프라이빗 블록체인 소개와 경량 맞춤형 블록체인(it-chain) 구현 사례 공유

Kosslab 5기 전담개발자 | 이준범

2018-10-18

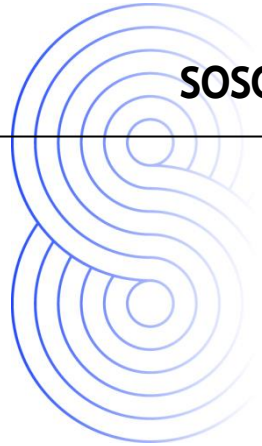
SOSCON 2018
SAMSUNG OPEN SOURCE CONFERENCE 2018

소개

이준범

- Kosslab 5기 전담 개발자
- 카이스트 소프트웨어 아키텍처 연구실 석사 졸업
- 중앙대학교 컴퓨터 공학부 졸업
- 취미: 카페에서 코딩하기
- 관심 분야: 소프트웨어 아키텍처, 머신러닝(딥러닝,NMT), 블록체인
- Github: https://github.com/junbeomlee

목차



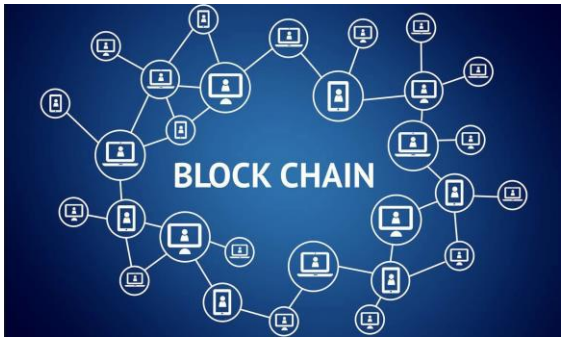
프라이빗 블록체인

퍼블릭 블록체인이란?

퍼블릭 블록체인

네트워크에 참여한 **모든 참여자**가 **전체 장부**를 공유하고, 대조를 통해 거래를 안전하게 만드는 기술

ethereum



https://goo.gl/8Awzmg

프라이빗 블록체인이란?

프라이빗 블록체인

허가된 참여자들간 장부를 공유하고, 대조를 통해 거래를 안전하게 만드는 기술

HYPERLEDGER
FABRIC

HYPERLEDGER
SAWTOOTH

c·rda

프라이빗 블록체인이란?

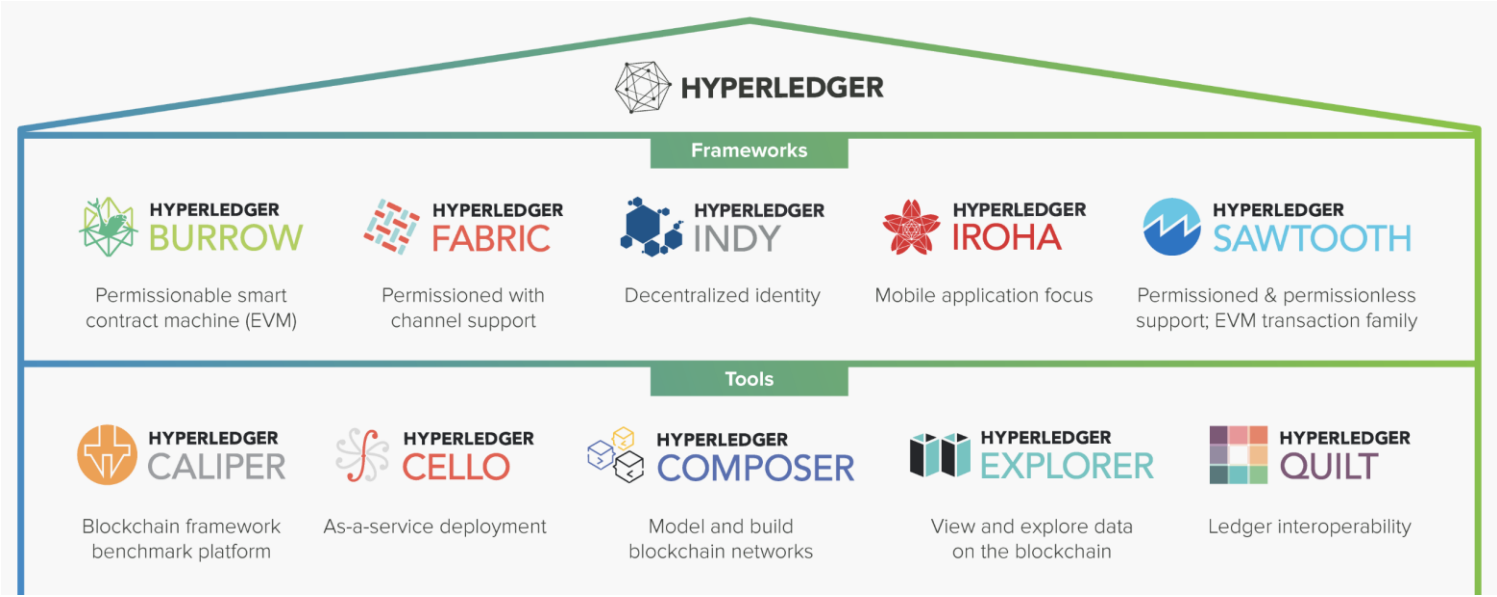
Why 프라이빗 블록체인?

