한국정보전자통신기술학회논문지(jkiiect)'19-4 Vol.12 No.2
논문 19-12-02-155 http://dx.doi.org/10.17661/jkiiect.2019.12.2.155

하이퍼레저 패브릭 블록체인을 활용한 시스템 복구 기법

배수환*, 조선옥, 신용태**

A System Recovery using Hyper-Ledger Fabric BlockChain

Su-Hwan Bae*, Sun-Ok Cho, Yong-Tae Shin

요 약 오늘날 수많은 기업과 기관들은 인터넷을 사용한 서비스를 제공하고 있으며, 이를 효율적이고 안정적으로 관리할 수 있도록 정보시스템을 구축하고 운영한다. 정보시스템은 재해 또는 장애로 인해 정상적인 서비스를 제공 할 수 있는 기능을 손실할 가능성을 내포하고 있다. 이에 재해복구시스템을 활용하여 이를 대비하고 있다. 그러나 기존의 재해 복구시스템은 시스템 복구를 위한 파일이 손상되는 경우 정상적으로 복구를 수행할 수 없다. 이에 본 논문에서는 하이퍼레저 패브릭 블록체인을 활용하여 시스템 복구 파일의 무결성을 검증하고 복구를 진행할 수 있는 시스템을 제안한다. 블록 생성을 위하여 PBFT 합의 알고리즘을 사용하며, 블록체인 네트워크의 리더 노드에 의해 수행된다. 장애 상황 발생 시 복구 대상의 복구 파일의 해시 값을 블록체인 내의 해시 값과 비교하는 검증 작업을 거쳐 복구 파일의 무결성을 확인하고 복구를 진행한다. 제안 기법의 평가를 위하여 기존의 시스템 복구기법과 데이터 정합성, 데이터 보존 여부, 복구 파일 무결성 검증, 제안 기법 사용 시 트래픽 발생량을 분석하여 실제 적용 가능 여부를 확인하였다.

Abstract Currently, numerous companies and institutes provide services using the Internet, and establish and operate Information Systems to manage them efficiently and reliably. The Information System implies the possibility of losing the ability to provide normal services due to a disaster or disability. It is preparing for this by utilizing a disaster recovery system. However, existing disaster recovery systems cannot perform normal recovery if files for system recovery are corrupted. In this paper, we proposed a system that can verify the integrity of the system recovery file and proceed with recovery by utilizing hyper-ledger fabric blockchain. The PBFT consensus algorithm is used to generate the blocks and is performed by the leader node of the blockchain network. In the event of failure, verify the integrity of the recovery file by comparing the hash value of the recovery file with the hash value in the blockchain and proceed with recovery. For the evaluation of proposed techniques, a comparative analysis was conducted based on four items: existing system recovery techniques and data consistency, able to data retention, recovery file integrity, and using the proposed technique, the amount of traffic generated was analyzed to determine whether it was actually applicable.

Key Words : BlockChain, Disaster Recovery, Hyper-Ledger Fabric, Smart Contract, System Recovery

1. 서론

오늘날 정보통신기술의 발전으로 많은 기업과 기관들은 인터넷을 사용하여 서비스를 제공하고 있다. 이를 효율적이고 안정적으로 관리하기 위하여 정보시스템을 구축하고 운영하고 있다. 하지만 각종 재해나 장애가 발생할 경우 정보시스템이 정상적인 기능을 수행하지 못하는 상황이 발생하면서 대비책으로 재해복구시스템을 도입하였다. 하지만 기존의 시스템은 복구 파일이 변경되는 경우 정상적인 역할을 수

**Corresponding Author : Dept. of Computer Science, Soongsil University (shin@ssu.ac.kr)
*Dept. of Computer Science, Soongsil University
Corp. LIME Company
Received April 09, 2019 Revised April 17, 2019 Accepted April 24, 2019

행할 수 없는 문제점이 존재한다. 이에 하이퍼레저 패브릭 블록체인을 활용하여 복구 파일을 생성하고 시스템 복구가 필요한 경우 이를 검증하여 정상적인 복구를 진행할 수 있는 시스템을 제안한다.

본 논문의 구성은 2장에서 제안하는 기술을 위한 관련연구에 대하여 기술한다. 3장에서는 제안하는 기술인 하이퍼레저 패브릭 블록체인을 활용한 시스템 복구 기법에 대하여 설명한다. 4장에서는 제안 기법을 데이터 정합성, 데이터 보존성, 복구 파일 무결성 검증, 제안 기법의 해시 알고리즘 성능 평가의 세 가지 항목에 대하여 평가한다. 마지막으로 5장에서는 본 논문에서 성능평가로부터 도출된 결과로 제안하는 기술의 효용성에 대한 내용을 결론으로 다룬다.

