(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0062355
(43) 공개일자 2024년05월09일

(51) 국제특허분류(Int. Cl.)
H04L 67/1042 (2022.01) *G06F 16/27* (2019.01)
H04L 67/289 (2022.01) *H04L 67/52* (2022.01)
(52) CPC특허분류
H04L 67/1042 (2022.05)
G06F 16/278 (2019.01)
(21) 출원번호 10-2022-0142805
(22) 출원일자 2022년10월31일
심사청구일자 2022년10월31일

(71) 출원인
포항공과대학교 산학협력단
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
박찬익
경상북도 포항시 남구 청암로 77
조용래
경상북도 포항시 남구 청암로 77
(74) 대리인
특허법인이상

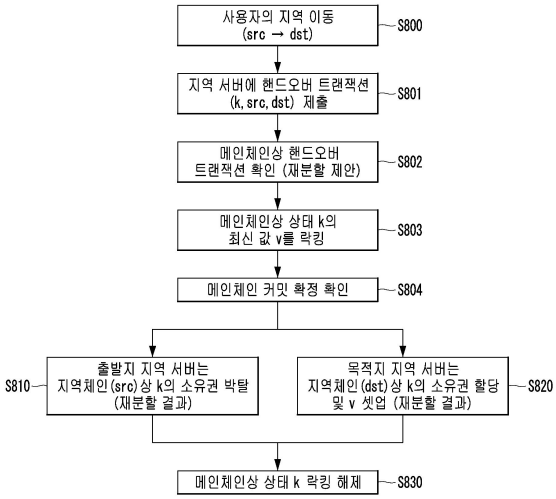
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **샤딩 블록체인 플랫폼에서 동적 지역성 지원을 위한 상태 재분할 방법 및 장치**

(57) 요 약

상태 정보를 기준으로 분할하는 샤딩 블록체인 플랫폼에서 동적 지역성 워크로드를 활용하기 위해 필요한 샤드 재구성을 효과적으로 수행할 수 있는 상태 재분할 방법 및 장치가 개시된다. 상태 재분할 방법은, 지역 내 통신 노드로부터 트랜잭션을 수신하는 단계, 수신된 트랜잭션을 포함한 로컬 체인상의 로컬 체인 블록을 메인 체인상의 메인 체인 블록으로 통합하는 단계, 메인 체인 블록상의 트랜잭션이 미리 설정된 유형의 특정 트랜잭션인지를 확인하는 단계, 및 수신된 트랜잭션이 특정 트랜잭션일 때, 수신된 트랜잭션을 상태 재분할 대상 집합에 추가하는 단계를 포함한다.

대 표 도 - 도8



(52) CPC특허분류
H04L 67/289 (2022.05)
H04L 67/52 (2022.05)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711125876
과제번호 2020-0-00936-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 블록체인융합기술개발
연구과제명 5G 초저지연 서비스를 위한 무선 단말용 블록체인 기술 개발
기 여 율 1/2
과제수행기관명 포항공과대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711152571
과제번호 2021-0-00484-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 데이터 경제를 위한 블록체인 기술개발(R&D)
연구과제명 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크 프로토콜 기술개발
기 여 율 1/2
과제수행기관명 포항공과대학교 산학협력단
연구기간 2022.01.01 ~ 2022.12.31

명 세 서

청구범위

청구항 1

블록체인 플랫폼 기반으로 동적 지역성을 지원하는 지역 서버의 상태 재분할 방법으로서,

지역 내 통신 노드로부터 트랜잭션을 수신하는 단계;

수신된 트랜잭션을 포함한 로컬 체인상의 로컬 체인 블록을 메인 체인상의 메인 체인 블록으로 통합하는 단계;

상기 메인 체인 블록상의 트랜잭션이 미리 설정된 유형의 특정 트랜잭션인지를 확인하는 단계; 및

상기 수신된 트랜잭션이 상기 특정 트랜잭션이면, 상기 수신된 트랜잭션을 상태 재분할 대상 집합에 추가하는 단계를 포함하는, 상태 재분할 방법.

청구항 2

청구항 1에 있어서,

상기 추가하는 단계는, 상기 확인하는 단계에서 선정된 재분할 대상 트랜잭션에 대한 재분할 제안(reshard proposal, RP)을 생성하는 단계, 및 상기 재분할 제안을 상기 메인 체인에 커밋하는 단계를 포함하는, 상태 재분할 방법.

청구항 3

청구항 2에 있어서,

상기 메인 체인에 커밋하는 단계는 상기 재분할 제안을 생성한 메인 체인 블록에 대한 합의 증명 데이터를 확보하는 것을 포함하며, 여기서 상기 합의 증명 데이터는 정족수(quorum)만큼의 합의 메시지를 포함하는, 상태 재분할 방법.

청구항 4

청구항 2에 있어서,

상기 메인 체인상에 상기 재분할 제안이 상기 메인 체인에 커밋되면, 상기 메인 체인 상의 상기 트랜잭션의 상태인 키의 가장 최신 값을 락킹하는 단계를 더 포함하는, 상태 재분할 방법.

청구항 5

청구항 4에 있어서,

상기 메인 체인의 커밋 확정에 의해 상기 합의 증명 데이터가 지역 서버에서 확인된 후, 상기 재분할 제안을 수행하는 단계를 더 포함하며,

상기 재분할 제안의 수행은 상기 재분할 제안에 기록된 출발지 지역의 지역 서버에서 상기 트랜잭션의 상태의 위상을 지역(Local)에서 전역(Global)으로 변경하는 것을 포함하고, 상기 위상의 변경에 따라 상기 출발지 지역의 지역 서버는 상기 상태에 대한 상태 소유권을 잃게 되는, 상태 재분할 방법.

청구항 6

청구항 5에 있어서,

상기 재분할 제안을 수행한 후에, 재분할 결과를 생성하는 단계를 더 포함하며, 여기서 상기 재분할 결과(reshard result, RR)는 목적지 지역의 지역 서버에서 트랜잭션 형태로 인코딩되고 상기 트랜잭션의 상태의 위상이 전역(Global)으로 기록되어 상기 메인 체인에 전달되는 것을 포함하는, 상태 재분할 방법.

청구항 7

청구항 6에 있어서,

상기 재분할 결과를 생성한 후에, 재분할 결과가 반영된 메인 체인 블록을 수신하고, 수신한 메인 체인 블록 상의 재분할 결과를 확인하는 단계를 확인하는 단계, 및 확인된 재분할 결과를 트랜잭션 형태로 인코딩하고 메인 체인 블록의 합의 증명 데이터에 삽입하는 단계를 더 포함하는, 상태 재분할 방법.

청구항 8

청구항 7에 있어서,

상기 확인된 재분할 결과에 대한 메인 체인 커밋이 확정되면, 재분할 결과를 수행하는 단계를 더 포함하며, 상기 재분할 결과의 수행은 목적지 지역의 지역 서버가 해당 트랜잭션에 포함된 상태의 위상을 전역(Global)에서 지역(Local)로 수정하고, 상기 상태의 값을 상기 목적지 지역의 지역 서버의 로컬 체인을 갱신하는 것을 포함하는, 상태 재분할 방법.

청구항 9

청구항 8에 있어서,

상기 재분할 결과를 수행하는 단계 후에, 상기 목적지 지역의 지역 서버가 상기 메인 체인 상에 락킹된 상기 트랜잭션의 상태의 락킹을 해제하는 단계를 더 포함하는, 상태 재분할 방법.

청구항 10

청구항 2에 있어서,

상기 트랜잭션의 데이터 구조는 특정 메인 체인 블록상에서 재분할 제안의 순서를 나타내는 인덱스, 상태의 문자열 키의 이름, 위상 정보, 출발지 지역 이름, 목적지 지역 이름, 재분할 제안으로 선정된 트랜잭션의 식별 아이디, 및 상태 값에 대한 필드들이나 정보를 포함하는, 상태 재분할 방법.

청구항 11

청구항 1에 있어서,

상기 특정 트랜잭션은 모든 접근 상태가 지역(Local) 위상인 트랜잭션이 메인 체인 검증에 실패하는 경우의 트랜잭션인 간섭 로컬 트랜잭션, 접근 상태가 전역(Global) 위상이면서 메인 체인 검증에 성공하는 경우의 트랜잭션인 성공 전역 트랜잭션, 및 핸드오버 트랜잭션 중 어느 하나를 포함하는, 상태 재분할 방법.

청구항 12

청구항 1에 있어서,

상기 메인 체인 블록은 복수 지역의 복수의 로컬 체인들에서 생성되는 로컬 체인 블록들을 로컬 체인 인덱스 기반의 순서로 통합하여 생성되는, 상태 재분할 방법.

청구항 13

청구항 1에 있어서

상기 특정 트랜잭션이 핸드오버 트랜잭션인 경우, 위치 기반 지역성을 사용하여 동적 지역성 변화를 감지하는 단계를 더 포함하는, 상태 재분할 방법.

청구항 14

청구항 13에 있어서,

상기 동적 지역성 변화를 감지한 경우, 상기 핸드오버 트랜잭션은 해당 사용자와 관계되는 상태를 정의하는 키, 출발지 지역 및 목적지 지역으로 구성된 구조를 구비하는, 상태 재분할 방법.

청구항 15

블록체인 플랫폼 기반으로 동적 지역성을 지원하는 상태 재분할 방법을 수행하는 프로세서를 포함한 지역 서버

의 상태 재분할 장치로서,

상태 재분할 프로토콜이 저장되는 메모리; 및

상기 메모리에 연결되어 상기 상태 재분할 프로토콜을 수행하는 프로세서를 포함하고,

상기 프로세서가, 지역 내 통신 노드로부터 트랜잭션을 수신하고, 수신된 트랜잭션을 포함한 로컬 체인상의 로컬 체인 블록을 메인 체인상의 메인 체인 블록으로 통합하고, 상기 메인 체인 블록상의 트랜잭션이 미리 설정된 유형의 특정 트랜잭션인지를 확인하고, 상기 수신된 트랜잭션이 상기 특정 트랜잭션이면, 상기 수신된 트랜잭션을 상태 재분할 대상 집합에 추가하는, 상태 재분할 장치.