- **퍼블릭 블록체인의 한계**
  - 속도 (비트코인 7TPS, 이더리움 10TPS)
  - 비용 (Mining에 사용되는 전기)
- **선별적 정보 공유의 필요성**
  - 기존의 기업과 정부기관의 구조에 적합

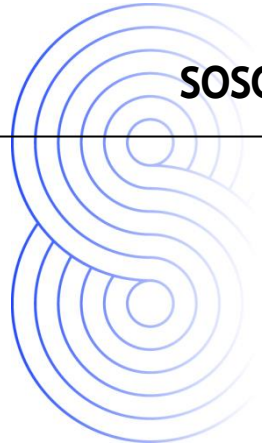
Hyperledger

Hyperledger 프로젝트란?

- 리눅스 재단에서 주관하는 블록체인 오픈소스 프로젝트
- 금융, 물류, 제조, 기술 산업등 여러 산업에 응용 가능한 블록체인 개발



Hyperledger Fabric



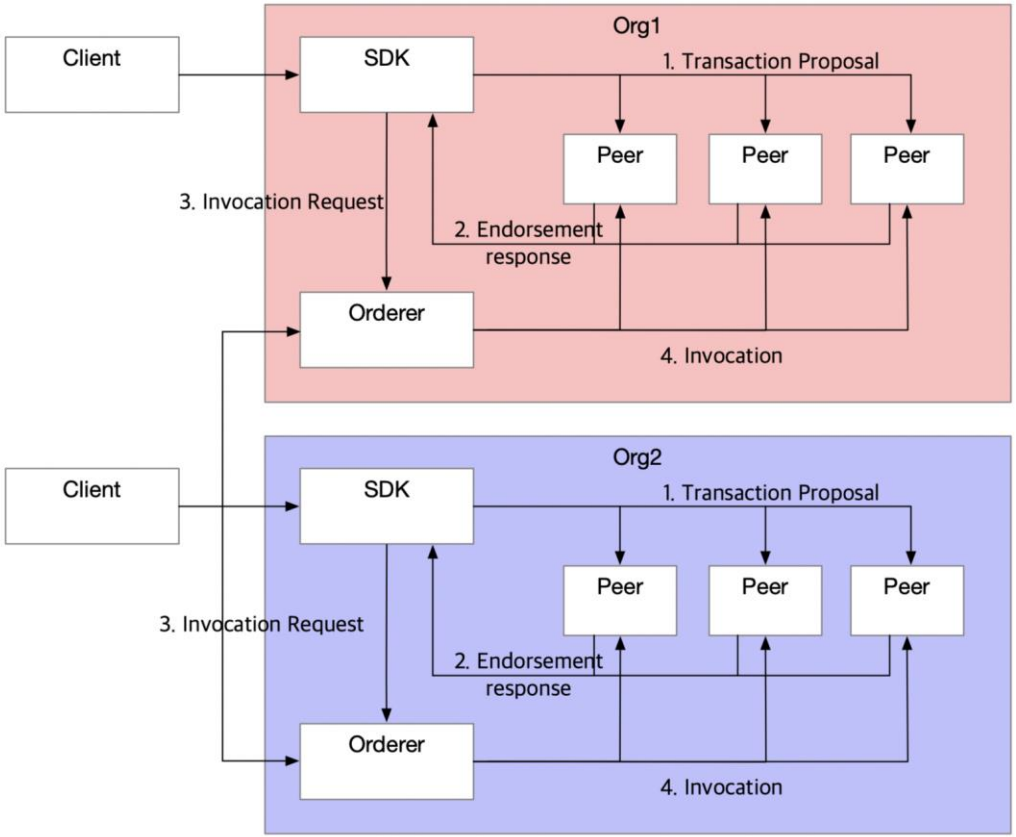
특징

- **Modular and configurable architecture**
  - Order service
  - Membership service
  - Ledger
  - Endorsement and validation policy
- **Support general-purpose programming languages(Chaincode)**
  - Java, Go, Node.js
- **Permissioned network**
- **Pluggable consensus protocols**