2. 관련 연구

본 장에서는 제안하는 기술의 기반이 되는 재해복구시스템, 블록체인, PBFT에 대하여 설명한다.

2.1 재해복구시스템

재해복구시스템은 재해가 발생 했을 때 재해복구 계획을 통해 신속하게 시스템을 복구하는 시스템을 말한다[1].

재해복구시스템의 구축형태는 독자구축, 공동구축, 상호구축 세 가지의 형태로 구분되며 운영형태는 자체운영, 공동운영, 위탁 운영의 세 가지로 구분된다. 다음의 표 1과 표2는 재해복구시스템의 운영방식별 특징을 나타낸다[1].

표 1. 구축 형태별 재해복구방식의 특징
Table. 1. Compare of Block Chain Network

Kind of deployment	Cost of deployment	Cost of operation	security	Recovery Reliability
Self	High	High	High	High
Co-work	Middle	Middle	Middle	Middle
Mutual	Low	Low	Low	Low

표 2. 운영 주체별 재해복구방식의 특징
Table. 2. Compare of Block Chain Network

Kind of deployment	Cost of deployment	Cost of operation	security
Self	High	High	High
Co-work	Middle	Dependent on negotiation	
Consignment	Low	Dependent on reliability	

제안 기법에서는 독자적으로 구축한 정보시스템과 자체적으로 운영하는 상황을 기반으로 동작하는 시스템이 사용된다.

2.2 블록체인

기존의 보안 기술은 암호화 혹은 접근 통제 등의 방식을 사용하여 원하는 정보를 보호하는 형태였다. 반면에 블록체인은 데이터를 숨기는 형태가 아닌 네트워크에 참여한 모두에게 공개한다. 이를 통해 모든 노드가 동일한 내용을 알고 있어 위변조가 발생해도 인정되지 못하게 만드는 방식이다[2]. 블록체인의 목적은 블록체인을 이용하여 복잡한 시스템을 간단하게 만들며, 데이터를 동기화 하여 조직간 혼선을 방지하는 것이다[3].

블록체인에서 생성된 블록은 다음의 그림 1처럼 서로 연결되어 있는 체인과 같은 대형을 가지며, 가장 길게 연결된 체인을 정상 체인으로 인식한다[4][5]. 또한 블록 페이로드의 무결성 검증을 위해서 해시 트리를 사용하여 이를 해결한다. 블록체인의 네트워크 유형으로는 퍼블릭, 프라이빗 두 가지로 구분된다. 각 네트워크 유형의 특징은 다음의 표 3과 같다.

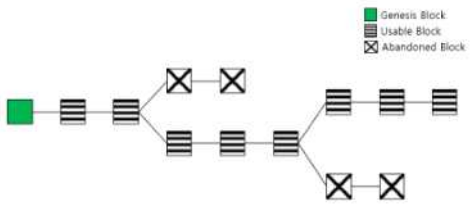

그림 1. 블록체인의 대형
Fig. 1. Formation of Block Chain

표 3. 블록체인 네트워크의 비교
Table. 3. Compare of Block Chain Network

	Public Block chain	Private Block chain
Read Permission	Don't Care	Authenticated User
Authentication and Commit	Don't Care	Authenticated User
Create Transaction	Don't Care	Authenticated User
Authorization	Not use	Use
Example	Bitcoin, Ethereum	Fabric, R3 Corda

2.3 BFT(Byzantine Fault Tolerance)

BFT는 동일한 네트워크에 악의적인 노드가 있고 시간 동기화가 이루어져 있지 않을 경우 발생하는 문제이다[6]. BFT는 블록체인 네트워크에서 서로 가지고 새로운 블록들이 생성될 때 일부 노드들이 가지고 있는 정보가 다른 노드들이 가지고 있는 정보과 상이할 수 있다. 이에 노드 간 상태가 일치되지 않는 것을 해결해주기 위한 합의 알고리즘이 필요하다. 이를 해결하기 위한 방식이 PBFT(Practical Byzantine Fault Tolerance)이다. PBFT는 네트워크에 포함되어 있는 노드들이 전달받은 정보를 다른 노드들과 비교하고 동일한 정보를 받았는지 재확인하는 절차를 진행한다. 다음의 그림 2는 PBFT의 동작 절차이다[7].

