블록체인 기반 핀테크 서비스 기술

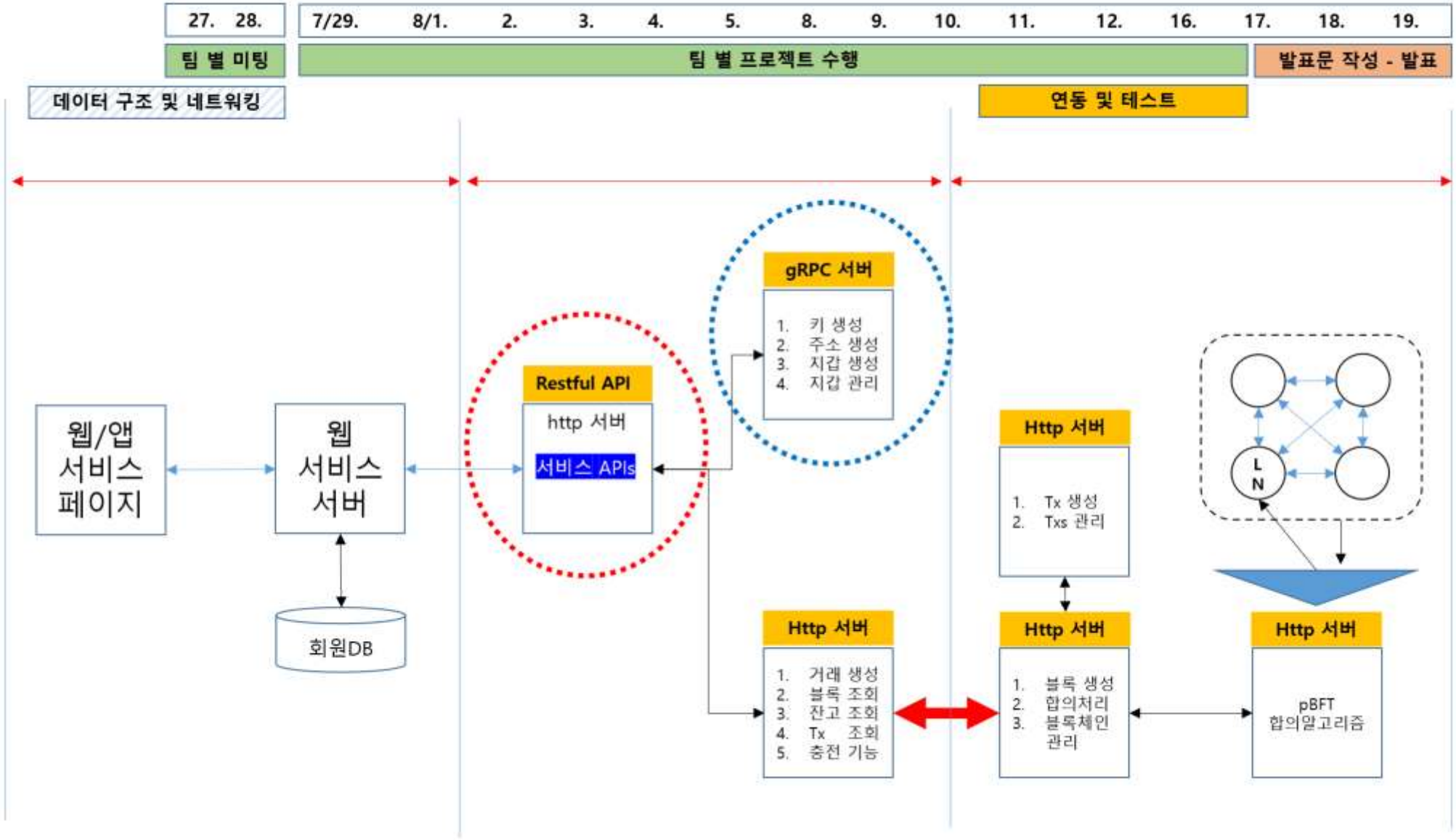
박광범

경력 보장을 위한 pBFT 합의 알고리즘 기반

블록체인 코어 플랫폼 구현

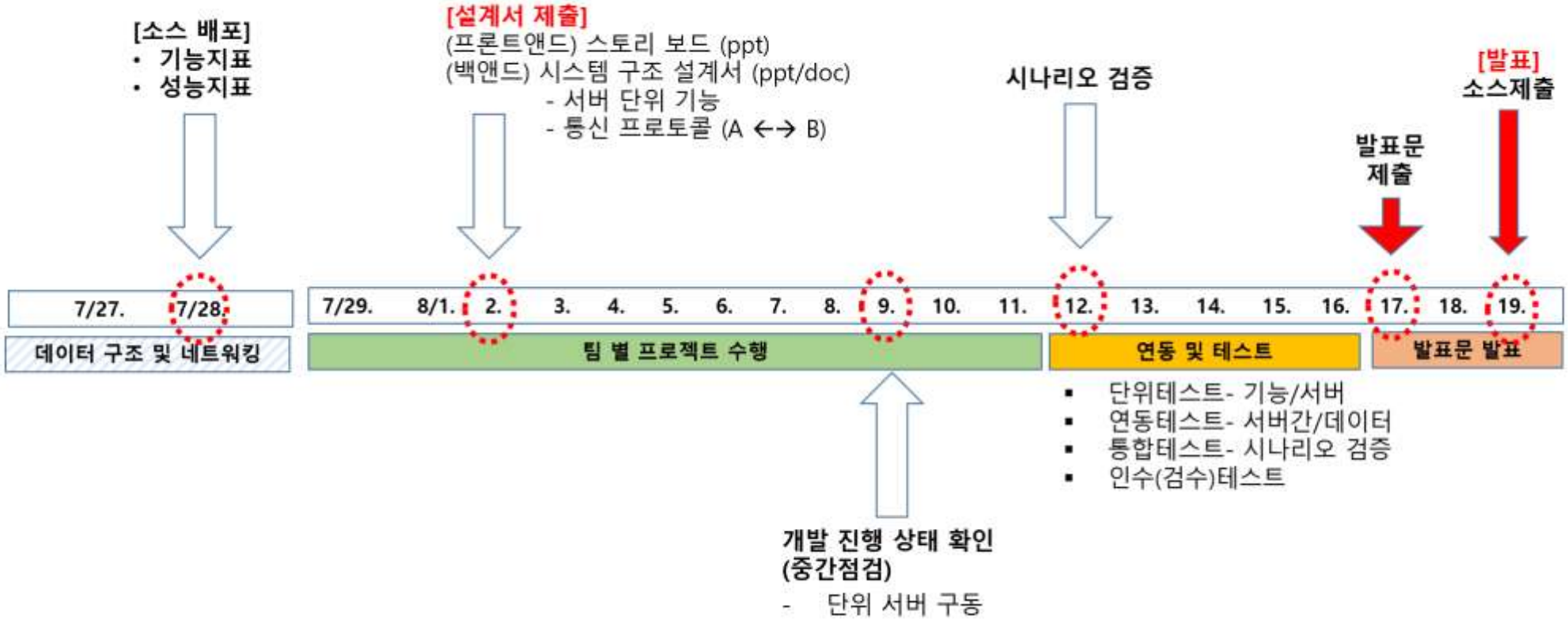
개발 목표

- 전체 시스템 구조
- Front-End vs Back-End 구분
- Team organization
- R&R in team



개발일정

-.진도대비 현황
-.진행 이슈공유



목차

1. Project Overview

프리랜서들의 경력을 보장해주는 웹서비스이다.

중앙 데이터베이스를 통한 프리랜서 경력 웹서비스는 이미 존재한다.

하지만 중앙 데이터베이스는 서비스 제공자를 전적으로 신뢰해야만 하는 방법이다. 만약 서비스 제공자가 데이터 베이스를 조작하여 경력을 조작한다고 해도 사용자들은 이를 알 수 가 없는 것이다.

이를 해결하기 위해 중앙 데이터베이스가 아닌 블록체인을 이용하여 경력에 대한 신뢰성을 보장해주는 웹 서비스를 계획했다.

결과적으로 PBFT 합의 과정을 적용한 블록체인을 활용한 프리랜서 경력 보장 웹서비스가 프로젝트의 목표이다.

프로젝트 선정 배경

•**59 million Americans** did freelance work in 2020.

A number that has stayed fairly steady, as **58 million** are still freelancers as of 2021.

•Freelancers contribute **$1.2 trillion** to the United States' economy each year.

•As of 2022, **36% of the U.S. workforce** does freelance work.

•The number of freelancers in the United States has increased by almost **12%** between 2014 and 2021.

•Freelancers earn, on average, **$28 an hour** for performing skilled services.

•Computer programming, marketing, IT, and business consulting are top industries for freelancing, with **50% of freelancers** providing such services.

•Freelancing is expected to grow by approximately **14% over the next six years**.