HYPERLEDGER
FABRIC

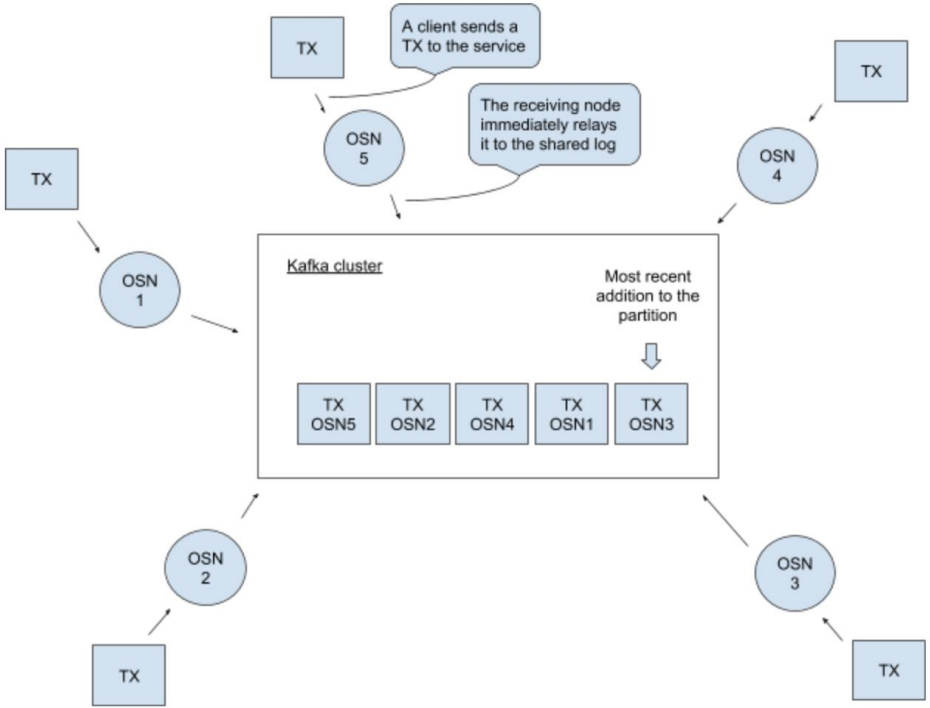
Hyperledger Fabric

아키텍처

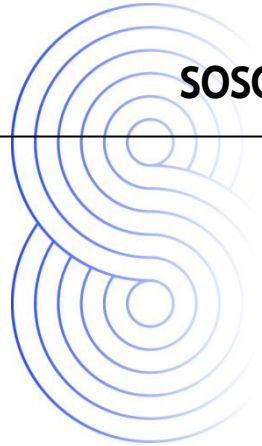


Hyperledger Fabric

Kafka in hyperledger fabric



Hyperledger Sawtooth

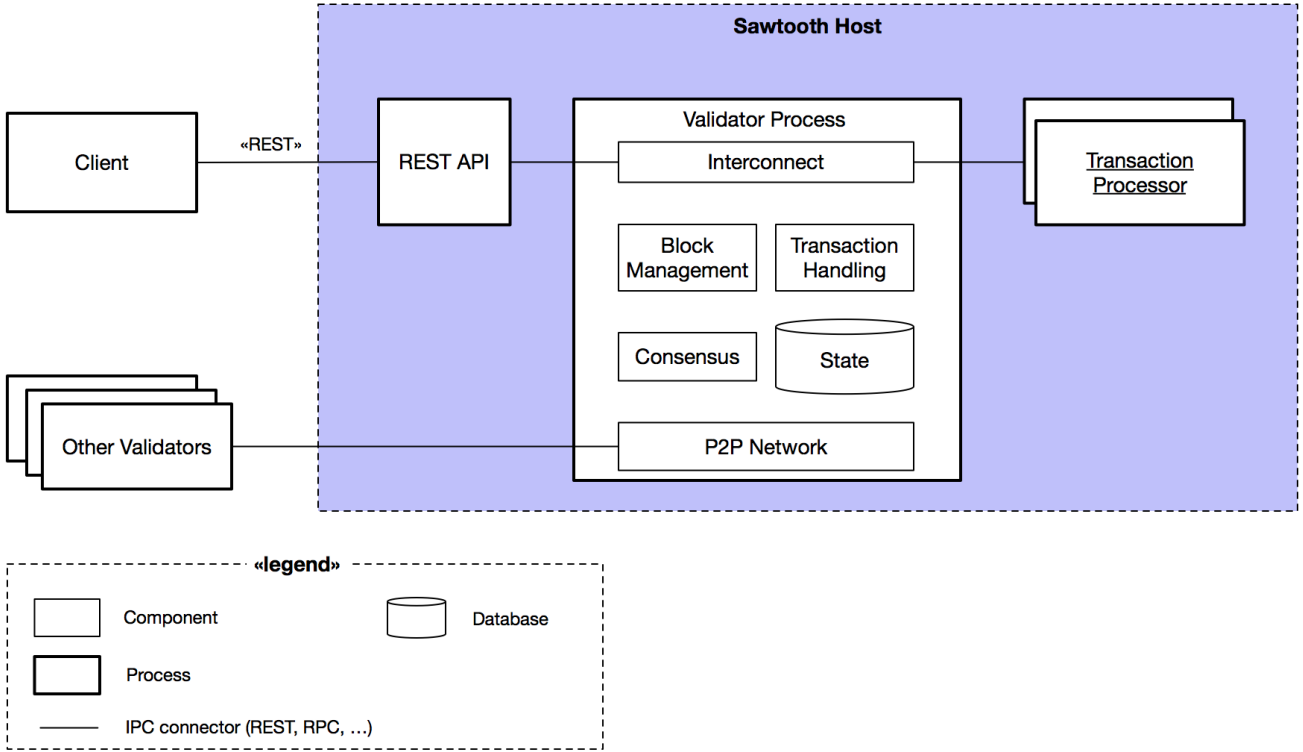


특징

- Separation between the application level and core system
  - Transaction processor(Application level)
  - Validator(Core system)
- Parallel Transaction Execution
- Event System
- Pluggable consensus algorithms

Hyperledger Sawtooth

아키텍처



Poet(Proof of elapsed time)

1. PoET stochastically elects individual peers to execute requests at a given target rate
2. Individual peers sample an exponentially distributed random variable and wait for an amount of time dictated by the sample.
3. The peer with the smallest sample wins the election

Poet(Proof of elapsed time)

- Fairness: The function should distribute leader election across the broadest possible population of participants.
- Investment: The cost of controlling the leader election process should be proportional to the value gained from it.
- Verification: It should be relatively simple for all participants to verify that the leader was legitimately selected.