청구항 16

청구항 15에 있어서,

상기 프로세서가, 상기 수신된 트랜잭션을 상태 재분할 대상 집합에 추가할 때, 상기 특정 트랜잭션인지를 확인하는 과정을 통해 선정된 재분할 대상 트랜잭션에 대한 재분할 제안(reshard proposal, RP)을 생성하고, 상기 재분할 제안을 상기 메인 체인에 커밋하는, 상태 재분할 장치.

청구항 17

청구항 16에 있어서,

상기 프로세서가, 상기 메인 체인에 커밋하는 과정에서 상기 재분할 제안을 생성한 메인 체인 블록에 대한 합의 증명 데이터를 확보하고, 여기서 상기 합의 증명 데이터는 정족수(quorum)만큼의 합의 메시지를 포함하는, 상태 재분할 장치.

청구항 18

청구항 16에 있어서,

상기 재분할 제안이 상기 메인 체인상에 커밋되면, 상기 프로세서가, 상기 메인 체인 상의 상기 트랜잭션의 상태인 키의 가장 최신 값을 락킹하는, 상태 재분할 장치.

청구항 19

청구항 18에 있어서,

상기 프로세서가, 상기 메인 체인의 커밋 확정에 의해 상기 합의 증명 데이터가 지역 서버에서 확인된 후, 상기 재분할 제안을 수행하는 것을 더 포함하며,

여기서 상기 재분할 제안의 수행은 상기 재분할 제안에 기록된 출발지 지역의 지역 서버에서 상기 트랜잭션의 상태의 위상을 지역(Local)에서 전역(Global)으로 변경하는 것을 포함하고, 상기 위상의 변경에 따라 상기 출발지 지역의 지역 서버는 상기 상태에 대한 상태 소유권을 잃게 되는, 상태 재분할 장치.

청구항 20

청구항 19에 있어서,

상기 프로세서가, 상기 재분할 제안을 수행한 후에 재분할 결과(reshard result, RR)를 생성하는 것을 더 포함하며, 여기서 상기 재분할 결과의 생성은 목적지 지역의 지역 서버에서 상기 재분할 결과를 트랜잭션 형태로 인코딩하고 상기 트랜잭션의 상태의 위상을 전역(Global)으로 기록하여 상기 메인 체인에 전달하는 것을 포함하는, 상태 재분할 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 모바일 에지 컴퓨팅(mobile edge computing, MEC)을 통한 고성능 블록체인 샤딩 프로토콜에 관한 것으로, 보다 상세하게는, 상태 정보를 기준으로 분할하는 샤딩 블록체인 플랫폼에서 동적 지역성 워크로드를 활용하기 위해 필요한 샤드 재구성을 효과적으로 수행할 수 있는 상태 재분할 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 블록체인 기반 서비스를 실생활에서 이용하기 위해서는, 블록체인 트랜잭션 처리 속도가 중요하며, 블록체인 기술 확산의 큰 걸림돌은 낮은 확장성이다. 예를 들어, 비트코인은 한 트랜잭션이 확정될 때까지 평균 10분이 소요된다고 알려져 있으며, 이더리움은 평균 22초 정도 소요된다.

[0003] 블록체인 성능 확장성을 해결하기 위하여 샤딩(sharding), 합의 알고리즘 개선, 암호 기법 개선, 오프체인 트랜잭션 처리 등 다양한 기법들이 개발되고 있다.

[0004] 그 중, 샤딩 기법은 블록체인 플랫폼 성능 확장을 위해 가장 널리 활용되며, 블록체인 트릴레마 즉, 탈중앙화, 보안, 성능 확장 문제를 함께 고려해야 하는 상황에서 필수적인 기술이다.

[0005] 샤딩은 블록체인 네트워크상 처리 과정을 샤드(shards)로 불리는 다수의 그룹으로 분할하고 처리하는 기법이다. 이 때, 분할 대상은 트랜잭션별 분할, 네트워크 노드별 분할, 그리고 상태 정보별 분할 등으로 구분할 수 있다. 따라서, 각 샤드별 병렬처리를 통해, 결과적으로 성능은 샤드 개수에 비례하여 선형적으로 증가하는 이점이 있다. 그러나, 샤드별로 트랜잭션을 독립적으로 처리할 수 없는 경우, 즉 크로스 샤드 트랜잭션을 처리하기 위해서는 복수의 샤드들에서 상호 동기적 처리가 수반됨에 따라 오버헤드가 증가하는 문제점을 가진다.

[0006] 상태 정보별 분할을 고려하는 블록체인 플랫폼에서, 에지 컴퓨팅 그리고 모바일 사용자 등을 고려할 때 위치 기반 지역성을 활용하는 것은 필수적이다. 즉, 트랜잭션별 분할이나 네트워크 노드별 분할 경우와 비교할 때, 상태 정보별 분할의 유지 및 관리 과정이 더 복잡하므로, 샤딩 기법을 활용하는 블록체인 플랫폼들에서는 대부분 트랜잭션별 분할이나 네트워크 노드별 분할을 적용하고 있다.

[0007] 한편, 상태 데이터를 분할하는 방법은 보통 일관된 해쉬(consistent hash), 해쉬 슬롯(hash slot) 등 상태 데이터를 랜덤하게 분할(randomized placement) 하는 방법이 널리 사용된다. 이러한 방법은 폐쇄형 데이터 센터의 클러스터 구성에는 적합하지만, 에지 컴퓨팅 등 지리적 분산 시스템에서 위치 기반 지역성 특성을 띠고 있는 워크로드에는 적합하지 않다. 왜냐하면, 지역성을 고려하지 않고 분할하는 경우, 원격 데이터 접근 및 그에 따른 크로스 샤드 트랜잭션 수가 많아지게 되며, 이는 성능 병목의 주요 걸림돌이기 때문이다. 따라서, 워크로드 지역성을 고려하는 상태 데이터 분할은 고성능 샤딩 시스템 구축에 필수적이다.

[0008] 지역성은 시간의 흐름에 따라 변화하는 특성을 지니고 있고, 이를 동적 지역성(Dynamic Locality)라 부른다. 이는 상태 데이터 분할이 초기에 아무리 완벽하게 이뤄졌다고 해도, 시간의 흐름에 따라, 워크로드의 지역성은 변할 수 있음을 의미한다. 예를 들어, 셀룰러 네트워크상 핸드오버, 실시간 인기 투표 등이 그 사례이다. 동적 지역성의 이해를 돕기 위해, 위 사례들의 보다 상세한 시나리오를 설명하면 다음과 같다.

[0009] 먼저, 셀룰러 네트워크상 핸드오버는 사용자가 출발지 기지국에서 도착지 기지국으로 이동하는 경우에 발생한다. 흔히 사용되는 모바일 엣지 컴퓨팅(Mobile Edge Computing, MEC)과 같은 경우, 기지국 간 샤딩된 분산 시스템을 구성하는 상황을 고려할 수 있다.

[0010] 사용자는 이동 전에는 출발지 기지국에 설치된 엣지 컴퓨터에 배치된 데이터에 빈번하게 접근하는 경향을 보인다. 이동 후에는, 목적지 기지국에 설치된 엣지 컴퓨터를 통해 데이터를 접근한다. 만약, 핸드오버하는 사용자의 상태에 대한 상태 재분할이 이뤄지지 않은 경우, 목적지 엣지 컴퓨터는 출발지 엣지 컴퓨터에 원격 데이터 접근을 하므로, 지연이 높아지는 성능 문제를 겪는다.

[0011] 또한, 이동 후의 사용자는 도착지 지역상 다른 사용자들과의 거래를 빈번하게 하게 되며, 이는 출발지 데이터와 목적지 데이터를 모두 접근하는 크로스 샤드 트랜잭션을 많이 발생시킨다. 크로스 샤드 트랜잭션은 원자성 커밋과 같은 복잡한 프로토콜이 수반되며 그 수가 많을 경우, 시스템 성능을 급격히 떨어뜨린다.

[0012] 다음으로, 위의 핸드오버의 경우와 유사하게, 실시간 인기 투표의 경우, 관객과 그 관객의 특정 후보자에 대한 선호도에 따라 상태 데이터를 효율적으로 분할 배치할 수 있으나, 후보자 인기가 변하는 경우, 관객 데이터도 그에 맞춰서 분할하지 않으면 위에서 언급한 원격 데이터 접근 및 크로스 샤드 트랜잭션의 수가 많아지는 문제가 발생한다.

[0013] 이와 같이 블록체인 성능 확장성은 보안 및 탈중앙화를 동시에 고려해야 하는 트릴레마(trilemma) 문제로 인식되며, 최근들어 샤딩(sharding) 기법을 통해 병렬처리를 가능하게 함으로써 블록체인 플랫폼의 성능 확장성을 높이고자 하는 결과들이 많이 공개되고 있다.

[0014] 하지만, 샤딩 기법을 적용하기 위해서는 먼저 어떤 기준으로 분할할 것인지, 즉 샤드 형태를 결정해야 하고, 복

수개 샤드 정보를 접근하는 크로스 샤드(cross-shard) 트랜잭션을 처리해야 한다. 샤드 형태는 세 가지 종류 즉, 사용자 트랜잭션, 블록체인 노드, 및 상태 정보를 기준으로 분할한다. 사용자 트랙잭션과 블록체인 노드를 기준으로 분할되는 샤드 형태는 샤드 재구성 등이 용이하지만, 로컬 샤드 내에서의 독립적인 트랜잭션 처리가 어려운 문제점을 가진다. 그리고 상태 정보를 기준으로 분할되는 샤드 형태는 로컬 샤드에서의 독립적 트랜잭션 처리가 가능하지만, 상대적으로 샤드 재구성이 대단히 어려운 문제점을 가진다.

발명의 내용

해결하려는 과제

[0015] 본 발명은 전술한 종래 기술의 문제를 해결하기 위해 도출된 것으로, 본 발명의 목적은 상태 정보를 기준으로 분할하는 샤딩 블록체인 플랫폼에서 동적 지역성 워크로드를 활용하기 위해 필요한 샤드 재구성을 효과적으로 수행할 수 있는 상태 재분할 방법 및 장치를 제공하는데 있다.