•There are an estimated **1.2 billion freelancers** in the world — that's over **34% of the global workforce**.

US FREELANCERS 2014-2020

Year	Number of Freelancers
2021	58 million
2020	59 million
2019	57 million
2018	56.7 million
2017	57.3 million
2016	55 million
2015	53.7 million
2014	53 million

footnote : https://www.zippia.com/advice/freelancing-statistics/#:~:text=Freelancing%20is%20expected%20to%20grow,34%25%20of%20the%20global%20workforce.

Expected Financial Statement Sheet

Company Name

Address 1
Address 2
City, State ZIP
(000) 000-0000
www.company-name.com

Seoul,Korea , F

www

Category	2019	2020	2021	2022
Total FreeLancer in US	57000000	59000000	58000000	60000000
Register Fee	$5.00	$5.00	$5.00	$5.00
Exp.Income	$85,500,000.00	$88,500,000.00	$87,000,000.00	$90,000,000.00

*Exp.Income = 10% of Total FreeLancer *3(Registered Career)

US FREELANCERS 2014-2020

Year	Number of Freelancers
2021	58 million
2020	59 million
2019	57 million
2018	56.7 million
2017	57.3 million
2016	55 million
2015	53.7 million
2014	53 million

Total Exp.Income $351,000,000.00

Annual Average Exp.Income: $87,750,000.00

2. What is the problem

사용자가 등록한 경력을 중앙 데이터 베이스를 통해 관리했을 때, 어떠한 이유로 서비스 제공자가 경력 조작을 할 가능성이 존재하고 사용자는 이를 하나하나 검증해보지 않는다면 조작의 사실을 알아차리기 힘들다는 큰 문제점이 존재한다.