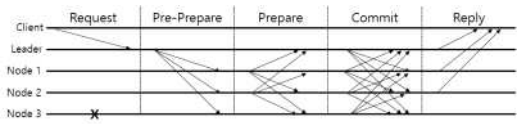

그림 2. PBFT 동작 절차
Fig. 2. Procedure of PBFT

① 클라이언트는 자신이 원하는 결과물을 얻기 위해 리더 노드에게 작업 수행 요청을 한다.
② 리더 노드는 요청 받은 사항을 네트워크 내의 다른 노드들에게 전파한다.
③ 각 노드는 자신이 받은 내용을 네트워크의 다른 노드들에게 재전송하여 동일한 내용을 받았는지 확인한다.
④ 전송받은 내용이 동일하다면 요청한 작업을 수행하고 이에 대한 결과를 모든 노드에게 전파한다.
⑤ 클라이언트에게 결과물을 제공한다.

3. 제안하는 시스템 복구 기법

본 장에서는 제안하는 기법인 하이퍼레저 패브릭 블록체인을 활용한 시스템 복구 기법에 대하여 설명한다. 제안 기술은 프라이빗 블록체인 네트워크 구성을 가지며 합의 알고리즘으로 PBFT를 사용하여 블록을 생성한다.

3.1 제안 기법의 구조

3.1.1 제안 기법의 물리적 구조

제안 기법의 물리적 구조는 다음의 그림 3과 같다.

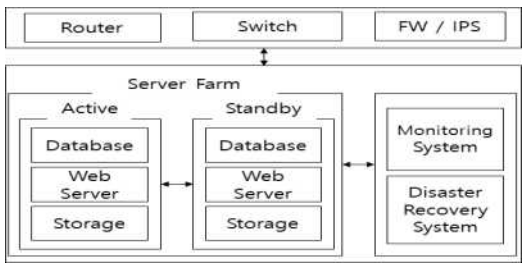

그림 3. 제안 기법의 물리적 구조
Fig. 3. Structure of Proposed Technique

제안 기법에서 정보시스템은 네트워크 장비를 통해 외부 인터넷으로 연결된다. 서버팜 내의 서버는 Activce-Standby 형태로 실시간으로 동기화되는 형태로 구성된다. 통합관제 시스템과 재해복구 시스템은 서버팜에 연결되어 실시간으로 모니터링을 수행하며 장애 발생 시 복구를 위해 사용된다.

3.1.2 블록 구조

제안 기법의 블록 구조는 다음의 그림 4와 같다.

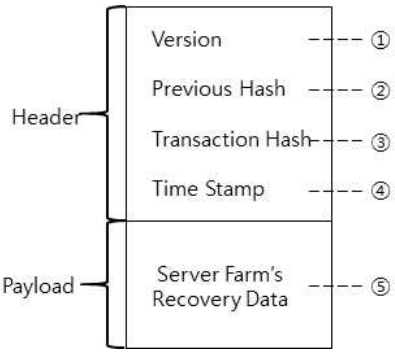

그림 4. 제안 기법의 블록 구조
Fig. 4. Block Format of Proposed Technique

① 현재 블록체인의 버전을 명시한다.
② 블록을 체인으로 연결하기 위해 이전 블록의 해시 값을 사용한다.
③ 트랙잭션의 정보를 해시하여 트리로 구성하고 트리의 루트 해시 값을 사용한다.
④ 블록 생성 시간을 표기하기 위해 사용한다.
⑤ 서버팜 내의 모든 서버들의 복구 데이터의 해시 값을 트랜잭션으로 사용한다.

3.2 블록 생성 및 등록 절차

제안하는 기법에서 블록생성은 서버팜 내의 Active-Standby 서버와 재해복구 시스템에서 수행한다. Active 서버가 스마트 컨트랙트를 실행시키고 참여 노드간의 합의 과정을 거쳐 생성된다. 블록 생성 절차는 다음의 그림 5와 같다.