[0016] 본 발명의 다른 목적은, 샤딩 블록체인 플랫폼상 동적 지역성 워크로드를 효과적으로 처리할 수 있고, 원격 데이터 접근 및 크로스 샤드 트랜잭션 발생 빈도를 줄일 수 있으며, 고성능의 블록체인 샤딩 시스템을 지원할 수 있는, 상태 재분할 방법 및 장치를 제공하는데 있다.

과제의 해결 수단

[0017] 상기 기술적 과제를 해결하기 위한 본 발명의 일 측면에 따른, 샤딩 블록체인 플랫폼에서 지역 서버에 의해 수행되는 동적 지역성 지원을 위한 상태 재분할 프로토콜은, 샤딩 블록체인 플랫폼에서 지역성 변화를 감지 시, 즉각적으로 샤드별 분할되어 있는 상태를 변화된 지역성에 부합되도록 재배치하여, 향후 발생할 크로스 샤드 트랜잭션을 줄이도록 구성된다. 상태 재분할 프로토콜을 구현하기 위한 방법으로, 우선 각 샤드에서 생성하는 블록들을 통합하는 메인 체인을 정의한다. 메인 체인은 상태 정보에 대한 전역 일관성을 지원함으로써 크로스 샤드 트랜잭션에 대하여 샤드 간 동일한 판단을 내릴 수 있도록 지원한다. 메인체인에서 생성하는 블록은 각 로컬 체인에서 개별적으로 생성하는 로컬 체인 블록을 일정 규칙을 기준으로 접합하는데, 예를 들어 로컬 체인의 식별자 순서대로 접합하는 규칙을 포함할 수 있다. 본 발명에서는 메인 체인상의 상태 재분할 제안 트랜잭션과 상태 재분할 결과 트랜잭션의 두 가지 시스템 트랜잭션들을 처리하도록 구성함으로써, 상태 재분할 과정에 필요한 데이터 신뢰성 문제를 해결한다.

[0018] 여기서, 각 로컬 체인은 상태 소유권(State Ownership)을 구비하며, 그에 따라 각 샤드 즉, 로컬 체인은 소유권이 있는 상태만 개별적으로 갱신할 수 있는 권한을 가진다. 또한, 각 로컬 체인에서 각 상태 데이터의 위상을 '지역(local)'과 '전역(global)'으로 정의하며, 샤드 즉, 로컬 체인에 부여된 고유 번호는 상태 데이터 위상의 소속 지역 정보로 사용될 수 있다.

[0019] 일 실시예에서, 본 발명은 메인 체인과 상태 소유권 개념 및 위상 정보를 활용하여 상태 재배치를 위한 프로토콜을 샤드(즉, 로컬 체인)의 해제(release)/할당(own)으로 이루어진 2단계 절차로 구성할 수 있다.

[0020] 일 실시예에서, 샤드의 해제 단계에서는, 대상 상태의 소유권을 샤드로부터 박탈하고 그 위상을 '전역'으로 변경함으로써, 대상 상태가 더 이상 원래 샤드에서 갱신될 수 없도록 동작한다. 대상 상태는 오직 메인 체인에서만 처리가 가능하다.

[0021] 여기서, 소유권이 박탈되는, 즉 샤드 재배치 대상이 되는 상태 정보 선정 절차는 메인 체인상 생성된 블록들을 순회하면서 트랜잭션들이 접근한 상태 데이터의 배치 상황 분석을 통해 지역성이 변경된 상태 정보를 대상으로 결정된다. 특히, 샤드의 해제 단계에서는, 핸드오버 트랜잭션, 크로스 샤드 트랜잭션, 및 검증이 실패한 로컬 트랜잭션은 지역성 변화에 큰 영향을 주는 트랜잭션들이며, 이들에 대한 분석이 집중적으로 진행될 수 있다.

[0022] 일 실시예에서, 샤드 재배치 대상으로 선정된 상태 데이터를 기준으로 재분할 제안(reshard proposal, RP) 트랜잭션을 생성할 수 있다. 재분할 제안(RP)에는 상태 데이터가 궁극적으로 재배치될 샤드 정보가 포함될 수 있다. 편의를 위해, 샤드 재배치 대상 상태 데이터가 속했던 원샤드를 '출발지', 그리고 재배치될 샤드를 '목적지'로 명명할 수 있다.

[0023] 일 실시예에서, 재분할 제안(RP) 트랙잭션 생성 후, RP 트랜잭션이 메인 체인에서 확정 커밋된 후, 출발지 샤드 내 노드들은 해당 상태 데이터의 소유권을 해제함으로써, 이후 출발지 샤드 안에서 해당 상태 데이터들이 로컬로 접근하려는 시도를 차단할 수 있다.

[0024] 일 실시예에서, 샤드의 할당 단계에서는, 소유권이 '전역(global)'로 되어 있는 상태 데이터 정보를 특정 샤드에 할당하여 소유권을 '지역(local)'으로 변경할 수 있다. 샤드의 할당 단계는 소유권 변경뿐만 아니라, 해당 상태 데이터를 샤드 내부에 새롭게 생성하여 기록할 필요가 있다. 샤드 내부에 새로운 상태 데이터 정보를 생성하고 기록하는 과정은 블록체인 상태 데이터의 일관성을 유지해야 하므로 반드시 신뢰성 검증을 수행해야 한다. 이를 위해, 상기의 RP 트랜잭션 생성 이후, 샤드 해제가 완료된 시점에서 재분할 결과(reshard result, RR) 트랜잭션을 생성할 수 있다.

[0025] 일 실시예에서, 샤드의 할당 단계 이후에, 메인 체인상에 RR 트랜잭션이 커밋되면, 상태 데이터의 소유권을 변경하고, 메인체인상 커밋된 상태 데이터 정보는 블록체인 일관성을 만족하므로, 이로써 신뢰성 검증을 거친 것으로 간주하고, 메인체인상 커밋된 상태 데이터 정보와 동일한 키, 값 쌍을 샤드-내부 데이터 베이스에 새롭게 생성하여 기록할 수 있다.

[0026] 일 실시예에서, 위치 기반 지역성을 반영하여 샤딩을 적용하는 경우에, 동적 지역성은 모바일 사용자들의 지역 간 이동시 관찰되며, 이러한 경우는 사용자가 새로운 지역에서 핸드오버 트랜잭션을 제출함으로써 상태 재분할 프로토콜이 시작될 수 있다.

[0027] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 측면에 따른 상태 재분할 방법은, 블록체인 플랫폼 기반으로 동적 지역성을 지원하는 지역 서버의 상태 재분할 방법으로서, 지역 내 통신 노드로부터 트랜잭션을 수신하는 단계; 수신된 트랜잭션을 포함한 로컬 체인상의 로컬 체인 블록을 메인 체인상의 메인 체인 블록으로 통합하는 단계; 상기 메인 체인 블록상의 트랜잭션이 미리 설정된 유형의 특정 트랜잭션인지를 확인하는 단계; 및 상기 수신된 트랜잭션이 상기 특정 트랜잭션이면, 상기 수신된 트랜잭션을 상태 재분할 대상 집합에 추가하는 단계를 포함한다.

[0028] 상기 추가하는 단계는, 상기 확인하는 단계에서 선정된 재분할 대상 트랜잭션에 대한 재분할 제안(reshard proposal, RP)을 생성하는 단계, 및 상기 재분할 제안을 상기 메인 체인에 커밋하는 단계를 포함할 수 있다.

[0029] 상기 메인 체인에 커밋하는 단계는 상기 재분할 제안을 생성한 메인 체인 블록에 대한 합의 증명 데이터를 확보하는 것을 포함할 수 있다. 여기서 상기 합의 증명 데이터는 정족수(quorum)만큼의 합의 메시지를 포함할 수 있다.

[0030] 상기 상태 재분할 방법은, 상기 메인 체인상에 상기 재분할 제안이 상기 메인 체인에 커밋되면, 상기 메인 체인상의 상기 트랜잭션의 상태인 키의 가장 최신 값을 락킹하는 단계를 더 포함할 수 있다.

[0031] 상기 상태 재분할 방법은, 상기 메인 체인의 커밋 확정에 의해 상기 합의 증명 데이터가 지역 서버에서 확인된 후, 상기 재분할 제안을 수행하는 단계를 더 포함할 수 있다. 상기 재분할 제안의 수행은 상기 재분할 제안에 기록된 출발지 지역의 지역 서버에서 상기 트랜잭션의 상태의 위상을 지역(Local)에서 전역(Global)으로 변경하는 것을 포함할 수 있다. 그리고, 상기 위상의 변경에 따라 상기 출발지 지역의 지역 서버는 상기 상태에 대한 상태 소유권을 잃게 될 수 있다.

[0032] 상기 상태 재분할 방법은, 상기 재분할 제안을 수행한 후에, 재분할 결과를 생성하는 단계를 더 포함할 수 있다. 여기서 상기 재분할 결과(reshard result, RR)는 목적지 지역의 지역 서버에서 트랜잭션 형태로 인코딩되고 상기 트랜잭션의 상태의 위상이 전역(Global)으로 기록되어 상기 메인 체인에 전달되는 것을 포함할 수 있다.

[0033] 상기 상태 재분할 방법은, 상기 재분할 결과를 생성한 후에, 재분할 결과가 반영된 메인 체인 블록을 수신하고, 수신한 메인 체인 블록 상의 재분할 결과를 확인하는 단계를 확인하는 단계, 및 확인된 재분할 결과를 트랜잭션 형태로 인코딩하고 메인 체인 블록의 합의 증명 데이터에 삽입하는 단계를 더 포함할 수 있다.

[0034] 상기 상태 재분할 방법은, 상기 확인된 재분할 결과에 대한 메인 체인 커밋이 확정되면, 재분할 결과를 수행하는 단계를 더 포함할 수 있다. 여기서 상기 재분할 결과의 수행은 목적지 지역의 지역 서버가 해당 트랜잭션에 포함된 상태의 위상을 전역(Global)에서 지역(Local)로 수정하고, 상기 상태의 값을 상기 목적지 지역의 지역 서버의 로컬 체인을 갱신하는 것을 포함할 수 있다.