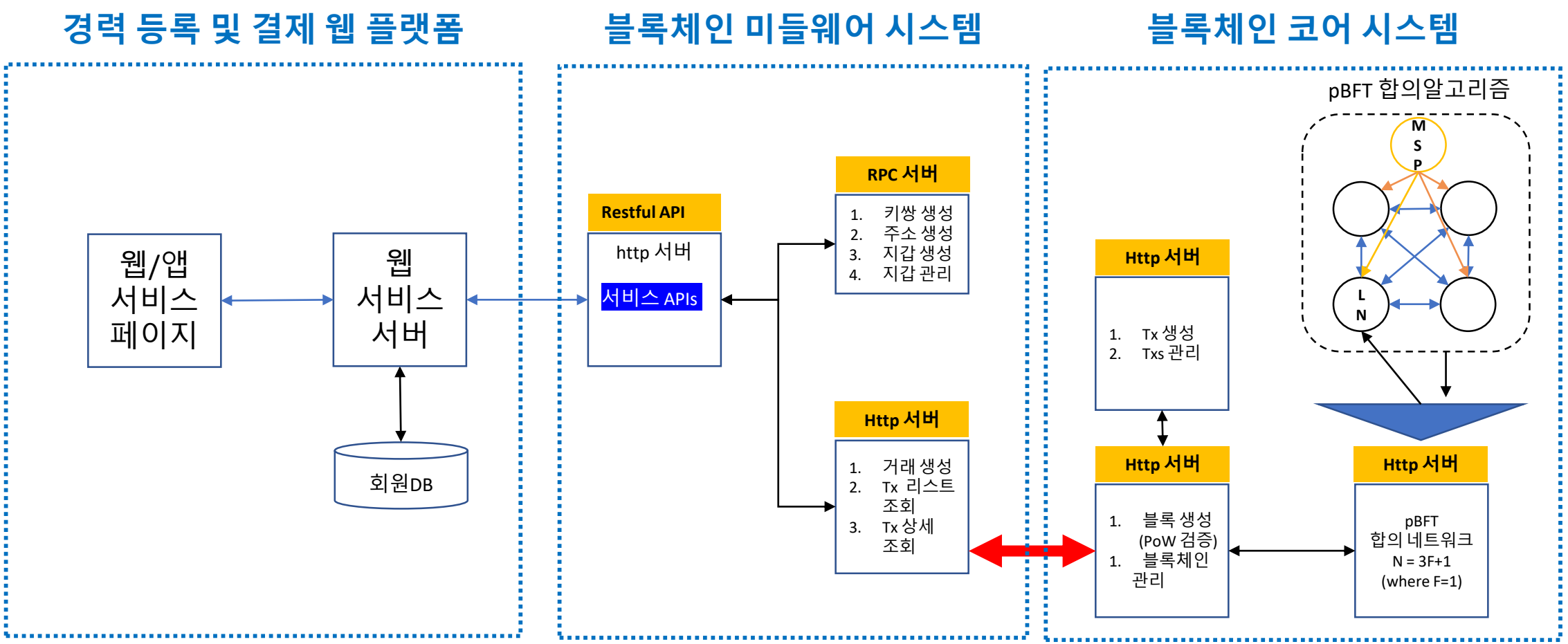
하지만 블록체인을 적용한다면 탈중앙화를 통해 경력에 대한 수정과 삭제를 신뢰할 수 있게 된다. 또한 PoW와 PBFT 의 합의 과정을 통해 트랜잭션과 블록에 관한 거래 생성을 보장할 수 있다.

3. What is needed

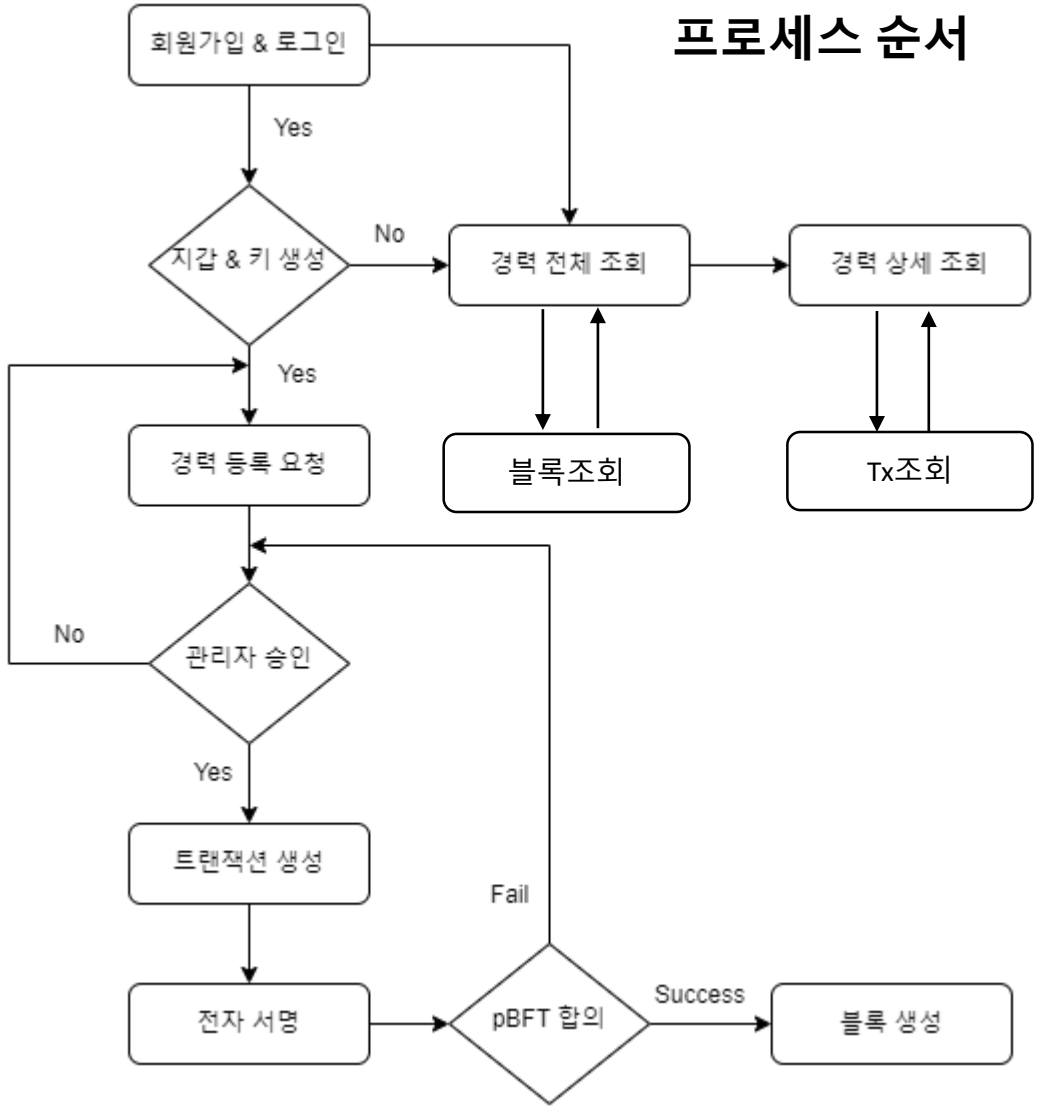
요구사항 번호	요구사항 명	요구사항 내용
RQ-1	월렛 생성	입력값 => 월렛생성 signal 출력값 => PrivateKey , PublicKey, Address
RQ-3	경력 등록 요청	입력 값 Address != nil & TxID == nil & PrivateKey 출력값 => 경력 등록된 TxID
RQ-4	경력 조회	비회원도 조회 가능 입력값 => Address 출력값 => TXs
RQ-5	상세 경력 조회	입력값 => TxID (받아와서 가공해 Block ID 추출) 출력값 => Block, TX

