Noname manuscript No.
(will be inserted by the editor)

Insert your title here

Do you have a subtitle? If so, write it here

First Author · Second Author

Received: date / Accepted: date

초록 본 서베이 논문은 비잔틴 장애를 허용(Byzantine-fault-tolerant)하는 상태 머신 복제(State Machine Replication) 알고리즘과 블록체인의 분산 원장에 활용되는 기술 등을 다룬다. 많은 수의 기업들은 정보 시스템을 활용하는 사업 아이템을 구상하고 있으며 IT 시스템에 대한 의존성은 높아지고 있다. 그리고 개발 비용을 절감하면서 생산성을 높이고 더 안정적인 시스템을 구축하기위해 타사의 API 서비스나 클라우드를 이용하여 새로운 시스템을 개발하는 추세이다. 그래서 현대의 대부분의 서비스는 분산된 노드가 서로 정보를 주고 받으며 동작한다. 이 과정에서 분산된 노드간에 동일한 설정 유지할때나 하나의 상태를 갖는 분산 컴포넌트를 개발할때 상태 머신 복제 알고리즘은 중요한 역할을 하게 된다. 상태 복제 알고리즘은 오랫동안 연구되어 왔으며 최근 블록체인의 발전으로 그 중요성이 부각되고 있다. 또한 HotStuff 같은 알고리즘의 등장으로 성능이 획기적으로 개선되기도 하였다. 이 서베이 논문은 비잔틴 장애 허용 알고리즘을 다루고 알고리즘 간에 성능 및 장단점을 비교하여 설명한다.

1 서론

소프트웨어의 이미 제작된 컴포넌트를 재활용할 수 있는 장점 덕분에 아이디어만 있다면 새로운 앱을 구현하는데 많은 시간을 들이지 않을 수 있다. 언어와 개발 도구의 발달, 오픈소스와 생태계의 발전, 웹 기술의 발전은 재활용 가능한 소프트웨어를 누구나 쉽게 구현하고 제공할 수 있게 하였다. 단순한 라이브러리나 프레임워크 수준을 넘어선 API 서비스의 등장으로 코드 뿐만 아니라 서비스 자체를 재활용하는 것이 가능해졌다. 분산된 노드의 통신이 빈번한 환경에서는

F. Author
first address
Tel.: +123-45-678910
Fax: +123-45-678910
E-mail: fauthor@example.com

S. Author
second address

악의적인 공격자에 의해 해킹을 당하기 쉽다. 해커는 시스템 중 약한 부위를 공격하여 루트권한을 획득하고 제어서버를 통해 시스템을 원하는 대로 조작할 수 있다. 위와 같은 분산된 환경에서 해커의 공격을 대응하는 것이란 개발자 입장에서 단순히 시스템의 장애를 해결하는 것 이상의 어려운 일이다. 또한 점점 시스템에 많고 중요한 데이터가 저장되기 때문에 악의적인 공격을 당했을때 그 피해는 어마어마하다.

다양한 분산 환경 중 여러 노드가 하나의 시스템 처럼 동일한 상태를 유지하고 서비스를 제공하는 경우가 있다. 특히 악의적인 노드가 존재하는 비잔틴 문제가 있더라도 시스템이 중요한 동작할 수 있게 해주는 비잔틴 장애 허용 상태 머신 복제 알고리즘은 보안성을 강화하기 위해 널리 활용되는 알고리즘이 되었다. 항상 시스템을 보호해주는 알고리즘은 아니고 3f+1개의 노드 중 f개 이하로 결함있는 노드가 유지될때 문제없이 상태를 복제할 수 있게한다.

흔히 알려진 것 처럼 상태 머신 복제 시스템은 safety와 liveness 성질을 가지고 있어야 한다. safety는 사용자가 전송한 시스템의 상태를 갱신하는 일련의 명령을 모든 노드가 동일한 순서대로 실행하여 같은 상태를 갖게해주는 능력이다. liveness는 사용자 요청에 대한 응답을 해주는 능력을 의미한다.

최근에 상태 복제 머신이 활용되는 분야 중 하나는 블록체인(Blockchain)이다. 블록체인은 수 많은 분산원장으로 구성된다. 일반적으로 모든 분산 원장은 동일한 암호화폐 거래내역을 저장해야 하며 거래 요청 처리 순서를 동기화 해야한다. 여기서 각 분산된 노드는 계좌내역(계좌번호, 잔액 등) 이라는 상태를 가지고 있고 이 상태를 모두 동일하게 복제하기 위해 상태 머신 복제 알고리즘이 사용되는 것이다.

예를들어 비트코인은 작업 증명(Proof of Work) 알고리즘을 활용하여 상태를 복제한다. 작업증명 알고리즘은 서비스 거부 공격을 방어하기 위해 개발되었지만 비트코인에서 각 노드간 동일한 블록과 블록체인을 유지하는데 사용되면서 유명해졌다.

그리고 노드는 태생부터 결정적(deterministic) 속성을 가지고 있어 거래 요청 처리 순서가 동일할 경우 같은 계좌 내역을 갖게 된다.