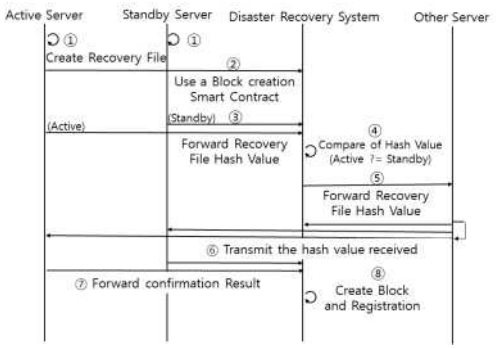

그림 5. 블록 생성 및 등록 절차
Fig. 5. Process of Block Creation and Linking

① Active-Standby 서버는 자신의 복구를 위해 사용할 복구 파일을 생성한다. 생성 주기는 관리자가 정한 시점마다 실행된다.
② Acitve 서버는 복구파일 생성을 시작하는 동시에 스마트 컨트랙트를 실행시켜 재해복구시스템에게 블록생성작업을 시작하도록 요청한다.
③ Active-Standby 서버는 복구 파일 생성을 완료하고 재해복구시스템으로 복구파일의 해시 값을 전달한다.
④ 재해복구시스템은 전달 받은 두 개의 복구파일 해시 값을 비교하여 정상적으로 작업이 수행되었는지 확인한다.
⑤ 서버팜 내에 존재하며 블록체인 네트워크에 참여하는 다른 모든 서버들에게 복구파일의 해시 값을 전파한다.
⑥ 서버팜 내의 다른 서버들은 Active-Standb y, 재해복구센터, 또 다른 서버들에게 재전송하여 자신이 전달받은 해시 값을 공유한다.
⑦ 블록체인 네트워크 내의 모든 서버들은 서로 주고 받은 해시 값을 비교하고, 이 결과를 재해복구시스템으로 전달한다.
⑧ 재해복구 시스템은 전체 서버들이 전달해온 결과를 확인한 후 블록을 생성하며, 이를 체인에 등록한다.

3.3 시스템 복구 절차

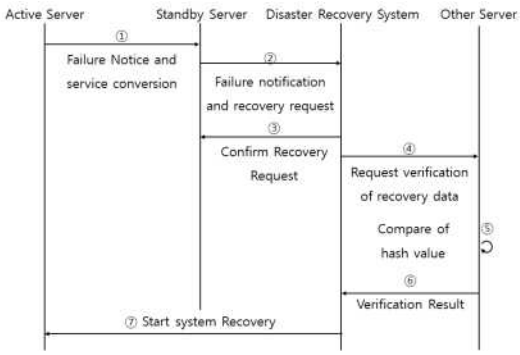

그림 6. 시스템 복구 절차
Fig. 6. Process of System Recovery

위의 그림 6은 시스템 복구 절차를 나타낸 그림

이다. 각 절차에서 수행되는 작업은 다음과 같이 진행된다.

① 장애 발생시 Active 서버는 Standby 서버에게 장애 사실을 통보하고 서비스 전환을 요청한다. 이때 자신이 소유한 복구 파일의 해시값 H_{Active}와 자신의 주소값 Add_{Active}를 전달한다.

② Standby 서버는 서비스를 전환하고 재해복구 시스템에게 장애상황에 대해 통보한다. 이때 Active 서버로부터 전달받은 H_{Active}와 Add_{Active}를 재해복구시스템으로 전달하고 복구 요청을 보낸다.

③ 재해복구시스템은 복구 요청을 접수하고 Standby서버에게 정상적으로 요청 받았음을 확인한다.

④ 재해복구시스템은 다른 서버들에게 H_{Active}와 Add_{Active}를 전파하고 각 서버에서 해당 해시값의 정상 유무 검증을 요청한다.

⑤ 각 서버들은 Add_{Active}에 해당하는 해시 트리를 검색하고 트리의 가장 최근 해시값인 H_{Tree}와 H_{Active}값이 동일한지 비교한다.

⑥ ⑤의 작업에서 비교한 결과를 재해복구 센터로 전달하고, 재해복구 시스템은 전체 결과를 취합하여 전체의 2/3 이상이 정상이라고 판단하면 복구를 수행한다. 이때 2/3에 도달하지 않는다면 Standby 서버가 소유한 $H_{Standby}$를 전달받아 ④~⑤ 작업을 재수행한다.

⑦ 재해복구시스템은 Active 서버의 복구를 진행한다.

4. 성능평가

본 장에서는 제안 기술인 하이퍼레저 패브릭을 활용한 시스템 복구 기법에 대하여 데이터 정합성, 데이터 보존 가능 여부, 복구파일 무결성 검증 세 가지 항목에 대하여 비교 분석을 실시한다. 또한 제안 기법의 트래픽 발생량을 평가하여 실제 적용 가능 여부를 분석한다.