4. What is our solution

◆ **PoW + pBFT 기반 프리랜서 경력 보장 웹서비스**



5-1. How it works



<Front Scenario>

메인 페이지에 들어와서 지갑을 생성하려고 하거나 , 경력을 추가하려고 했을때는 로그인이 필요하고 ,

로그인을 하지 않아도 타인의 이메일 주소만 가지고 지갑 주소를 검색할 수 있고 ,

지갑 주소로 타인의 경력들을 조회할수 있고 , 그 경력들을 각각 상세 조회도 가능함.

회원가입은 따로 없고 구글 아이디만 있으면 로그인이 가능하며 ,

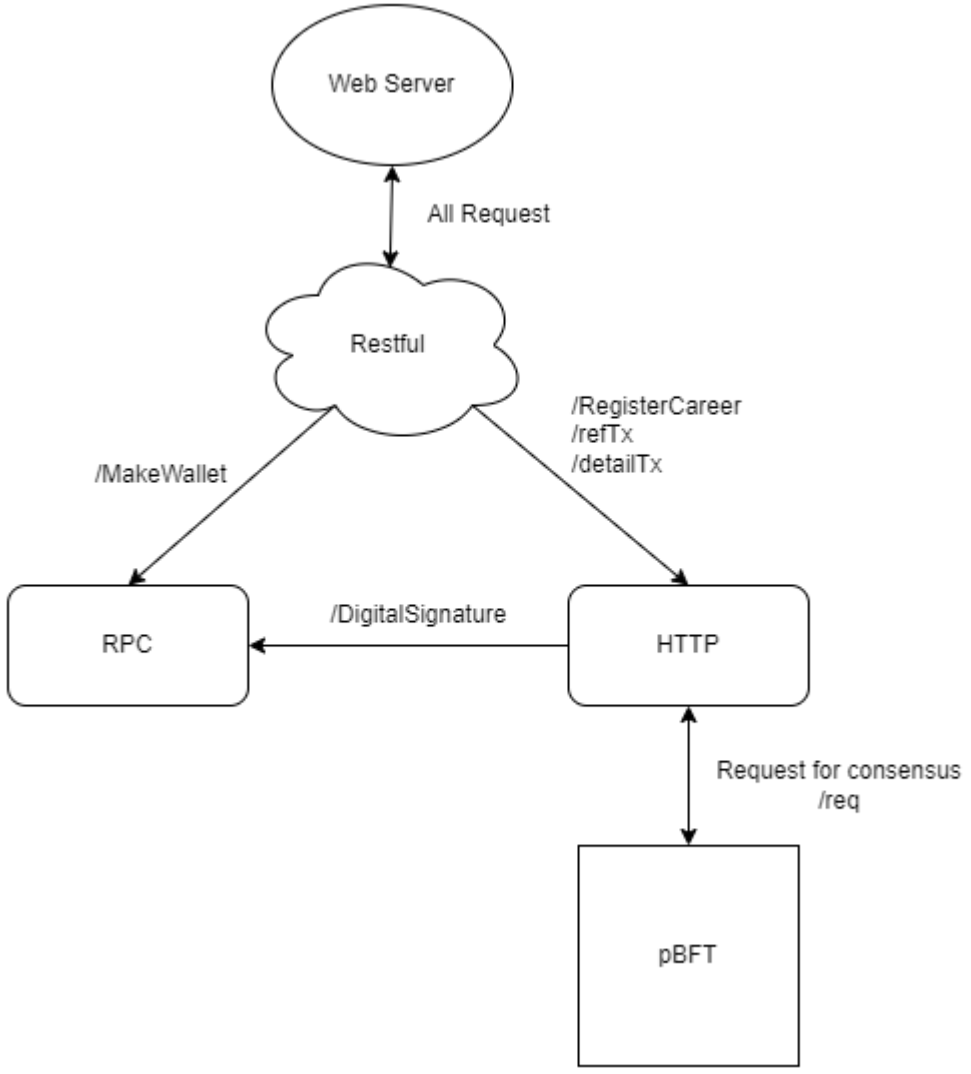
로그인 했어도 경력을 추가하기 위해서는 지갑 주소를 생성 해야하며 , 지갑 주소를 생성한 후에

경력 추가를 할 때 서명을 해야지 등록을 할 수 있다는 동의서를 받고 , 결제를 완료한 후에 ,

그 경력이 관리자에게 넘어가고 관리자는 그 경력이 사실 이라는 것 을 검증을 마친 후에 승인.

승인이 완료되면 그 데이터는 코어로 넘어가서 블록으로 만들어 블록체인에 넣음.

5-2. How it works



<Scenario>

Front에서 요청이 들어왔을때 , MiddleWare가 그 요청을 받아서 ,
그 요청에 맞는 Core에 요청을 보냄

블록 생성의 요청의 경우 , 요청 들어온 데이터를 받아서 Transaction을 만들고 그 Transaction 데이터를 대표할수있는 Txid를 생성하고
,
MSP로부터 LeaderNode의 주소를 받아서 , 그 주소에 합의 요청을 보냄.