It-chain

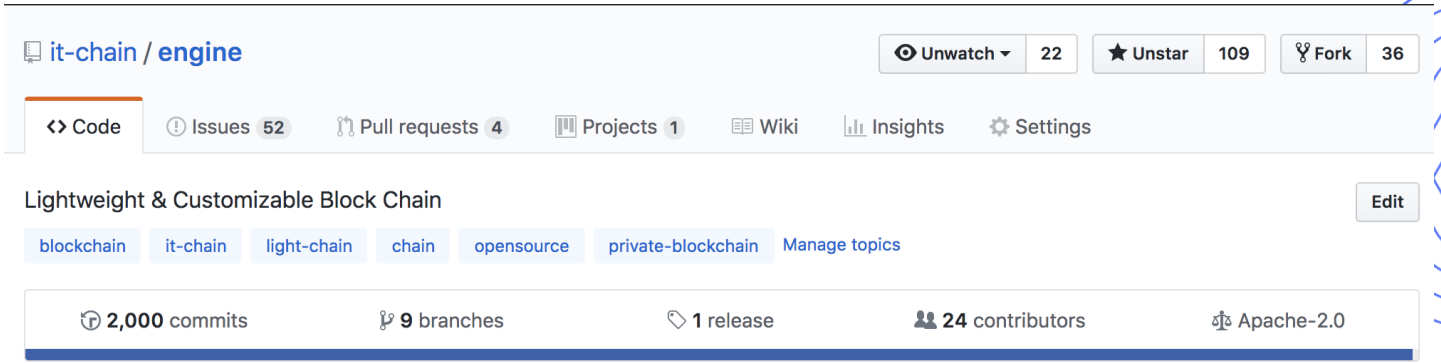
경량 맞춤형(Customizable and lightweight) 블록체인

SOSCON 2018

SAMSUNG OPEN SOURCE CONFERENCE 2018

It-chain 오픈소스 커뮤니티

- It-chain 오픈소스 커뮤니티(2018/01 ~ 진행중)
- Github: https://github.com/it-chain/engine
- 컨트리뷰터: 24명
- Star: 109
- Commit: +2000



It-chain 오픈소스 커뮤니티

제주도 합숙 코딩

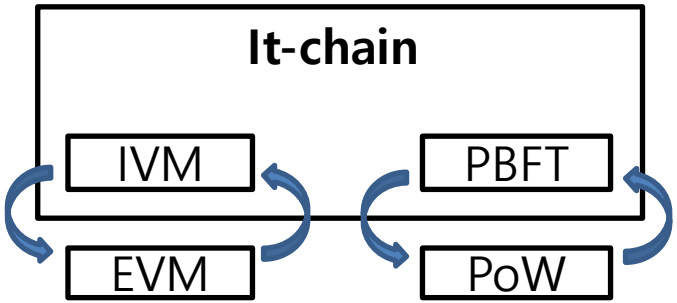
It-chain 오픈소스 커뮤니티

토요일 정기 미팅

목표

중소규모 커뮤니티에서 유연하고 자유롭게 이용가능한
‘경량 맞춤형 블록체인 엔진’ 개발 및 **‘블록체인 코어 공부 ‘**

- 핵심서비스의 모듈화를 통해 목적에 맞게 쉽게 교체 가능 하도록 개발
- 핵심서비스 교체시 많은 부분을 수정하지 않도록 개발



It-chain - Architecture

핵심 요구사항

- 제3자가 손쉽게 수정/확장 가능
- 오픈소스로 쉽게 개발될 수 있도록, 최대한 개발자들이 다른 컴포넌트의 변화에 간섭 받지 않고 개발을 진행
- 중앙 관리자 없는 P2P구조
- 기본적인 블록체인 기능들(블록저장, 합의, 인증)을 지원
- Consensus는 PBFT를 지원

