram				
Responsibility	<p>App 이 CryptoSuite 를 활용한 SW 기반 key 생성할 때 필요한 저장소. 만약 App 이 SW 기반 key 생성을 안하면, default 로 로컬 file 시스템 기반의 저장소를 사용한다.</p> <p>권한이 있는 User 객체만 접근할 수 있으며, key 는 user 객체의 이름이고, value 는 User 객체의 상태를 저장한다.</p> <p>optional 캐시로서 User 등록 도구(private key, CA-인증서)를 저장한다.</p>			
Attribute	Type	Name	Description	
Operation	Return Type	Method Name	Parameter Type	Parameter Name
		get_value		
	Description	key 를 받아서 value 를 반환한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_value		
	Description	key 에 대한 value 를 저장한다.		

[CryptoSuite<<Interface>>]				
Class Diagram	<pre> classDiagram class CryptoSuite { <<Interface>> +encrypt() +decrypt() +sign() +genKeyPair() +deriveKey() +importKey() +getKey() +hash() +verify() } </pre>			
Responsibility	<p>전자 서명과 암호화를 위한 알고리즘을 제공한다. ECDSA, AES, SHA, MAC 이 제공된다.</p>			
Attribute	Type		Name	
Operation	Return Type	Method Name	Parameter Type	Parameter Name
		generate_key		
	Description	option(암호화 객체)에 기반해 key 를 새로 생성한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		deriveKey		
	Description	option(암호화 객체)가 가진 key 를 추출해낸다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		importKey		
	Description	byte 형식의 raw key 를 래핑하여, key 객체를 반환한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		getKey		
	Description	Subject Key Identifier(ski)에 연관된 CSP 의 key 를 반환		
	Return Type	Method Name	Parameter Type	Parameter Name

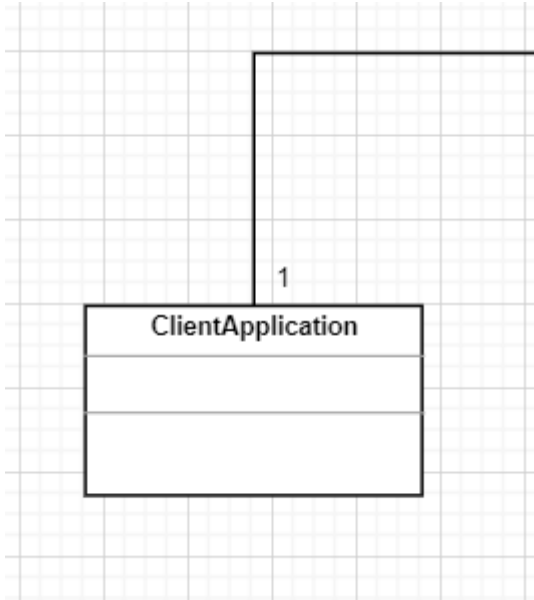
		hash		
	Description	메시지를 hash 화 한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		encrypt		
	Description	평문을 암호화한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		decrypt		
	Description	암호문을 복호화한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		sign		
	Description	데이터를 서명한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		verify		
	Description	서명을 검증한다.		

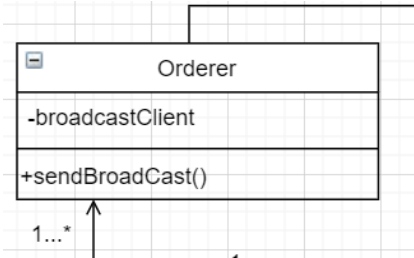
[Node]

Class Diagram	<pre> classDiagram class Node { -url -tlsCert +getUrl() +getTlsCert() +setTlsCert() } </pre>			
Responsibility	Orderer 나 Peer 의 부모 클래스가 되는 Node 클래스는 통신을 위한 기초적인 정보를 가지고 있다.			
Attribute	Type	Name	Description	
	string	url	Node 의 url	
	Object	tlsCert	TLS 를 위한 인증서	
Operation	Return Type	Method Name	Parameter Type	Parameter Name
		get_url		
	Description	Node 의 url 을 가져온다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		get_tls_certificate		
	Description	TLS 를 위한 인증서를 가져온다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		set_tls_certificate		
	Description	TLS 를 위한 인증서를 설정한다.		

[MemberService]				
Class Diagram	<pre> classDiagram class MemberService { -ECA_Client -ACA_Client -TCA_Client -TLSCA_Client +register() +enroll() +delete() +suspend() +reactivate() } </pre>			
Responsibility	<p>신원이 확인되고 가입에 대해 사전 승인을 받은 조직/개인 만이 네트워크에 가입할 수 있다. 어느 조직에서 누가 클라이언트로, 누가 피어로, 누가 endorser 로 들어 올 수 있는지, orderer 는 누가 될 것인지 등등을 컨트롤한다.</p> <p>채널의 관리 권한, 접근 권한을 공개키 기반으로 관리한다.</p> <p>root CA, intermediate CA 들로 구성되며, 조직마다 다르게 사용할 수도 있고 같은 것을 사용할 수도 있다. 여러 조직이 같은 intermediate CA 를 발급받을 수도 있다.</p>			
Attribute	Type	Name	Description	
		TLSCA_Client	intermediate CA 가 발급한 인증서	
Operation	Return Type	Method Name	Parameter Type	Parameter Name
		register		
	Description	인증서를 등록한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		enroll		
	Description	인증 권한을 부여한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		delete		

	Description	인증 권한을 삭제한다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		suspend		
	Description	인증권한을 정지시킨다.		
	Return Type	Method Name	Parameter Type	Parameter Name
		reactivate		
	Description	suspend 된 인증 권한을 재활성화 시킨다.		

[ClientApplication]				
Class Diagram				
	사용자와 블록체인을 연결하기 위한 역할을 한다. Rest API 를 이용해 요청을 보내 처리를 하는 웹앱을 이용한다.			
Attribute	Type		Name	Description
Operation	Return Type	Method Name	Parameter Type	Parameter Name
	Description			

[Orderer]				
Class Diagram	 <pre> classDiagram class Orderer { -broadcastClient +sendBroadCast() } class BaseClass { } BaseClass < -- Orderer </pre>			
Responsibility	<p>트랜잭션 내용에 관계 없이, 채널에서 발생하는 트랜잭션을 받아서 시간 순서대로 정렬하여 합의를 통해 블록을 생성한다. 합의하는 방식은 기본적으로 pluggable 하며, SOLO 와 Kafka 두 가지 알고리즘을 제공한다.</p>			
Attribute	Type	Name		Description
	Object	broadcastClient		Broadcast 할 Client 의 목록
Operation	Return Type	Method Name	Parameter Type	Parameter Name
		sendBroadCast		
	Description	모든 Peer 노드에 트랜잭션을 BroadCast 한다.		