[0035] 상기 상태 재분할 방법은, 상기 재분할 결과를 수행하는 단계 후에, 상기 목적지 지역의 지역 서버가 상기 메인 체인 상에 락킹된 상기 트랜잭션의 상태의 락킹을 해제하는 단계를 더 포함할 수 있다.

[0036] 상기 트랜잭션의 데이터 구조는 특정 메인 체인 블록상에서 재분할 제안의 순서를 나타내는 인덱스, 상태의 문자열 키의 이름, 위상 정보, 출발지 지역 이름, 목적지 지역 이름, 재분할 제안으로 선정된 트랜잭션의 식별 아

이디, 및 상태 값에 대한 필드들이나 정보를 포함할 수 있다.

[0037] 상기 특정 트랜잭션은 모든 접근 상태가 지역(Local) 위상인 트랜잭션이 메인 체인 검증에 실패하는 경우의 트랜잭션인 간섭 로컬 트랜잭션, 접근 상태가 전역(Global) 위상이면서 메인 체인 검증에 성공하는 경우의 트랜잭션인 성공 전역 트랜잭션, 및 핸드오버 트랜잭션 중 어느 하나를 포함할 수 있다.

[0038] 상기 메인 체인 블록은 복수 지역의 복수의 로컬 체인들에서 생성되는 로컬 체인 블록들을 로컬 체인 인덱스 기반의 순서로 통합하여 생성될 수 있다.

[0039] 상기 상태 재분할 방법은, 상기 특정 트랜잭션이 핸드오버 트랜잭션인 경우, 위치 기반 지역성을 사용하여 동적 지역성 변화를 감지하는 단계를 더 포함할 수 있다.

[0040] 상기 동적 지역성 변화를 감지한 경우, 상기 핸드오버 트랜잭션은 해당 사용자와 관계되는 상태를 정의하는 키, 출발지 지역 및 목적지 지역으로 구성된 구조를 구비할 수 있다.

[0041] 상기 기술적 과제를 해결하기 위한 본 발명의 다른 측면에 따른 상태 재분할 장치는, 블록체인 플랫폼 기반으로 동적 지역성을 지원하는 상태 재분할 방법을 수행하는 프로세서를 포함한 지역 서버의 상태 재분할 장치로서, 상태 재분할 프로토콜이 저장되는 메모리; 및 상기 메모리에 연결되어 상기 상태 재분할 프로토콜을 수행하는 프로세서를 포함하고, 상기 프로세서가, 지역 내 통신 노드로부터 트랜잭션을 수신하고, 수신된 트랜잭션을 포함한 로컬 체인상의 로컬 체인 블록을 메인 체인상의 메인 체인 블록으로 통합하고, 상기 메인 체인 블록상의 트랜잭션이 미리 설정된 유형의 특정 트랜잭션인지를 확인하고, 상기 수신된 트랜잭션이 상기 특정 트랜잭션이면, 상기 수신된 트랜잭션을 상태 재분할 대상 집합에 추가한다.

[0042] 상기 프로세서는, 상기 수신된 트랜잭션을 상태 재분할 대상 집합에 추가할 때, 상기 특정 트랜잭션인지를 확인하는 과정을 통해 선정된 재분할 대상 트랜잭션에 대한 재분할 제안(reshard proposal, RP)을 생성하고, 상기 재분할 제안을 상기 메인 체인에 커밋할 수 있다.

[0043] 상기 프로세서는, 상기 메인 체인에 커밋하는 과정에서 상기 재분할 제안을 생성한 메인 체인 블록에 대한 합의 증명 데이터를 확보할 수 있다. 여기서 상기 합의 증명 데이터는 정족수(quorum)만큼의 합의 메시지를 포함할 수 있다.

[0044] 상기 재분할 제안이 상기 메인 체인상에 커밋되면, 상기 프로세서는, 상기 메인 체인 상의 상기 트랜잭션의 상태인 키의 가장 최신 값을 락킹할 수 있다.

[0045] 상기 프로세서는, 상기 메인 체인의 커밋 확정에 의해 상기 합의 증명 데이터가 지역 서버에서 확인된 후, 상기 재분할 제안을 수행하는 것을 더 포함할 수 있다. 여기서 상기 재분할 제안의 수행은 상기 재분할 제안에 기록된 출발지 지역의 지역 서버에서 상기 트랜잭션의 상태의 위상을 지역(Local)에서 전역(Global)으로 변경하는 것을 포함할 수 있다. 상기 위상의 변경에 따라 상기 출발지 지역의 지역 서버는 상기 상태에 대한 상태 소유권을 잃게 될 수 있다.

[0046] 상기 프로세서는, 상기 재분할 제안을 수행한 후에 재분할 결과(reshard result, RR)를 생성하는 것을 더 포함할 수 있다. 여기서 상기 재분할 결과의 생성은 목적지 지역의 지역 서버에서 상기 재분할 결과를 트랜잭션 형태로 인코딩하고 상기 트랜잭션의 상태의 위상을 전역(Global)으로 기록하여 상기 메인 체인에 전달하는 것을 포함할 수 있다.

발명의 효과

[0047] 본 발명의 상태 재분할 방법 또는 상태 재분할 장치를 사용하면, 샤딩 블록체인 플랫폼에서 지역성이 동적으로 변하는 워크로드를 효과적으로 처리할 수 있다. 특히, 기존 샤딩 블록체인들이 트랜잭션별 샤딩이나 네트워크 노드별 샤딩을 적용하여 상태 데이터의 지역성 변경에 제대로 대응하지 못하는 문제를 해결할 수 있다. 즉, 상태 재분할 방법은 지역성이 변하는 시점에 상태 데이터를 적응적으로 재배치함으로써 원격 데이터 접근 및 크로스-샤드 트랜잭션의 빈도를 크게 줄일 수 있고, 그에 의해 고성능 샤딩 블록체인 시스템을 유지할 수 있는 장점을 가진다.

[0048] 또한, 본 발명에 의하면, 샤딩 블록체인 플랫폼에서 지역성 변화를 감지할 때, 샤드별로 분할되어 있는 상태를 변화된 지역성에 부합되도록 즉각적인 상태 재분할을 통해 재배치하여, 향후 발생할 크로스 샤드 트랜잭션의 발생을 사전에 방지하고 실제로 발생하는 크로스 샤드 트랜잭션을 크게 줄일 수 있다.

[0049] 또한, 본 발명에 의하면, 메인 체인 상에 커밋되는 상태 재분할 제안 트랜잭션과 상태 재분할 결과 트랜잭션의

두 가지 시스템 트랜잭션들을 처리하는 방식으로 상태 재분할을 수행하도록 구성함으로써, 상태 재분할 과정에 필요한 데이터 신뢰성 문제를 효과적으로 해결할 수 있다.

도면의 간단한 설명

[0050] 본 발명에 관한 이해를 돕기 위해 상세한 설명의 일부로 포함되는, 첨부 도면들은 본 발명에 대한 실시예를 제공하고, 상세한 설명과 함께 본 발명의 기술적 사상을 예시한다.

도 1은 본 발명의 일실시예에 따른 샤딩 블록체인 플랫폼 구조를 나타낸 것으로, 다수의 샤딩된 로컬 체인들과 동적 재분할을 위한 전역 일관성을 지원하는 메인 체인으로 이루어진 계층적 블록체인 구조를 나타낸 블록도이다.

도 2는 도 1의 샤딩 블록체인 플랫폼 구조에 채용할 수 있는 메인 체인 블록의 생성 절차를 설명하기 위한 예시도이다.

도 3은 본 발명의 일실시예에 따른 샤딩 블록체인 플랫폼 상에서 상태 재분할을 수행하는 상태 재분할 방법의 주요 절차에 대한 흐름도이다.

도 4는 도 3의 상태 재분할 방법에서 재분할 대상 트랜잭션을 선정하는 절차를 나타낸 흐름도이다.

도 5은 도 3의 상태 재분할 방법에서 재분할 제안 및 재분할 결과에 활용되는 재분할 데이터 구조를 나타낸 블록도이다.

도 6는 도 3의 상태 재분할 방법에서 상태의 위상 변경에 대한 다이어그램이다.

도 7은 도 3의 상태 재분할 방법에 채용할 수 있는 상태 재분할 제안에서의 핸드오버 트랜잭션 구조를 설명하기 위한 예시도이다.

도 8은 도 3의 상태 재분할 방법을 핸드오버 트랜잭션의 처리 과정 관점에서 설명하기 위한 흐름도이다.

도 9는 본 발명의 다른 실시예에 따른 샤딩 블록체인 플랫폼 상에서 상태 재분할을 수행하는 상태 재분할 장치의 주요 구성을 설명하기 위한 블록도이다.

도 10은 도 9의 상태 재분할 장치의 적용예를 설명하기 위한 개념도이다.

발명을 실시하기 위한 구체적인 내용

[0051] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다.

[0052] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. '및/또는'이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0053] 본 출원의 실시예들에서, 'A 및 B 중에서 적어도 하나'는 'A 또는 B 중에서 적어도 하나' 또는 'A 및 B 중 하나 이상의 조합들 중에서 적어도 하나'를 의미할 수 있다. 또한, 본 출원의 실시예들에서, 'A 및 B 중에서 하나 이상'은 'A 또는 B 중에서 하나 이상' 또는 'A 및 B 중 하나 이상의 조합들 중에서 하나 이상'을 의미할 수 있다.

[0054] 어떤 구성요소가 다른 구성요소에 '연결되어' 있다거나 '접속되어' 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 '직접 연결되어' 있다거나 '직접 접속되어'있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0055] 본 출원에서 사용한 용어는 단지 특정한 실시예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서, '포함한다' 또는 '가진다' 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부

품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0056] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가진 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0057] 이하, 첨부한 도면들을 참조하여, 본 발명의 바람직한 실시예를 보다 상세하게 설명하고자 한다. 본 발명을 설명함에 있어 전체적인 이해를 용이하게 하기 위하여 도면상의 동일한 구성요소에 대해서는 동일한 참조부호를 사용하고 동일한 구성요소에 대해서 중복된 설명은 생략한다.