합의 요청을 받은 LeaderNode는 합의를 진행하고 , 합의가 완료된 데이터를 응답으로 돌려줌.

응답 받은 데이터를 Base로 블록을 생성

만약 합의가 실패되었다면 ,응답으로 합의 실패를 보내주고 , 합의 실패 응답을 돌려받은 경우 ,마지막 합의 요청을 다시 보냄 .

블록 조회의 경우 지갑 주소를 받아서 그 주소에 해당하는 모든 블록을 리턴

트랜잭션 조회의 경우 지갑 주소를 받아서 그 주소에 해당하는 모든 데이터를 리턴 .

MSP(Membership Service Provider)

MSP 는 멤버쉽 전체를 관장하며 , 멤버쉽의 변경 (추가/제거)에 있어서 그 멤버들이 들어있는 주소록을 Control 함.

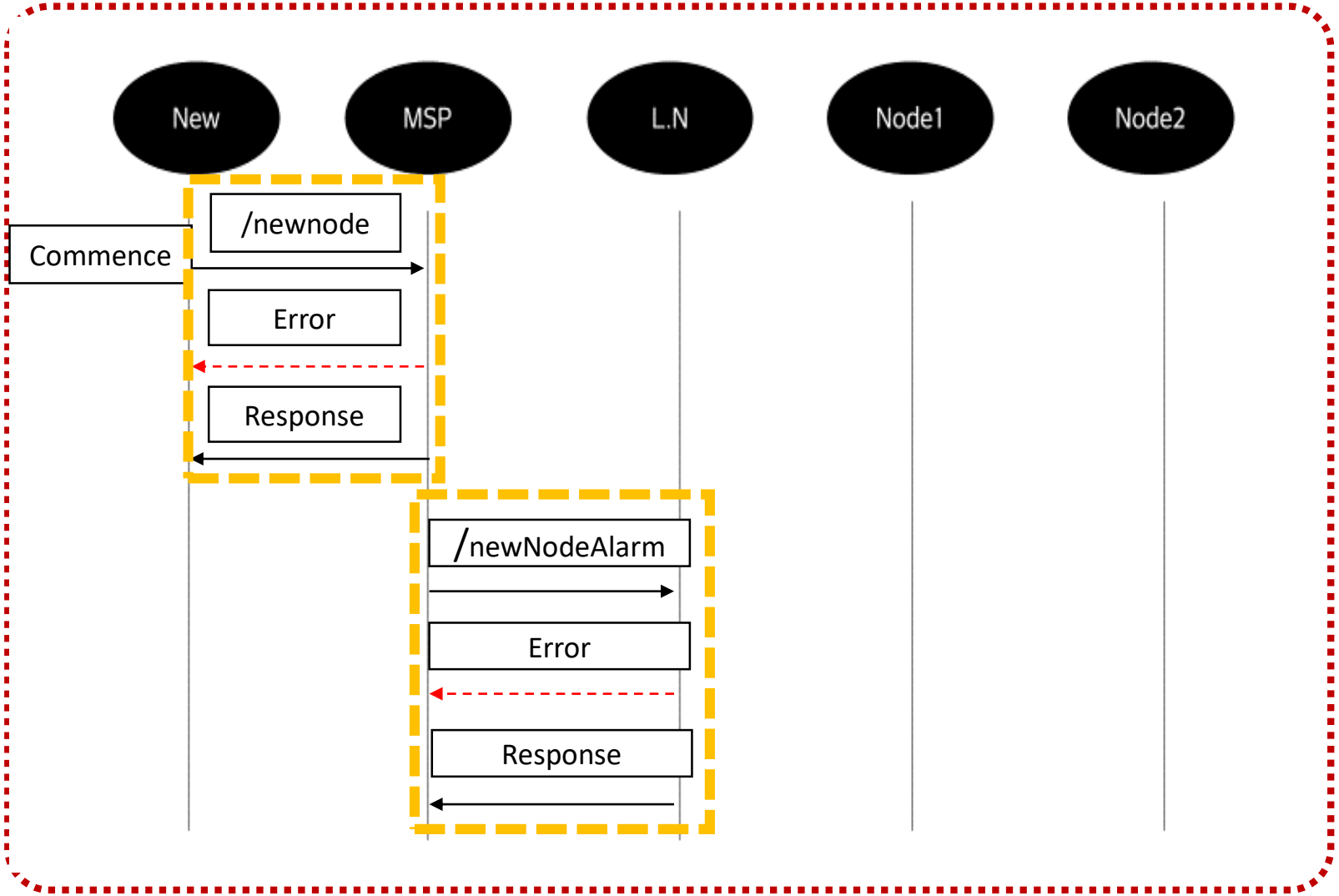
1. 멤버 추가의 경우 새로운 멤버를 먼저 검증하고 , 그것이 통과되면 기존의 멤버들에게 그 사실을 알림 (FLOW CHART 참조)

2. 멤버 제거의 경우 기존의 멤버가 응답이 없을경우 그 멤버를 주소록에서 제거 하고 , 갱신된 주소록을 전파.