It-chain - Architecture

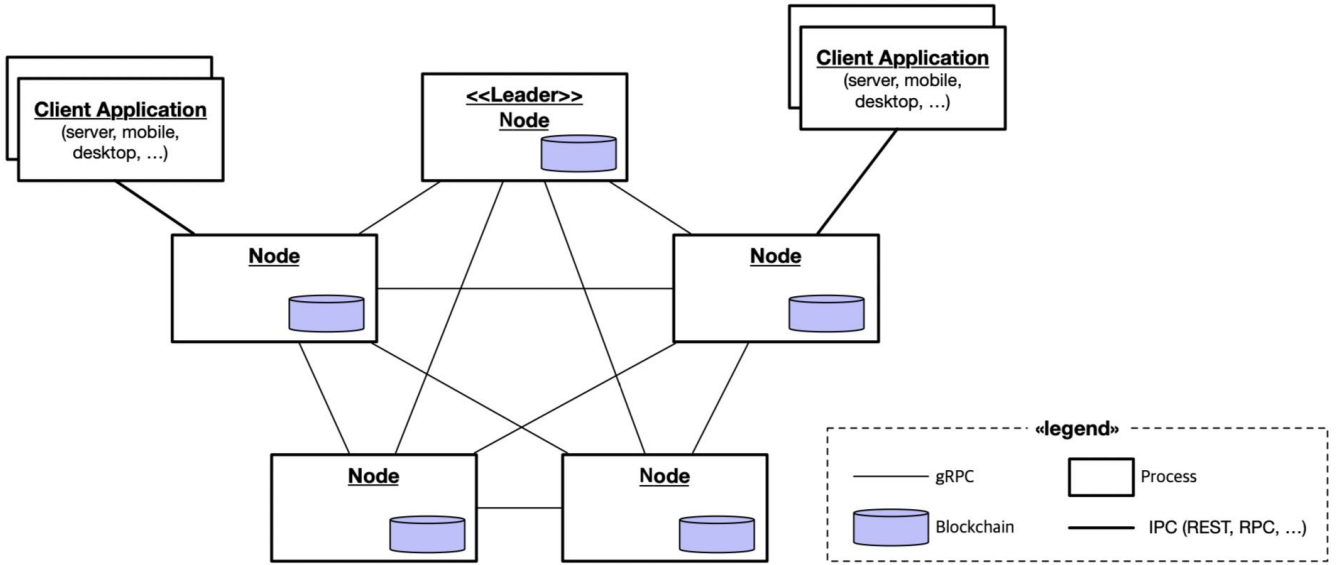
아키텍처 설계

- 제3자가 손쉽게 수정/확장 가능
- 오픈소스로 쉽게 개발될 수 있도록, 최대한 개발자들이 다른 컴포넌트의 변화에 간섭 받지 않고 개발을 진행
  - **핵심 기능을 지원하는 컴포넌트들을 완전히 독립적으로 구성**
  - **Event driven 아키텍처 스타일 도입**
- 중앙 관리자 없는 P2P 구조
  - **P2P Network 구성**
- 기본적인 블록체인 기능들(블록저장, 합의, 인증)을 지원
  - **Block storage 컴포넌트**
  - **Authentication 컴포넌트**
  - **Consensus 컴포넌트**
- Consensus는 PBFT를 지원
  - **Transaction pool 컴포넌트, 리더 노드 개념 도입**

It-chain - Architecture

It-chain Network

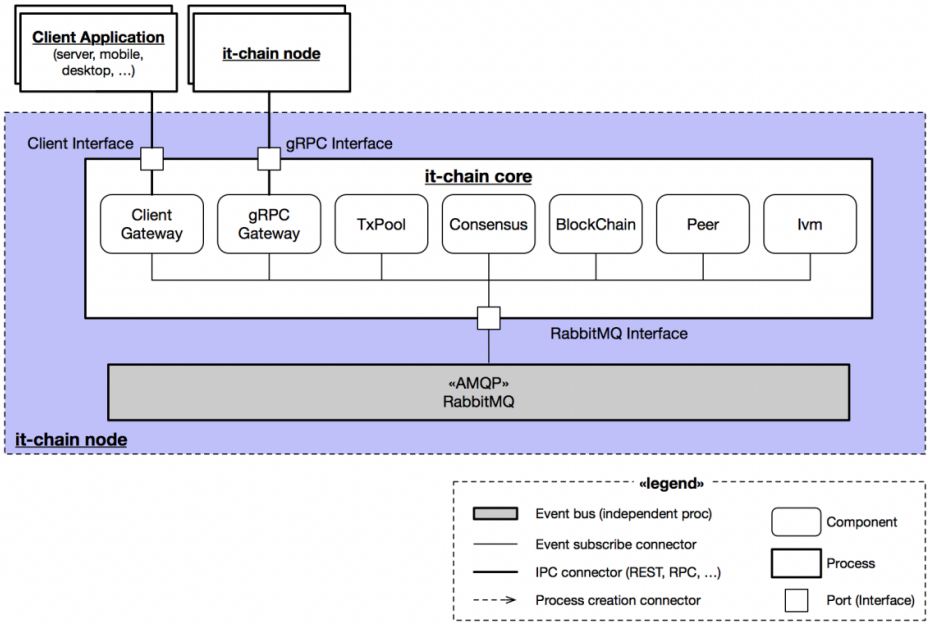
- It-chain network는 it-chain node들로 구성된 P2P network
- 모든 Node들은 서로 연결됨
- Leader와 Peer로 구성(PBFT)



It-chain - Architecture

It-chain Node Architecture

- **it-chain은 6개의 독립적으로 동작하는 핵심 컴포넌트들로 구현되며 각각은 AMQP(Asynchronous Message Queue Protocol)를 통해 커뮤니케이션한다.**



It-chain - Architecture

SOSCON 2018

아키텍처 문서

- Link: **https://github.com/it-chain/engine/blob/develop/ARCHITECTURE-KR.md**
- 20 Page

It-chain 아키텍처 문서

1. 개발 배경 및 목적

기존 블록체인은 그 규모가 방대하고 복잡하여 지역사회, 소규모 상인연합과 같은 비IT 중소규모 커뮤니티에서 사용하기에 높은 진입장벽을 갖고 있다. 또한 이더리움, 비트코인, 하이퍼레저와 같은 기존의 블록체인은 자신들의 목적에 맞춰 수정하여 사용하기에 어려움이 있다.

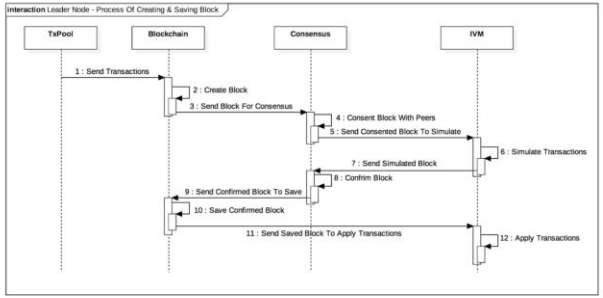
그리고 누군가가 블록체인에 대해서 심도 있게 학습하고자 할 때 일반적인 블록체인 이론과 관련된 자료는 많지만 그 이론을 이용해서 실제로 어떻게 블록체인을 구현할 지에 대해서 자세히 알려주는 자료와 오픈소스는 거의 없다. 그나마 존재하는 자료들도 코어가 아닌 Dapp에 대한 것이 대부분이다.