가장 널리 알려진 PBFT는 비동기 환경에서 비잔틴 문제를 해결할 수 있는 최초의 알고리즘이다. 실행 결과 커밋까지 3가지 단계 Pre-Prepare, Prepare, Commit로 구성되며 Pre-Prepare과 Prepare 단계는 동일한 순서로 명령이 실행되는 것을 보장하며, Prepare과 Commit 단계는 커밋된 명령이 여러 뷰에서 완전히 정렬되는 것을 보장한다. 이후 PBFT의 성능을 개선한 많은 변형이 탄생하였다.

그리고 2019년 현대 시스템 환경에서 PBFT보다 빠르고 실용적인 리더 기반 상태 머신 복제 알고리즘 HotStuff이 등장하였다. HotStuff는 리더 기반 프로토콜로 부분적으로 동기 모델(Partially Synchronous Model)에서 동작하는 상태 머신 복제 알고리즘이다. 네트워크 커뮤니케이션이 동기적일때 네트워크 지연시간의 속도에 맞춰 합의에 도달할 수 있게 해주는 responsiveness 속성을 보장한다. 그리고 복제본의 수에 선형적인 통신 복잡도를 갖는 linearity를 보장한다. 아마 HotStuff는 위 2가지 속성을 갖는 최초의 부분 동기화 BFT 복제 프로토콜이며, 거대한 복제 서비스에서 활용될 수 있는 여러가지 성능 최적화를 제공한다.

그리고 같은 해인 2019년에 LibraBFT라는 Libra 블록체인을 위한 알고리즘이 등장한다. LibraBFT는 HotStuff 알고리즘을 기반으로 몇가지 아이디어가 추가된 알고리즘이다. LibraBFT는 새로운 라운드 동기화 매커니즘을 제공하며,

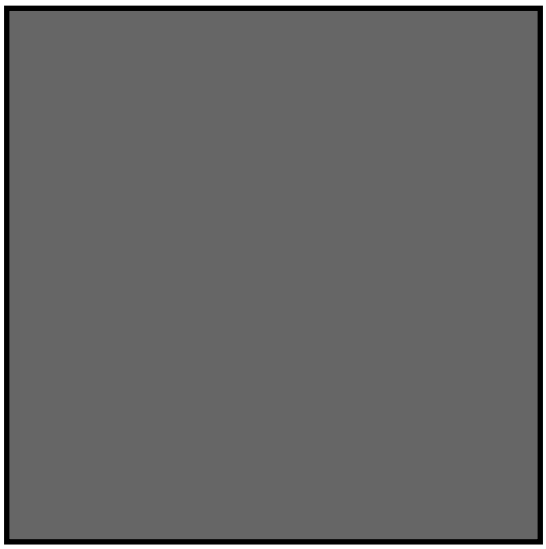

Fig. 1 Please write your figure caption here

Table 1 Please write your table caption here

first	second	third
number	number	number
number	number	number

결함있는 리더 노드가 존재하더라도 제안이 커밋되는 것을 허용하는 nil-block 투표 방식 등을 제공한다.

2 논문 분석

Text with citations [2] and [1].

2.1 Subsection title

as required. Don't forget to give each section and subsection a unique label (see Sect. 2).

Paragraph headings Use paragraph headings as needed.

$$a^2 + b^2 = c^2 \tag{1}$$

3 토론

Text with citations [2] and [1].

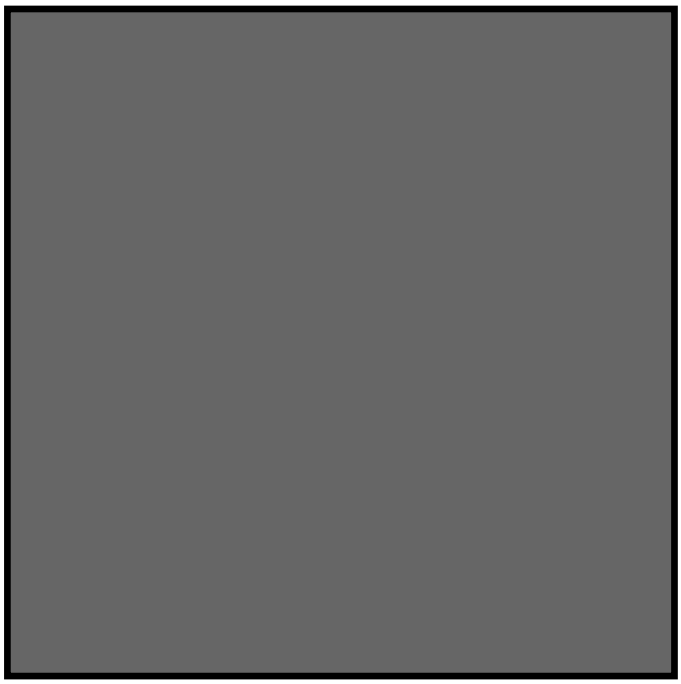

Fig. 2 Please write your figure caption here

4 결론

Text with citations [2] and [1].

References

1. Author, Article title, Journal, Volume, page numbers (year)
2. Author, Book title, page numbers. Publisher, place (year)