3. Status 요청에 대해 응답하며 , 응답의 내용은 현재 주소록 데이터.

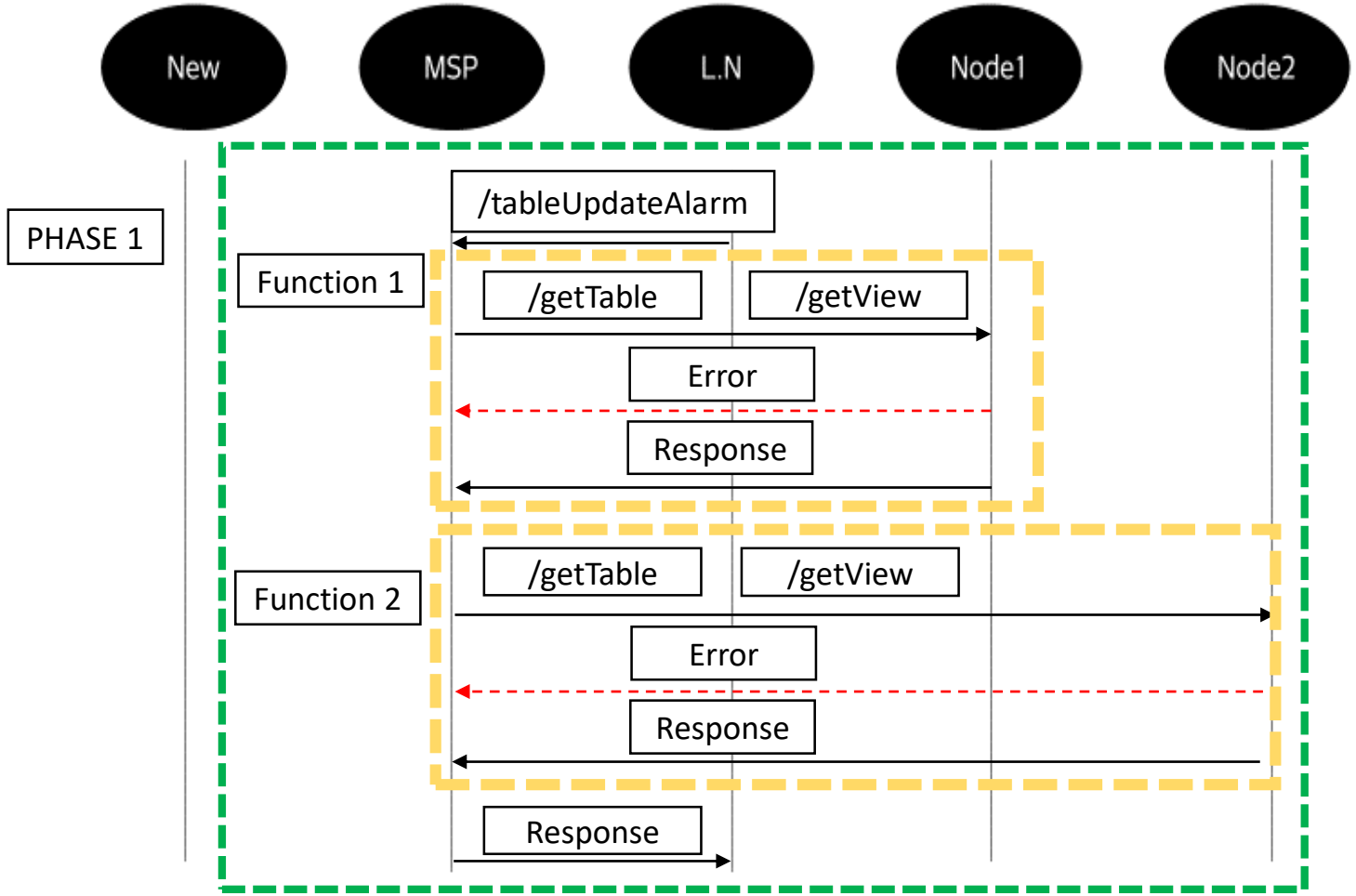
4. 리더노드가 어떠한 요인으로 오작동을 하거나 응답을 하는 경우, MSP가 판단하여 리더를 재 선출하고 , 기존에 있던 리더를 주소록에서 제거하여 , 서비스를 멈추지 않고 Sustainable 하게 유지할수있도록 함.