본 프로젝트는 이러한 문제점들을 해결하기 위해서 중소규모 커뮤니티에서 유연하게 수정하여 자신들의 목적에 맞게 활용할 수 있는 경량 맞춤형 블록체인 It-chain을 만든다. It-chain은 수정 용이한 구조를 가진 블록체인으로써 it-chain을 사용하는 사람들이 각자의 필요에 따라서 쉽게 수정할 수 있게 만들고자 한다.

또한 블록체인의 핵심이라고 할 수 있는 PBFT 합의 알고리즘이나 RAFT 리더 선출 알고리즘과같이 일반적인 이론을 통해서는 사람들에게 널리 알려져있지만 실제로 그것을 어떻게 구현할지 고민이 필요한 부분에 대해서 it-chain은 오픈소스로써 수 많은 해결책 중 한 가지를 제시하고자 한다.

It-chain이 이루고자 하는 것은 단순히 하나의 프로젝트에 그치지 않는다. 국내 블록체인 관련 오픈소스 커뮤니티이자 그 활성화를 위한 발걸음이 되고자 한다. 오픈소스는 진입장벽이 높아 프로젝트에 처음 기여하기까지 꽤 오랜 시간이 필요하기 마련이다. 특히, 블록체인 코어 개발에 대한 자료나 커뮤니티 등이 매우 부족하기 때문에 블록체인 관련 오픈소스에 기여하기는 더욱 어려울 수 밖에 없다. 그러나 it-chain은 slack 등의 메신저, 정기적인 오프라인 모임 등 활발한 자료 공유와 커뮤니케이션으로 오픈소스에 한발 더 쉽게 다가갈 수 있게 도울 수 있다.

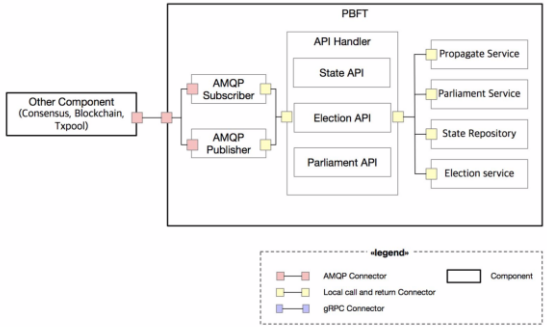
자신이 리더 노드일 경우, 트랜잭션 풀 컴포넌트(TxPool Component)로부터 요청을 받아 블록을 생성하고, 컨센서스 컴포넌트(Consensus Component)에 블록의 합의를 요청한다. 컨센서스 컴포넌트(Consensus Component)에서 합의를 완료하면, 네트워크 내 모든 노드는 해당 블록을 블록체인에 저장한다.



블록체인 동기화는 네트워크 내 모든 노드의 블록체인을 동일하게 하기 위한 과정으로, 새로운 노드가 네트워크에 참여할 시 다른 노드와의 블록체인 동기화를 진행한다.

이와 같이 it-chain은 각각의 완전히 독립적인 컴포넌트들이 모여서 전체 시스템을 구성하기 때문에 사용자의 필요에 따라서 수정이 용이하다는 장점이 있다. 예를 들어 현재 it-chain에서 사용하고 있는 PBFT 합의 알고리즘을 바꾸고 싶은 경우 컨센서스 컴포넌트(Consesus Component)의 도메인 로직만 교체하면 된다. 혹은 블록체인의 블록 구조를 바꾸고 싶은 경우에는 블록체인 컴포넌트(Blockchain Component)의 도메인 로직만 교체하면 그 니즈를 충족시킬 수 있다.

Consensus

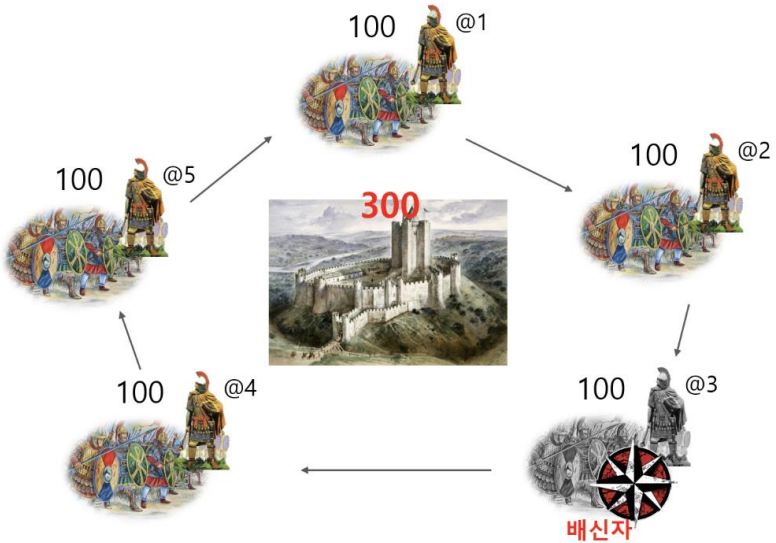


컨센서스 컴포넌트(Consesus Component)는 블록체인 컴포넌트(Blockchain Component)에서 생성된 블록(Block)에 대해, P2P 네트워크의 구성원들이 블록의 저장 순서에 대해 합의하는 역할을 수행한다. It-chain 에서 이러한 합의 과정은 PBFT 합의 알고리즘을 통해 구현되며, PBFT의 리더는 RAFT 리더 선출 알고리즘을 통해 선출된다.