[0058] 도 1은 본 발명의 일실시예에 따른 샤딩 블록체인 플랫폼 구조를 나타낸 것으로, 다수의 샤딩된 로컬 체인들과 동적 재분할을 위한 전역 일관성을 지원하는 메인 체인으로 이루어진 계층적 블록체인 구조를 나타낸 블록도이다.

[0059] 도 1을 참조하면, 샤딩 블록체인 플랫폼 구조는 복수의 샤딩된 로컬 체인들(110, 111, 112, 113, 114)과 개별 로컬 체인에서 생성하는 로컬 블록들을 일정 규칙대로 합하여 메인 블록(101)을 생성하고 처리하는 메인 체인(100)으로 구성된다. 메인 체인(100)은 로컬 블록들로 구성되어 로컬 체인들에 전역 일관성을 지원함으로써 동적 재분할을 지원한다.

[0060] 로컬 체인들(110, 111, 112, 113, 114)과 메인 체인(100)은 블록 내 트랜잭션들을 바탕으로 상태 데이터를 저장하는 키-값(key-value, K-V) 저장소를 각각 로컬 체인 상태 DB(115, 116, 117, 118, 119)와 메인 체인 상태 DB(102) 형태로 구비할 수 있다.

[0061] 메인 체인(100)의 생성 방식에 있어서, 메인 블록(101)은 로컬 체인상 합의된 블록들을 각 로컬 체인에 부여된 식별 번호를 기반으로 사전 정렬된 순서로 정렬된 형태로 구성할 수 있고, 이에 의해 로컬 체인들(110, 111, 112, 113, 114)에 대한 전역 일관성 및 상태 재분할 데이터의 신뢰성을 확보한다.

[0062] 샤딩 블록체인 플랫폼의 상태 재분할 프로토콜에서 사용하는 전용 트랜잭션들은 오직 메인 체인(100)에서 확정된 후에 사용함으로써, 로컬 체인들(110, 111, 112, 113, 114) 간 데이터 이동 시 발생하는 신뢰성 문제를 효과적으로 해결한다.

[0063] 또한, 도 1에서는 특정 로컬 체인(112)에서 다른 로컬 체인(113)으로 사용자 단말(120)이 이동하는 시나리오를 나타내고 있다. 이 경우, 상태 재분할 프로토콜은 메인 체인(100) 및 후술할 메인 체인을 기반으로 하는 재분할 전용 트랜잭션들을 활용하여 사용자의 상태를 출발지 로컬 체인(112)에서 목적지 로컬 체인(113)으로 신뢰성 있게 이동시킬 수 있다.

[0064] 이하, 샤딩 블록체인 플랫폼 구조는 본 실시예의 상태 재분할 방법을 이용하여 블록체인 기반의 상태 재분할을 수행하는 수단이거나 상태 재분할 방법을 사용하는 상태 재분할 장치를 적어도 일부의 구성부로 포함하는 장치에 대응할 수 있다.

[0065] 도 2는 도 1의 샤딩 블록체인 플랫폼 구조에 채용할 수 있는 메인 체인 블록의 생성 절차를 설명하기 위한 예시도이다. 본 실시예에서는 메인 체인 블록(MC-Block) 생성시, 로컬 체인 블록을 로컬 체인 식별자 정보를 기준으로 통합하는 규칙을 적용하는 경우를 예시한다.

[0066] 도 2를 참조하면, 메인 체인 블록은 기설정된 최대 메인 체인 블록(MC-Block) 생성 주기 내에 하나의 메인 체인 블록을 생성하도록 구성될 수 있다.

[0067] 최대 메인 체인 블록 생성 주기(P)는 다음의 수학식 1과 같이 표현될 수 있다.

수학식 1

[0068] $$P = \min(\Delta_{MC\text{-}Bucket} \times \Delta_{MC\text{-}Timeout})$$

[0069] 수학식 1에서 $\Delta_{MC\text{-}bucket}$은 MC 블록 크기를 의미한다.

[0070] 상태 재분할 장치는, 제1 로컬 체인(local chain 0), 제2 로컬 체인(local chain 1) 및 제3 로컬 체인(local chain 2)에서 각각 2개씩의 블록을 받고 미리 설정된 순서에 따라 정렬하여 메인 체인 블록(MC_Block_{i-1})(200)을 생성할 수 있다. 미리 설정된 순서는 로컬 체인들에 부여된 인덱스를 포함할 수 있다.

[0071] 한편, 상태 재분할 장치는 특정 로컬 체인 예컨대 제3 로컬 체인(local chain 2)의 블록 처리가 늦어질 경우, 메인 체인 블록의 해당 블록에 빈 블록(empty block, 230)을 채워 또 다른 메인 체인 블록(MC_Block_i)(210)을 생성할 수 있다.

[0072] 보다 구체적으로 설명하면, 제1 메인 체인 블록(200)은 3개의 로컬 체인들에서 각각 생성된 블록들(0, 1)로 구성되며, 이들은 전술한 로컬 체인상 합의된 블록들이 로컬 체인에 부여된 식별 번호를 기반으로 사전 정렬된 순서로 정렬된다.

[0073] 메인 체인 블록의 크기는 버킷으로 정의된다. 버킷은 한 메인 체인 블록에 포함되는 각 로컬 체인 블록의 최대 블록 개수를 의미한다. 예를 들어, 버킷 크기가 2이고, 3개의 로컬 체인들이 있는 경우, 도 2의 메인 체인 블록(200)의 구성과 같이 각 로컬 체인의 블록 개수가 2개, 총 6개의 로컬 블록들이 하나의 메인 체인 블록을 구성하게 된다.

[0074] 이와 같이, 고정 크기의 메인 체인 블록 생성을 지원하는 경우, 특정 로컬 체인의 블록이 생성되지 않는 경우가 발생할 수 있다. 그 경우, 해당 로컬 체인은 빈 블록(230)을 생성하여 전파함으로써, 버킷 크기를 맞출 수 있다.

[0075] 여기서, 버킷 크기의 메인 체인 블록을 생성하는 주기는 제3 메인 체인 블록(MC_Block_{i+1})(230)과 같이 버킷이 모두 온전한 블록들(240)로 제때에 채워지는 시간으로 정의되거나, 또는 제2 메인 체인 블록(220)과 같이 빈 블록(230)을 포함하도록 강제하는 타이머 만료 시간 중 낮은 시간으로 정의될 수 있다.

[0076] 도 3은 본 발명의 일실시예에 따른 샤딩 블록체인 플랫폼 상에서 상태 재분할을 수행하는 상태 재분할 방법의 주요 절차에 대한 흐름도이다.

[0077] 도 3을 참조하면, 상태 재분할 프로토콜에 의해 동작하는 지역 서버가 메인 체인 블록을 수신하면 본 프로세스가 시작될 수 있다(S300). 메인 체인 블록은 지역 샤드 즉 로컬 체인이 생성한 블록들의 집합으로 구성되고, 지역들 간 전역 일관성 확보를 위해 활용된다. 로컬 체인이 생성한 블록에는 각 지역별로 발생한 사용자 트랜잭션, 블록 합의 트랜잭션 등이 포함된다.

[0078] 지역 서버는 특정 블록 번호(i)를 가진 메인 체인 블록을 수신한 후, 그 내부 트랜잭션들을 순회하면서 재분할 대상 트랜잭션을 선정한다(S301). 재분할 대상 선정에 포함되는 트랜잭션은, 예를 들어, 명시적으로 다른 지역으로 상태 데이터를 옮길 때 활용되는 사용자 핸드오버 트랜잭션을 포함한다.

[0079] 다음, 사용자 트랜잭션의 접근 상태가 다른 지역을 재분할할 필요가 있는지 확인하고, 그럴 필요가 있는 트랜잭션인 경우에 그 상태들을 기준으로 재분할 제안 생성을 수행한다(S302).

[0080] 재분할 대상 선정 절차 즉, 재분할 제안(reshard proposal, RP)은 재분할 대상으로 선정된 트랜잭션 상의 상태들(keys)로 구성되고, 인덱스, 출발지 지역, 목적지 지역 등을 포함하여 트랜잭션 형태로 인코딩된다. RP의 상세 구성은 후술할 도 3에서 보다 상세히 설명된다.

[0081] 다음, 재분할 제안 트랜잭션이 메인 체인상 커밋으로 확정되기 까지 기다릴 수 있다(S303). 재분할 제안 트랜잭션이 메인 체인상 커밋으로 확정된다는 것은 해당 재분할 제안을 생성한 메인체인 블록에 대한 합의 증명 데이터, 이를 테면, 정족수(quorum)만큼의 합의 메시지가 확보됨을 의미할 수 있다.

[0082] 다음, 메인체인 블록 합의 증명 데이터가 지역 서버에서 확인되면, 상태 재분할 장치는 재분할 제안을 수행한다(S304). 이것은, 재분할 제안에 기록된 상태 중에 출발지 지역에 해당하는 지역 서버인 경우, 해당 상태의 위상을 "지역(Local)"에서 "전역(Global)"으로 변경하는 것을 의미한다. 재분할 제안이 수행되면, 그 이후의 지역 서버는 해당 상태에 관한 상태 소유권(state ownership)을 잃게 되며, 그에 따라 로컬 수정 권한을 박탈당한다.

[0083] 다음, 목적지 지역에 해당 상태의 소유권을 이전하기 위하여, 재분할 결과를 생성한다(S305). 재분할 결과(reshard result, RR)는 재분할 제안과 동일한 데이터 구조를 사용하며 상태의 위상 값이 "전역(Global)"으로 기록되는 점에서 차이가 있다.

[0084] 재분할 결과는 또한 트랜잭션 형태로 인코딩이 되고, 생성 후에는 메인체인에 전달된다(S306). 재분할 결과가

생성된 메인 체인에 전달되고, 메인체인에 커밋되는 블록은 앞서 수신된 메인 체인 블록(i)과 구별하여 i* 로 표기될 수 있다.