4.1 데이터 정합성 비교 분석

데이터 정합성 항목은 현재의 데이터와 복구했을 때의 데이터가 일치하는 정도를 나타낸다. 비교 분석 시 복구가 진행되었을 경우 데이터의 정합도가 100% 일치할 경우 High, 일치하지 않는 경우 Low로 평가한다. 동기식 방식과 제안 기법의 경우 Active 서버에 장애가 발생할 경우 이중화 되어있는 Standby에서 서비스를 이어받기 때문에 데이터 정합성의 차이가 발생하지 않는다. 반면, 비동기식의 경우 복구에 사용하는 데이터를 관리자가 지정한 특정 시간에 진행한다. 이는 장애가 발생하고 복구가 진행 되었을 때 정상적으로 서비스를 제공하였을 때와 비교하였을 때 차이가 발생하게 된다. 이에 동기식 방식과 제안 기법의 데이터 정합성은 High, 비동기식의 데이터 정합성은 Low로 평가한다.

4.2 데이터 보존 가능 여부 비교

데이터 보존성은 서버에 장애가 발생하여 데이터 자체의 손실이 발생하더라도 기존의 데이터를 보존할 수 있는지에 대한 사항이다. 데이터 보존 가능성 여부는 사용 가능 및 불가능 두 가지 항목으로 평가한다. 동기식 방식의 경우 Active-Sta ndby의 이중화 구성으로 동작하여 서버에 문제가 발생하는 경우 서비스를 이전하여 동작하는 형태를 가진다. 다만, 두 서버 모두에 문제가 발생하는 경우 데이터를 보존할 수 없다는 단점이 존재한다. 반면, 비동기식 방식과 제안기법에서는 복구에 사용할 복구 파일을 생성하여 보관하고 있어, 두 서버 모두에 문제가 발생하여도 복구를 진행할 수 있다. 이를 통해 데이터 보존이 가능하다.

4.3 복구 파일 무결성 검증 기능 평가

복구 파일 무결성 검증 기능 평가는 무결성 검증 가능 여부를 통해 비교 분석을 실시한다. 복구 파일 무결성 검증의 경우 기존의 동기식, 비동기식 방식은 복구 파일 자체가 손상 되었을 때 이를 자체적으로 해결하는 기술이 적용 되어 있지 않다. 그렇기 때문에 물리적으로 테이프나 저장장치에 분산 저장하는

형태로 리스크를 최소화 하는 방식을 사용한다. 반면, 제안하는 기법에서는 복구를 진행하기 이전에 복구 대상 서버가 가지고 있는 복구 파일의 해시 값을 블록체인 네트워크상의 공유 원장에서 비교한다. 이를 통해 복구에 사용하려는 파일의 무결성을 검증할 수 있는 기능을 얻는다. 또한 Active 서버가 소유한 복구 파일에 문제가 발생했을 경우, 자동으로 Standby 서버가 소유한 복구 파일을 사용하여 복구할 수 있는 기능을 제공하여 복구 시간을 단축 시킬 수 있다. 위의 세 가지 항목을 토대로 성능평가를 실시했을 때 제안 기법의 성능은 아래의 표 4와 같이 평가된다.

표 4. 시스템 복구 성능 비교
Table. 4. Compare of System Recovery Performance

Evaluation Item	Synchronous	Asynchronous	Proposed
Data Consistency	High	Low	High
Data Retention	Not Available	Available	Available
Verification of Recovery file	Not Available	Not Available	Available

4.4 제안 기법의 트래픽 발생량 분석

본 절에서는 제안 기법의 트래픽 발생량을 확인하고 제안 기법을 사용했을 때 시스템에 영향을 미칠 수 있는지에 대한 여부를 분석한다. 전체 노드 수가 N개 일 때 PBFT 합의 알고리즘을 사용할 경우 발생하는 트래픽은 Pre-Prepare, Prepare, Commit, Reply의 세 가지 상황에서 발생한다. 각 단계에서 발생되는 트래픽을 수식으로 작성하면 (1)~(4)와 같다.

$$T_{\mathrm{Pre-Prepare}} = N-1 \quad (1)$$

$$T_{\mathrm{Prepare}} = N(N-1) \quad (2)$$

$$T_{Commit} = N(N-1) \quad (3)$$

$$T_{Reply} = N \quad (4)$$

위의 식을 통해 발생되는 트래픽의 총량을 계산하면 (5)와 같은 식으로 도출된다.

$$T \quad (5)$$

PBFT의 특성상 최소 4개 이상의 노드가 필요하기 때문에 노드가 4개 이상일 때의 트래픽 발생량을 그래프로 나타내면 다음의 그림 7과 같다.