MSP Mechanism FLOW CHART (MSP ←→ NODE(CORE)) - Commencing Phase



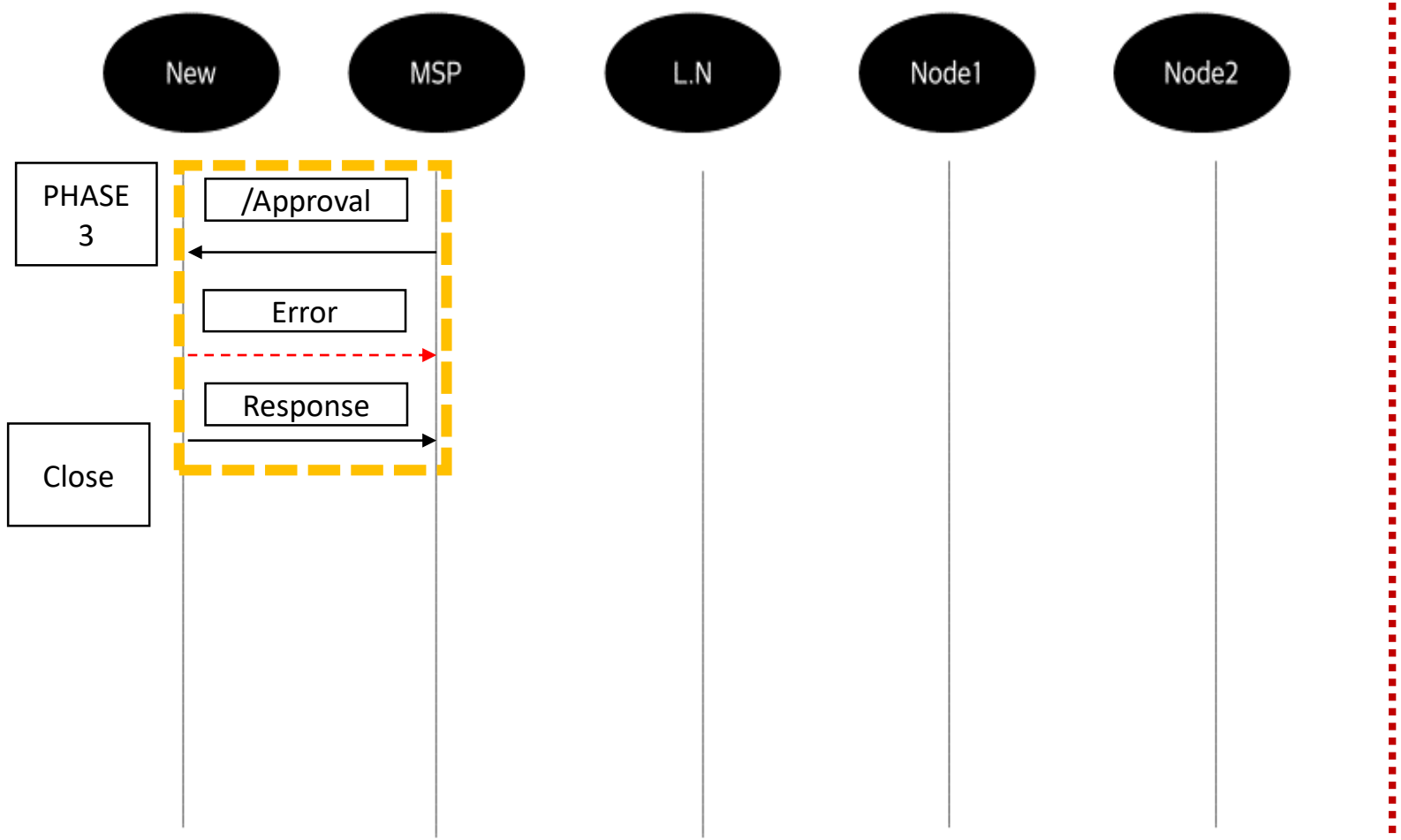
- Commence Phase : 새로운 노드가 MSP에게 규격에 맞춰서 Request를 보내고
- 그 요청을 받아서 MSP가 Identify한 후에 통과가 된다면 Stay 하도록 New Node에게 Response를 보냄.
- 만약 통과하지 않았다면 , 응답이 없음.
- 그리고 리더노드에게 새로운 노드가 들어왔다는 알림을 보냄.

MSP Mechanism FLOW CHART (MSP ←→ NODE(CORE)) - PHASE 1



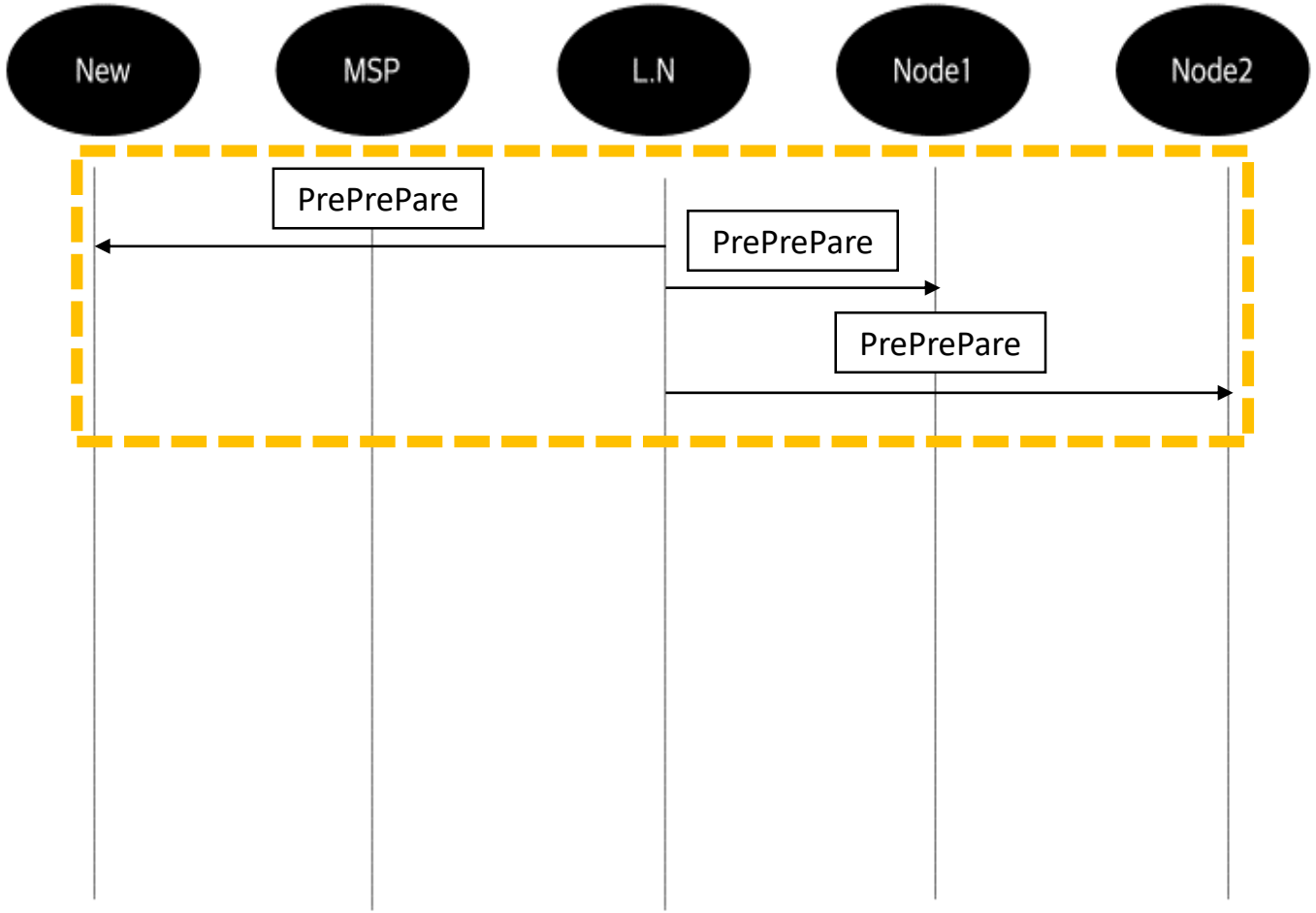
- Phase 1 : 새로운 노드가 정상적으로 식별되었다는 가정하에 , 리더노드에게 새로운 노드가 들어왔다고 알림.
- 리더노드는 새로운 합의를 시작하기전에 항상 새로운 노드가 들어왔다는 알림이 있는지 체크하고 , 있다면 합의를 진행하지 않고 MSP에게 주소록 업데이트 요청 과 ViewID(식별자) 주고 대기
- MSP는 새로운 노드의 주소를 담아서 주소록을 갱신하고 그걸 노드1 , 노드2, 노드3 한테 보내고 응답을 받을때까지 기다림.