[0085] 다음, 지역 서버는 i* 번째 메인체인 블록을 수신하고(S300 참조), 수신한 메인체인 블록의 내부 트랜잭션들을 순회하면서, i*번째 새로운 메인체인 블록 상의 재분할 대상을 선정하면서(S301), 재분할 대상 선정과 병렬적으로 재분할 결과를 확인한다(S307).

[0086] 다음, 메인 체인 블록(i) 상의 재분할 대상에 대한 재분할 결과가 확인되면, 상태 재분할 장치는 확인된 상태 재분할 결과를 트랜잭션 형태로 인코딩하고 메인체인 블록 합의 증명 데이터 내부에 삽입한다(S308). 그리고, 메인체인 블록 커밋 확정까지 대기한다.

[0087] 그런 다음, 메인체인 커밋이 확정되어 메인체인 블록 합의 증명 데이터가 지역 서버에서 확인되면(S303 참조), 상태 재분할 장치는 재분할 결과를 수행한다(S309). 재분할 결과 수행은 재분할 제안 수행(S304)과 유사하게 진행되는데, 재분할 결과 데이터에 목적지 지역으로 명시된 지역 서버에서, 데이터에 포함된 상태의 위상을 "전역"에서 "로컬"로 수정하고, 상태의 값을 지역 샤드에 새롭게 구성하는 것을 포함할 수 있다. 결과적으로, 위와 같은 절차를 수행함으로써, 지역들 간 데이터를 안전하게 이동시킬 수 있다.

[0088] 도 4는 도 3의 상태 재분할 방법에서 재분할 대상 트랜잭션을 선정하는 절차를 나타낸 흐름도이다.

[0089] 도 4를 참조하면, 상태 재분할 방법에서 재분할 대상 트랜잭션을 선정하기 위해, 메인 체인 블록을 수신하고(S400), 수신한 메인 체인 블록 내부의 트랜잭션들을 순회하면서 트랜잭션을 확인하고(S401), 그 후에 트랜잭션 유형 및 메인 체인상의 검증 결과를 기준으로 특정 트랜잭션(transaction, Tx)를 재분할 대상 트랜잭션으로 선정할 수 있다(S403).

[0090] 재분할 대상 트랜잭션의 선정 기준은, 모든 접근 상태가 "지역" 위상인 트랜잭션이 메인 체인 검증에 실패하는 경우의 트랜잭션 즉, 간섭 로컬 트랜잭션(interfered local Tx), 접근 상태가 "전역" 위상이면서 메인 체인 검증에 성공하는 경우의 트랜잭션 즉, 성공 전역 트랜잭션(successful global Tx), 및 핸드오버 트랜잭션 중 어느 하나를 포함할 수 있다.

[0091] 특히, 간섭 로컬 트랜잭션과 성공 전역 트랜잭션의 두 경우에는, 재분할 대상이 암묵적으로(implicit) 선정될 수 있지만, 핸드오버 트랜잭션은 명시적으로(explicit) 선정되는 특징이 있다. 암묵적으로 선정되는 재분할 대상 상태 집합은 목적지 지역은 출발지 지역과 동일하며, 명시적으로 선정되는 재분할 대상 상태 집합은 후술할 핸드오버 트랜잭션에 사용자가 명시한 목적지 지역으로 재분할 대상을 기록할 수 있다.

[0092] 다음, 재분할 대상 트랜잭션을 선정하고 나면, 상태 재분할 장치는 재분할 대상 트랜잭션의 내부 상태 집합을 재분할 대상 집합에 추가한다(S404). 그리고 블록 내 트랜잭션을 모두 순회했는지 여부 즉, 마지막 트랜잭션까지 확인하고(S405), 최종적으로 재할당 대상 집합을 출력한 후 본 프로세스를 종료할 수 있다.

[0093] 도 5은 도 3의 상태 재분할 방법에서 재분할 제안 및 재분할 결과에 활용되는 재분할 데이터 구조를 나타낸 블록도이다.

[0094] 도 5을 참고하면, 재분할을 위한 데이터 구조(500)는, 인덱스(index, 501), 상태(key, 502), 위상(status, 503), 출발지(src, 504), 목적지(dst, 505), 트랜잭션 식별아이디($TxID_{from}$, 506) 및 값(value, 507)을 나타내는 필드들을 포함하도록 구성될 수 있다.

[0095] 인덱스(index, 501)는 특정 메인체인 블록상의 재분할 대상으로 선정되는 순서를 나타낸다. 상태(key, 502)는 키-값 저장소에 쓰여진 상태의 문자열로 된, 키의 이름을 나타낸다. 위상(status, 503)은 상태의 위상 정보를 나타낸다. 출발지(src, 504)는 출발지 지역 정보를 나타낸다. 목적지(dst, 505)는 목적지 지역 정보를 나타낸다. 트랜잭션 식별 아이디($TxID_{from}$, 506)는 재분할 선정 당시 해당 상태가 포함한 트랜잭션의 식별 아이디를 나타낸다. 그리고 값(value, 507)은 상태의 값을 나타낸다.

[0096] 도 6는 도 3의 상태 재분할 방법에서 상태의 위상 변경에 대한 다이어그램이다.

[0097] 도 6를 참조하면, 최초의 상태 생성은, 그 상태를 생성한 트랜잭션에 의해 초기화될 수 있다(S600). 모든 상태는 지역 서버에서 각 지역에 속한 "지역(Local)" 위상으로 초기화될 수 있다(S610).

[0098] 그리고 상태가 메인체인상의 재분할 제안 대상으로 선정되고 재분할 제안의 수행이 진행되면(S602), "전역(Global)" 위상으로 전이할 수 있다(S630).

[0099] 그런 다음, 재분할 결과가 지역 서버에서 수행되고(S640), 그 이후에 다시 "지역" 위상으로 돌아오는 구조를 가질 수 있다.

[0100] 도 7은 도 3의 상태 재분할 방법에 채용할 수 있는 상태 재분할 제안에서의 핸드오버 트랜잭션 구조를 설명하기 위한 예시도이다.

[0101] 도 7를 참조하면, 핸드오버 트랜잭션(handover_TX, 700)은 단순한 구조를 가질 수 있다. 즉, 사용자 단말에서 생성되고 지역 서버에서 사용되는 핸드오버 트랜잭션(700)은 키-값 저장소에 저장될 상태의 키 이름(key, k), 사용자 단말의 이동 전의 지역 체인(source chain, src), 및 사용자 단말의 이동 후의 지역 체인(destination chain, dst)으로 구성될 수 있다.

[0102] 도 8은 도 3의 상태 재분할 방법을 핸드오버 트랜잭션의 처리 과정 관점에서 설명하기 위한 흐름도이다.

[0103] 도 8을 참조하면, 사용자 단말을 휴대한 사용자가 출발지 지역에서 목적지 지역으로 이동할 수 있다(S800). 이 경우, 목적지 지역의 지역 서버에서 핸드오버 트랜잭션을 생성할 수 있다. 이 때, 사용자 단말은 자신과 상태 정보를 나타내는 키의 이름(k), 출발지 지역 이름(src), 목적지 지역 이름(dst)을 바탕으로 핸드오버 트랜잭션을 생성하고 이를 목적지 지역 서버에 제출한다(S801).

[0104] 다음, 목적지 지역의 지역 서버의 메인 체인상의 핸드오버 트랜잭션이 재분할 선정 절차를 통해 확인되면(S802), 상태 재분할 장치에 대응하는 지역 서버는, 메인 체인상의 상태 즉, 키(k)의 가장 최신 값(v)을 락킹할 수 있다(S803). 그리고, 그 값을 재분할 제안 집합에 포함시킬 수 있다.

[0105] 해당 재분할 제안 집합에 대한 메인 체인 커밋이 확정되면(S804), 출발지 지역 서버는 메인 체인상의 해당 키(k)의 소유권을 박탈할 수 있다(S810). 즉, 재분할 결과를 수행할 수 있다. 또한, 목적지 지역 서버는 재분할 결과 수행하여 메인 체인상의 해당 키(k)의 소유권을 할당받고, 그 값(v)을 자신의 지역 샤드 즉, 로컬 체인에 셋업할 수 있다(S820).

[0106] 그런 다음, 목적지 지역 서버는 메인체인상의 해당 상태 즉, 해당 키(k)의 락킹을 해제할 수 있다(S830).

[0107] 도 9는 본 발명의 다른 실시예에 따른 샤딩 블록체인 플랫폼 상에서 상태 재분할을 수행하는 상태 재분할 장치의 주요 구성을 설명하기 위한 블록도이다.

[0108] 도 9를 참조하면, 상태 재분할 장치(900)는, 적어도 하나의 프로세서(910)를 포함할 수 있다. 이 경우, 적어도 하나의 프로세서(910)는 사용자 단말의 상태를 샤딩 블록체인 플랫폼 상에서 처리하도록 구성될 수 있다. 즉, 적어도 하나의 프로세서(910)는 사용자 단말의 특정 트랜잭션을 샤딩 블록체인 플랫폼 상에서 처리하기 위해 로컬 체인과 메인 체인을 구비하고 상태 재분할 프로토콜에 따라 작동하도록 구성될 수 있다.

[0109] 또한, 상태 재분할 장치(900)는, 선택적으로 메모리(920), 송수신 장치(930), 저장 장치(940), 입력 인터페이스 장치(950), 출력 인터페이스 장치(960) 또는 이들의 조합 구성을 더 포함할 수 있다. 상태 재분할 장치(900)에 포함된 각각의 구성 요소들은 버스(bus, 970)에 의해 연결되어 서로 통신을 수행할 수 있다.

[0110] 상태 재분할 장치(900)의 프로세서(910)는, 메모리(920) 및 저장 장치(940) 중 적어도 하나에 저장된 프로그램 명령(program command)을 실행할 수 있다. 프로그램 명령은 도 3의 상태 재분할 프로토콜 동작의 절차를 수행하기 위한 명령이나 도 4의 재분할 대상 선정 동작의 절차를 수행하기 위한 명령을 포함할 수 있다. 이러한 프로그램 명령은 적어도 하나의 소프트웨어 모듈 형태로 구현될 수 있다. 전술한 프로세서(910)는 중앙 처리 장치(central processing unit, CPU), 그래픽 처리 장치(graphics processing unit, GPU), 또는 본 발명의 실시예에 따른 방법들 중 적어도 하나의 방법이 수행되는 전용의 프로세서를 의미할 수 있다.