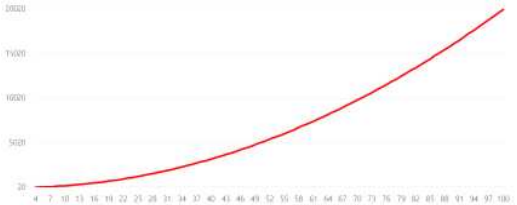

그림 7. 제안기법의 트래픽 발생량
Fig. 7. Amount of Traffic using proposed technique

정보 시스템에서는 초당 수십만개에서 수백만개까지의 트래픽을 처리한다. 제안 기법을 활용하면 기존 기법들에서 불가능한 복구 파일의 무결성 검증이 가능하다. 이를 위해 발생하는 트래픽 량이 위의 결과와 같이 발생하는 경우, 현재의 정보시스템에서 처리할 수 있는 트래픽에 문제가 발생하지 않는다. 또한 정상적인 서비스를 제공하는데 지장이 발생하지 않는 환경으로 제안하는 기법이 동작가능하다.

5. 결론

최근 기업들은 정보시스템을 구축하고 재해나 장애로부터 대비하기 위한 재해복구시스템을 구축하고 있다. 이러한 노력에도 불구하고 기존의 재해복구시스템은 복구에 사용하는 파일이 변질되었을 때 정상적인 복구를 진행하는데 어려움이 존재했다. 이에 본 논문에서는 하이퍼레저 패브릭 블록체인을 활용하여 시스템 복구를 진행할 수 있도록 하였다. 정보 시스템 내부에 존재하는 서버들이 블록체인 네트워크 노드에 참여하여 복구 파일의 해시 값을 사용하여 블록을 생성하고 체인에 등록한다. 또한 복구를 진행할 때 블록체인 원장에 기재된 내용과 현재 복구 파일의 해시 값을 비교하는 형태를 사용하여 복구 파일 변질 여부를 확인하고 정상적인 복구를 진행한다.

제안 기법의 성능 평가로 데이터 정합성, 데이터

보존성, 복구 데이터 무결성 보장, 복구 파일의 무결성 검증의 세 가지 항목에 대하여 평가하였다. 성능 평가 결과 동기식 방식의 높은 데이터 정합성과 비동기식 방식의 데이터 보존성의 특성을 모두 제공할 수 있음을 확인하였다. 또한 기존의 방식의 문제점인 복구 파일의 무결성 검증을 수행하는데 발생되는 트래픽이 있더라도 서비스에 영향을 끼칠 정도가 아님을 확인하였다. 이를 통해 안정적인 시스템 복구 기법으로 동작 가능하며, 기존의 서비스를 정상적으로 제공 가능하다.

REFERENCES

[1] National Information Society Agency. “Guideline for Disaster Management of Information System”. Ministry of Informat ion and Communication. 2005.

[2] IBM. “What is blockchain?”. 2019.

[3] Noguchi Yukio. “The Impact of the Blockchain”. BookSta., 2017.

[4] Satoshi Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System”. 2009.

[5] Vitalik Buterin. “Ethereum White Paper A Next Gerneration Smart Contract & Decentrali zed Application Platform”. 2014.

[6] Kevin Driscoll et al. “Byzantine Falut Tolerance, from Theory to Reality”. Compupter safty, Realiability, and Security. pp235-248. 2003.

[7] Miguel Castro, Barbara Likov. “Practical Byzantine Fault Tolerance”. Third Symposium on Operating System Design and Implementation. 1999.

저자약력

배 수 환(Su-Hwan Bae) **[정회원]**

•2016.03 - 2018.02,
숭실대학교 일반대학원
융합소프트웨어학과 석사
•2018.03 - 현재,
숭실대학교 일반대학원
컴퓨터학과 박사과정

〈관심분야〉 블록체인, 정보보호, 컴퓨터 통신, 5G

조 선 옥(Sun-Ok Cho) **[정회원]**

•2017.03 - 현재.
숭실대학교 일반대학원
IT정책경영학과 박사과정
•2019 - 현재,
라임컴퍼니 대표이사

〈관심분야〉 IT 서비스경영, 마케팅전략, 서비스 분야

신 용 태(Yong-Tae Shin) **[정회원]**

•1991 - 1994,
University of Iowa
컴퓨터학과 공학 박사
•1995.03 - 현재,
숭실대학교 컴퓨터학부
교수

〈관심분야〉 컴퓨터네트워크, 분산 컴퓨팅,
인터넷 프로토콜, 초고속통신망, 전자상거래 기술