It-chain - Consensus

비잔틴 장군 문제

- 5명중 3명 이상의 장군들이 같은 시각에 공격해야만 승리
- 장군들 중에서 배신자가 있어서 서로 신뢰할 수 없음



It-chain - Consensus

Consensus 알고리즘

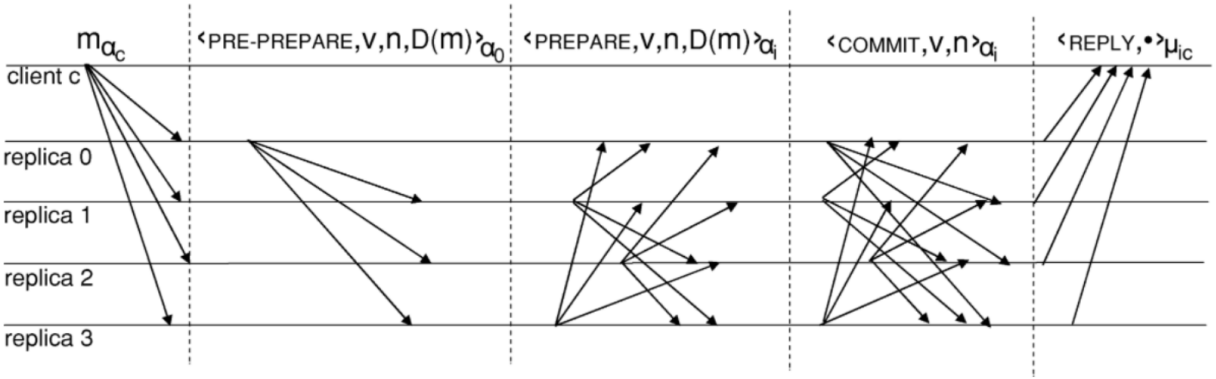
- 분산 프로세스 또는 시스템간의 단일 데이터 값에 대한 합의를 달성하는데 사용되는 알고리즘
- 여러 개의 신뢰할 수 없는 노드가 포함된 네트워크에서 안정성을 달성하도록 설계
- 비잔틴 장군 문제 해결

	PoW	PoS	PBFT
Major Blockchain Platform	Bitcoin, Ethereum	Cardano	Hyperledger fabric 0.6

It-chain - Consensus

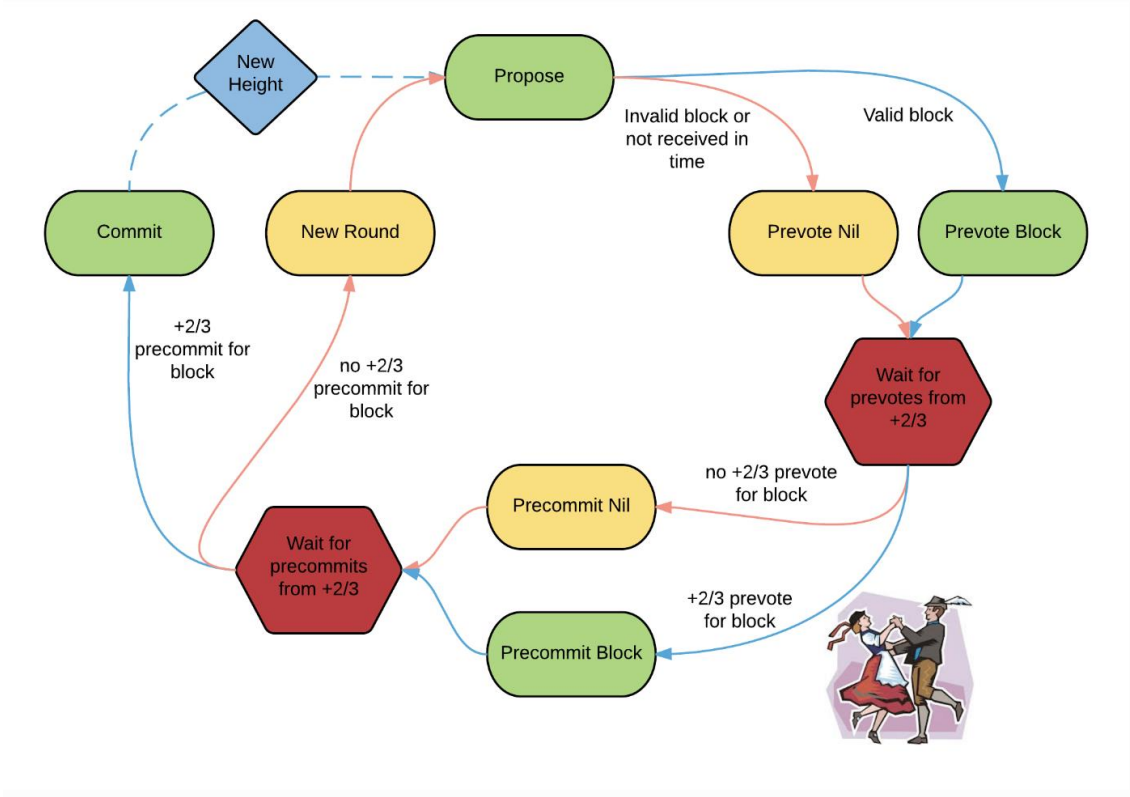
PBFT

- 1999년 Miguel Castro와 Barbara Riskop에 의해 도입 된 알고리즘
- 네트워크의 모든 노드는 사전에 알고 있어야하며, 한 노드는 리더