[0111] 메모리(920) 및 저장 장치(940) 각각은 휘발성 저장 매체 및 비휘발성 저장 매체 중에서 적어도 하나로 구성될 수 있다. 예를 들어, 메모리(920)는 읽기 전용 메모리(read only memory, ROM) 및 랜덤 액세스 메모리(random access memory, RAM) 중에서 적어도 하나로 구성될 수 있다.

[0112] 송수신 장치(930)는 사용자 단말이나 다른 지역의 지역 서버와 유선, 무선, 위성 또는 이들의 조합 네트워크에서의 통신을 지원하는 수단이나 이러한 수단에 상응하는 기능을 수행하는 구성부를 포함한다. 송수신 장치(930)는 유선, 무선, 위성 또는 이들 조합을 위한 적어도 하나의 서브통신시스템을 포함할 수 있다.

[0113] 입력 인터페이스 장치(950)는 키보드, 마이크, 터치패드, 터치스크린 등의 입력 수단들과, 입력 수단들 중에서 선택되는 적어도 하나와 적어도 하나의 입력 수단을 통해 입력되는 신호를 기저장된 명령과 매핑하거나 처리하

여 프로세서(910)로 전달하는 입력 신호 처리부를 포함할 수 있다.

[0114] 출력 인터페이스 장치(960)는 프로세서(910)의 제어에 따라 출력되는 신호를 기저장된 신호 형태나 레벨로 매핑하거나 처리하는 출력 신호 처리부와, 출력 신호 처리부의 신호에 따라 진동, 빛 등의 형태로 신호나 정보를 출력하는 적어도 하나의 출력 수단을 포함할 수 있다. 적어도 하나의 출력 수단은 스피커, 디스플레이 장치, 프린터, 광 출력 장치, 진동 출력 장치 등의 출력 수단들에서 선택되는 적어도 하나를 포함할 수 있다.

[0115] 전술한 상태 재분할 장치(900)는 통신 네트워크의 하나의 노드인 기지국의 적어도 일부 기능부나 이러한 기능부의 기능을 수행하는 구성부로 구현될 수 있다. 여기서, 기지국은 NB(NodeB), eNB(evolved NodeB), gNB, ABS(advanced base station), HR-BS(high reliability-base station), BTS(base transceiver station), 무선 기지국(radio base station), 무선 트랜시버(radio transceiver), 액세스 포인트(access point), 액세스 노드(node), RAS(radio access station), MMR-BS(mobile multihop relay-base station), RS(relay station), ARS(advanced relay station), HR-RS(high reliability-relay station), HNB(home NodeB), HeNB(home eNodeB), RSU(road side unit), RRH(radio remote head), TP(transmission point), TRP(transmission and reception point) 등으로 지칭될 수 있다.

[0116] 또한, 상태 재분할 장치(900)는 통신 노드로서 기능하는 퍼스털 컴퓨터, 웹 서버, 컴퓨팅 서버, 애플리케이션 서버, 데이터베이스 서버, 파일 서버, 게임 서버, 메일 서버, 프록시 서버 또는 이들의 조합 형태로 사용될 수 있다.

[0117] 또한, 이동 가능한 기지국의 측면에서, 상태 재분할 장치(900)는 무선 단말, 또는 유선 단말과의 혼합 형태인 유무선 단말을 포함할 수 있다. 무선 단말은 이동 단말(mobile terminal), 이동국(mobile station), 진보된 이동국(advanced mobile station), 고신뢰성 이동국(high reliability mobile station), 가입자국(subscriber station), 휴대 가입자국(portable subscriber station), 접근 단말(access terminal), 사용자 장비(user equipment), 위상 단말 등으로 지칭될 수 있고, 네트워크에 연결되어 신호 및 데이터를 송수신하고, 간섭 로컬 트랜잭션, 성공 전역 트랜잭션, 핸드오버 트랜잭션 등의 트랜잭션을 샤딩 블록체인 플랫폼에서 메인 체인을 이용한 상태 재분할 프로토콜 기반으로 처리할 수 있는 통신 노드나 컴퓨팅 장치를 모두 포함할 수 있다.

[0118] 도 10은 도 9의 상태 재분할 장치의 적용예를 설명하기 위한 개념도이다.

[0119] 도 10을 참조하면, 상태 재분할 장치는 기지국 트랜시버 스테이션(base transceiver station) 등의 모바일 에지에 설치될 수 있다. 상태 재분할 장치는 모바일 에지 컴퓨팅(mobile edge computing, MEC)을 위한 MEC 서비스 제공자의 MEC 서버에 결합하거나 탑재되는 형태로 설치될 수 있다. 또한, 상태 재분할 장치는 샤딩 블록체인 플랫폼에서 동작하는 기지국 장비에 결합하거나 탑재되는 형태로 설치될 수 있다. 즉, 상태 재분할 장치는 지역 서버(region server)에 대응될 수 있다.

[0120] 상태 재분할 장치는 상태 샤딩을 사용하여 계층적으로 구성된 블록체인(blockchain)을 포함할 수 있다. 즉, 지역성을 활용하고 이동성을 효과적으로 처리하는 고성능 블록체인을 구축하기 위해, 상태 재분할 장치는 단일 전역 메인 체인으로 여러 로컬 체인을 계층적으로 구성하는 블록체인 샤딩 프레임워크를 이용한다. 이하 블록체인 샤딩 프레임워크를 간략히 MEC-Chain이라고 한다.

[0121] 상태 재분할 장치는 상태 샤딩을 통해 계층적으로 구성된 블록체인으로 설계되는 MEC-Chain을 구비할 수 있다. MEC-Chain은 로컬 체인과 메인 체인의 2단계 블록체인으로 구성될 수 있다.

[0122] 상태 재분할 장치는, 지역 전반에 걸쳐 전역적으로 일관된 데이터(globally consistent data) 상태를 위해 단일 최상위 메인 체인(main chain)을 구비할 수 있다. 메인 체인들(W, X, Y) 각각의 상태 즉, 메인 상태(main state)(Sa, Sb, Sc, Sd, Se, Sf, Sg)는 메인 체인 블록들을 처리하는 것으로부터 구축되며, 데이터 액세스 지역 예컨대, 지역적 워크로드에 따라 상태 소유권(state ownership)이 할당될 수 있다. 지역적 워크로드는 제1 로컬 블록 체인들(w_0, x_0, y_0, z_0)를 포함한 제1 메인체인 블록, 제2 로컬 블록 체인들(w_1, x_1, y_1, z_1)를 포함한 제2 메인체인 블록, 제3 로컬 블록 체인들(w_2, x_2, y_2, z_2)를 포함한 제3 메인체인 블록 등을 포함할 수 있다.

[0123] 상태 소유권은 트랜잭션의 로컬 상태(local state)에 대한 임시 로컬 업데이트를 허용하여 고성능 로컬 트랜잭션 실행을 가능하게 한다. 전술한 상태 재분할 장치는 각 지역에 배치되는 복수의 로컬 체인들 중 하나의 로컬 체인을 구비할 수 있다. 복수의 로컬 체인들은 여러 지역들의 로컬 체인에서 독립적으로 발생한 지역 합의에 따라 병렬로 운용될 수 있다.

[0124] 지역에는 지역 서버(region server), 지역 복제 서버(local replicas) 및 사용자가 있다. 지역 서버는 지역 및

메인 체인 모두에 대한 지역 인식 하이브리드 트랜잭션 실행 및 블록 주문을 담당한다. 특히, 지역 서버는 사용자로부터 트랜잭션 요청을 수신하고 트랜잭션의 지역성 유형(locality type) 즉, 로컬 샤드 또는 교차 샤드를 결정하고 지역성 유형에 따라 스마트 계약에서 다르게 트랜잭션을 실행한다. 지역 서버는 새로운 로컬 블록을 생성하도록 명령하고 생성된 로컬 블록을 지역 내의 로컬 복제 서버로 전달할 수 있다.

[0125] 또한, 지역 서버는 지역으로 커밋된 블록(local-commit blocks)을 메인 네트워크(main network)를 통해 원격 지역들에 브로드캐스팅하여 메인 체인 블록을 생성하는데 참여할 수 있다. 본 실시예에서 각 지역에는 하나 이상의 지역 서버가 존재할 수 있고 장애가 발생할 때까지 각 지역에 하나의 지역 서버만 활성화되어 있다고 가정한다.

[0126] 지역 복제 서버는 지역 상태만을 유지하며 로컬 체인에 대한 블록 합의(block consensus)를 집합적으로 수행하여 지역 내 지역 서버의 동작에 대한 안정적인 복제 및 감사를 수행할 수 있다. 특히, 지역 서버로부터 새로운 블록을 수신하면, 각 지역 복제 서버는 수신된 로컬 블록의 블록 번호/해시, 복제본의 신원(identity) 및 서명을 포함하는 로컬 뷰(local-view)의 간결한 암호화 그래픽 증명을 생성할 수 있다.

[0127] 또한, 지역 복제 서버는, 로컬 뷰를 트랜잭션으로 인코딩하여 로컬 체인 상에 지역 복제 서버들 간의 뷰 공유가 유지되도록 할 수 있다. 지역 복제 서버는 신뢰성을 위해 로컬 블록에서 발견된 로컬 뷰에 대한 분석을 수행할 수 있다. 지역 서버의 악의적인 동작을 감지할 때, 지역 복제 서버는 다른 지역 복제 서버에 서버 변경 제안을 직접 브로드캐스팅함으로써 변경 프로토콜을 호출할 수 있다. 변경 프로토콜을 사용하면, 지역으로 커밋된 모든 블록들은 지역 내의 새로운 지역 서버로 안전하게 이동될 수 있다.