MSP Mechanism FLOW CHART (MSP ←→ NODE(CORE) - PHASE 2 to Close



- Phase 2 : 모든 노드들의 응답을 받은 후에 리더노드에게 갱신된 주소록을 응답으로 보내줌.
- Phase 3 : MSP는 새로운 노드에게 갱신된 주소록과 ViewID를 보내줌.
- Close : NewNode 는 OK 응답을 MSP에게 보내줌.
- 리더노드는 갱신된 주소를 바탕으로 PrePrePareMsg를 새로운 노드가 추가된 주소록으로 BroadCast.

MSP Mechanism FLOW CHART (MSP ←→ NODE(CORE) - New Consensus



• New Consensus : 리더노드는 갱신된 주소를 바탕으로 PrePreParеMsg를 새로운 노드가 추가된 주소록으로 BroadCast.

• 새로운 노드도 기존에 있던 노드들과 같이 합의를 시작

7. Who we are

Team Member

진재호 (팀원)
MSP / Core
Go

허진혁 (팀원)
CORE
GO

이민아 (팀원)
Front(SpringBoot)
Java,Mysql

박재현 (팀원)
Front(SpringBoot)
Java,Mysql

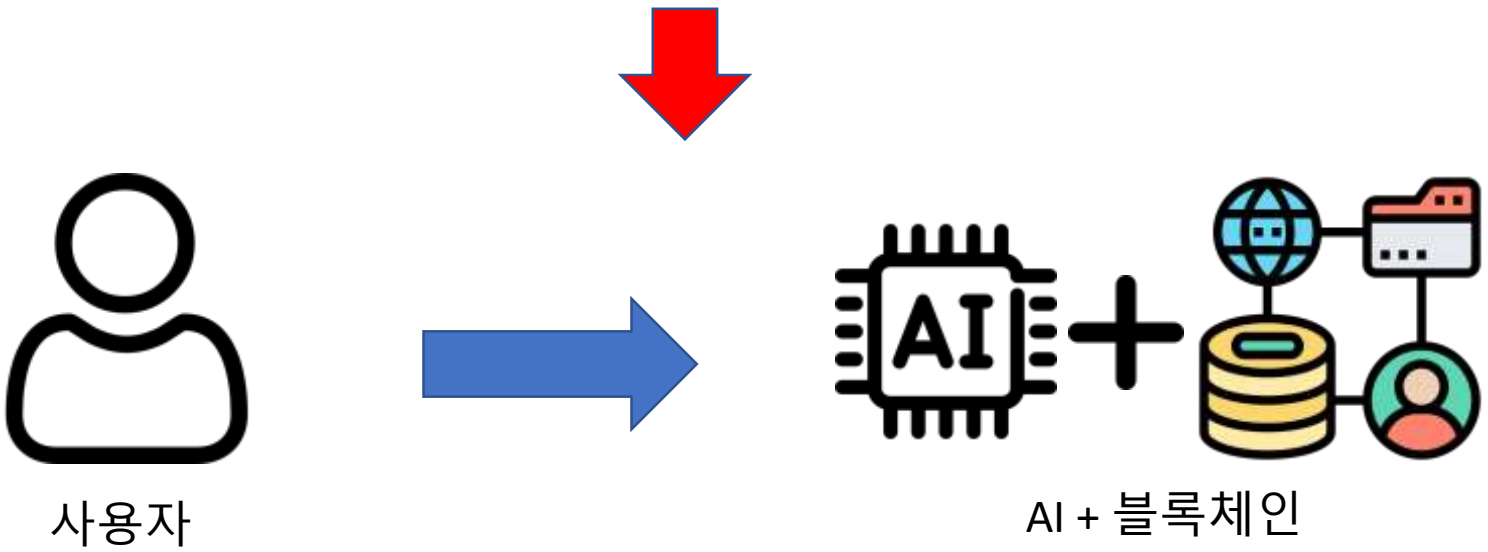
김태오 (팀원)
Middleware/Document
Go

Who I am

박광범 (리더)
OverAll(Front/Middleware/Core)
GO,Java,SpringBoot

8. Future Goal

현재는 관리자라는 순수 인력을 사용하여 사용자가 등록한 경력의 진위 여부를 판단하도록 설계되어 있지만, 서비스를 운영하며 경력 인증서에 대한 빅데이터를 모아서, 여러 경력 인증서들에 대한 딥러닝 모델을 개발하여 서비스에 적용한다면 더 퀄리티 높은 비즈니스 모델이 될 것 이라고 생각한다.



Future Work

현재 결제는 카카오페이로만 할 수 있도록 되어있지만 , 다양한 결제 방식을 지원하도록 해야함.

관리자가 리더노드를 교체하고 싶을 경우 교체할수 있도록 해야함.

노드들의 Status 나 MSP의 Status를 Log나 Web으로 보기쉽게 Visualize 작업을 해야함.

미숙한 Error Handling 을 좀 더 바꿔야함 .