It-chain - Consensus

Tendermint



It-chain - Consensus

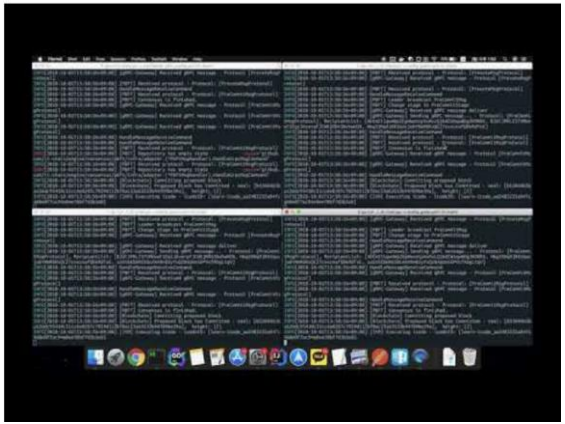
It-chain Consensus 알고리즘

- Permissioned P2P Network(Private Network)
- 소수의 노드로 구성
- 빠른 합의 속도

➔ PBFT Consensus 알고리즘 사용

진행상황

- 8월 Solo 모드 구현 완료
- 10월 초 PBFT 알파 버전(매우 불안정)
- ICode 튜토리얼 제공 중
  - https://github.com/junbeomlee/learn-icode
  - https://github.com/it-chain/engine/blob/develop/doc/TUTORIAL.md



https://www.youtube.com/watch?v=ivVhqk2er14

오픈소스 커미터로 블록체인 개발하기

SOSCON 2018

SAMSUNG OPEN SOURCE CONFERENCE 2018

오픈소스 커미터로 블록체인 개발하기 - 시작

SOSCON 2018

오픈소스 커미터로 블록체인 개발하기 - 팀 구성

- Nexters 연합 개발 동아리
- 5명의 개발자, 3명의 디자이너

오픈소스 커미터로 블록체인 개발하기 - 준비

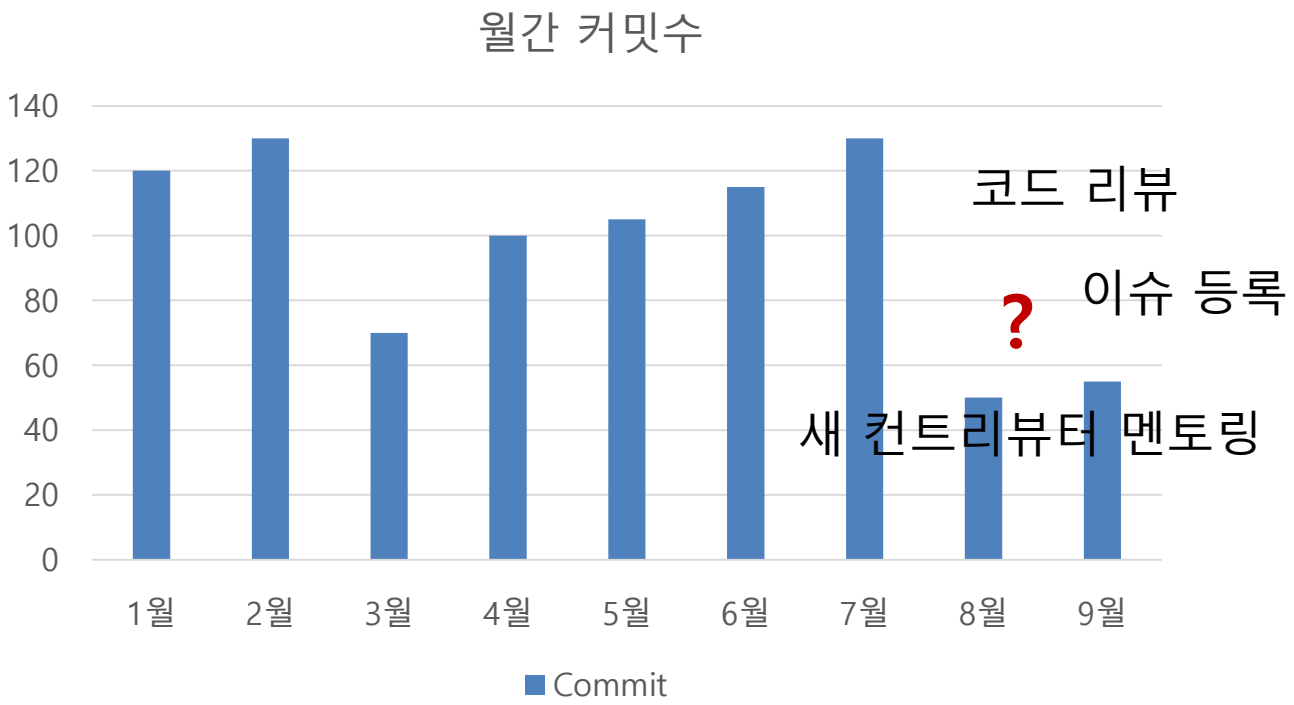
- Coding Style
- TDD
- Documentation
- Template(Issue, Pull request)
- Issue
- CI
- Test coverage

Feature/consensus/implement leader election ✓

#830 by frontalnh was merged 15 days ago • Approved

145 ?

오픈소스 커미터로 블록체인 개발하기 - 힘듦



오픈소스 커미터로 블록체인 개발하기 - 즐거움

- 열정적인 팀원(매주 2회 오프라인 미팅)들의 **자극**
- 코드 리뷰를 통해 함께 **성장**
- 독자를 고려한 코딩의 **습관**

THANK YOU

SOSCON 2018

SAMSUNG OPEN SOURCE CONFERENCE 2018