[0128] 메인 체인은 지역 전반에 걸쳐 전역적으로 일관된 뷰(globally consistent veiw)를 제공하며, 모든 지역 서버가 로컬 블록을 서로에게 브로드캐스트할 수 있도록 분산 방식으로 구축된다. 상태 재분할 장치는 일관된 블록 오더링(block ordering)를 위해 미리 정의된 규칙이나 사전에 수행된 블록 합의(block consensus)를 적용하여 각 지역에서 수신된 로컬 블록들로부터 메인 체인(main chain) 블록을 생성할 수 있다.

[0129] 이를 위해, 상태 재분할 장치는 먼저 라운드(round)라는 고정 간격을 정의할 수 있다. 정의된 라운드에 따라, 지역 서버는 고정된 개수의 로컬 커밋 블록을 메인 네트워크(main netwokr)의 다른 모든 지역 서버로 브로드캐스트할 수 있다. 또한, 여러 지역들로부터 고정된 개수의 로컬 블록들을 수신한 후, 지역 서버의 상태 재분할 장치는 일관된 오더링을 위해 지역 식별자 예컨대, 지역 서버의 공개 키인 해시 값별로 사전순(lexicographical order)으로 지역으로 커밋된 블록들을 정렬하여 메인 체인 블록을 생성할 수 있다.

[0130] 또한, 지역 서버는, 사용자 트랜잭션이 발생되지 않았을 때, 필요한 개수의 로컬 커밋 블록들을 브로드캐스트하지 않을 수 있다. 이 경우, 지역 서버는 빈 블록들(empty blocks)을 생성하고 필요한 개수의 블록들을 채우기 위해 빈 블록들을 브로드캐스트할 수 있다. 역으로, 지역 서버는 빈 블록들을 수신할 수 있다. 이러한 절차에 의하면, 각 라운드에서 미리 정의된 개수의 로컬 커밋 블록들이나 빈 블록들로 메인 체인 블록을 생성할 수 있다.

[0131] 상태 재분할 장치는, 고성능을 위하여 로컬 체인을 가속화하기 위해 자체 검증 가능한 원장을 통해 신뢰할 수 있는 합의로부터 블록 오더링 작업을 분리할 수 있다. 블록 오더링을 위해, 지역 서버는 상태 재분할 장치로서 지역으로 수신된 트랜잭션들의 순서를 지정하여 새로운 블록을 생성하고 생성된 블록을 지역 복제 서버로 전파하도록 구성될 수 있다.

[0132] 자체 검증 가능한 원장을 통한 합의를 위해, 지역 복제 서버는 합의 메시지를 교환하기 위한 통신 매체로 로컬 체인을 사용하여 집단적으로 합의를 수행할 수 있다. 즉, 지역 복제 서버는 로컬 체인 상에 로컬 뷰를 트랜잭션으로 유지하고, 수신된 블록에서 로컬 뷰를 분석한 다음, 로컬 체인의 새로 합의된 공통 접두사를 계산하여 합의를 달성할 수 있다. 지역 합의 알고리즘(local consensus algorithm)의 경우, 위의 메커니즘을 지원하기 위해 필요에 따라 일부 수정과 함께 실용적인 비잔틴 결함 허용(byzantine fault tolerance)을 사용할 수 있다. 이러한 구성에 의하면, 지역 서버에서 블록들을 생성하는 속도만큼 지역 합의의 성능이 선형적으로 증가할 수 있다.

[0133] 한편, 지역 서버는 안전 및 실시간 활성(liveness) 측면에서 잠재적으로 단일 고장점이 될 수 있다. 따라서, 안전을 위해, 지역 복제 서버는 정족수(quorum) 기반 비잔틴(Byzantine) 허용 합의 알고리즘을 실행하여 2f+1개의 일관성 있는 숫자를 확인한 후에만 제안된 로컬 블록을 받도록 구성될 수 있다. 또한, 활성을 위해, 지역 복제 서버는 블록 순서지정(ordering) 작업의 속도를 늦출 수 있고, 그래서 각 지역 복제 서버의 블록 도착 시간을 기반으로 타이밍 오류를 감지하기 위해 사용하는 미리 정의된 타이머를 구비할 수 있다.

[0134] 상태 재분할 장치는 MEC 환경에서 용이하게 구현될 수 있으나, 이에 한정되지는 않는다. 상태 재분할 장치 또는

상태 재분할 장치로서 작동하는 지역 서버는 평판이 좋은 에지 서비스 제공자(예컨대, 통신 회사)가 운영 및 관리하는 기지국 트랜시버 스테이션(BTS)에 설치되어 가입자에게 높은 컴퓨팅 리소스를 제공하고 대부분 안정적으로 작동하는 일반적인 에지 컴퓨팅 서버를 포함할 수 있다.

[0135] 또한, 상태 재분할 장치는 지역 인식 하이브리드 트랜잭션을 실행할 수 있다. 즉, 상태 재분할 장치는 소유권이 할당 상태에서만 로컬 트랜잭션에 접근할 수 있고, 그에 의해 전역 합의를 요구하지 않고 지역적으로 로컬 트랜잭션을 업데이트할 수 있다. 한편, 크로스 샤드 트랜잭션은 전역적으로 일관된 메인 체인에 대해 실행되고 검증되어야 하므로, 상태 재분할 장치는 크로스 샤드 트랜잭션의 처리 흐름을 로컬 체인에서의 트랜잭션 실행과 구분하거나 분리할 수 있다. 트랜잭션 실행 중에 로컬 트랜잭션의 읽기/쓰기 세트는 로컬로 유지관리되는 상태에 대해 구축되나, 크로스 샤드 트랜잭션은 전역적으로 유지관리되는 상태에 대해 구축될 수 있다. 그리고 로컬 트랜잭션들은 로컬 상태에서 빠른 실행 중 잠정적으로 업데이트될 수 있으나, 크로스 샤드 트랜잭션은 메인 체인 유효성 검사가 성공한 후에만 적용될 수 있다.

[0136] 또한, 상태 재분할 장치는, 세분화된 사용자 지원형의 상태 재분할 프로토콜에 의해 작동될 수 있다. 즉, 상태 재분할(resharding)은 데이터 접근 지역에 따라 가장 최근에 접근한 지역으로 상태를 적응적으로 교체함으로써 해당 지역에서 발생하는 트랜잭션의 지역 비율을 증가시킬 수 있다. 즉, 재분할 효과는 크로스 샤드 트랜잭션 수가 감소함에 따라 나타나고, 그 결과 메인 체인에서 성공적인 다중 버전 동시성 제어(multi-version concurrency control, MVCC) 검증이 증가할 수 있다.

[0137] 상태 재분할 프로토콜에 대한 네 가지 요구 사항은 다음과 같다.

[0138] i) 상태 정확성: 소스 샤드 즉, 출발지 로컬 체인의 상태가 유효해야 한다. 즉, 올바른 사용자가 생성해야 하며 가장 최근 값을 가져야 한다.

[0139] ii) 소유권 검증 가능성(ownership verfiability): 소유권 양도 이력을 투명하게 확인할 수 있어야 한다.

[0140] iii) 원자성 결정(atomic decision): 재분할(reshard)의 결과는 분할되지 않는 결정이나 중단되지 않는 결정에 의해 모든 지역에서 동일해야 한다. 또한, 동적 지역성에 대한 성능요구사항이 정의될 수 있다.

[0141] iv) 세분화(fine-grained): 세분화는 사용자와 관련된 상태가 사용자의 결정에 따라 재분할되어야 함을 의미한다.

[0142] 상태 재분할 장치는, 재분할(reshard) 프로토콜을 통해 메인 체인을 상태 재할당을 위한 매체로 활용하여 상태 재분할의 요구 사항을 충족할 수 있다. 메인 체인은 지역으로 커밋된 블록들만 포함함으로써 데이터 신뢰성을 보장하고, 샤드들 간 또는 로컬 체인들 간에 복제되기 때문에 샤드들 간의 데이터 전송 기록이 변경 불가능하고 사용 가능함을 보장할 수 있다. 그리고, 상태 재분할 장치는 메인 체인의 정보만 확인하고 처리함으로써 샤드들 간의 원자성 결정에 대한 요구 사항을 충족할 수 있다.

[0143] 상태 재분할(reshard) 프로토콜은 다음의 2단계로 구성될 수 있다.

[0144] 첫째, 메인 체인 유효성 검사에서 수행되는 릴리스(release) 단계에서 지역 서버는 명시적 재분할 트랜잭션을 필터링하여 재분할가능한 트랜잭션을 식별한다. 그런 다음 해당 트랜잭션에 포함된 상태의 소유권을 해제하여 더 이상 지역으로 해당 상태를 업데이트할 수 없도록 동작한다.

[0145] 둘째, 자체(own) 단계는 해제된 상태의 소유권을 새 지역에 재할당한다. 재분할 트랜잭션에는 사용자가 지정한 명시적 대상 지역이 포함되어 있으므로, 상태 재분할 장치는 이를 참조하여 소유권을 대상 지역에 재할당한다.

[0146] 본 실시예에 따르면, 상태 재분할 프로토콜은 샤딩 블록체인에서도 지역성이 동적으로 변하는 워크로드를 효과적으로 처리할 수 있다. 특히, 기존 샤딩 블록체인들이 트랜잭션별 샤딩이나 네트워크 노드별 샤딩을 적용하여 상태 데이터의 지역성 변경에는 대응하지 못하는 문제점을 해결할 수 있다. 즉, 상태 재분할 장치는 지역성이 변하는 시점에 상태 데이터를 적응적으로 재배치함으로써 원격 데이터 접근 및 크로스-샤드 트랜잭션의 빈도를 크게 줄임으로써 고성능 샤딩 블록체인 시스템을 유지할 수 있는 장점을 가진다.

[0147] 본 발명의 실시 예에 따른 방법의 동작은 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 프로그램 또는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의해 읽혀질 수 있는 정보가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0148] 또한, 컴퓨터가 읽을 수 있는 기록매체는 롬(rom), 램(ram), 플래시 메모리(flash memory) 등과 같이 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치를 포함할 수 있다. 프로그램 명령은 컴파일러(compiler)에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다.

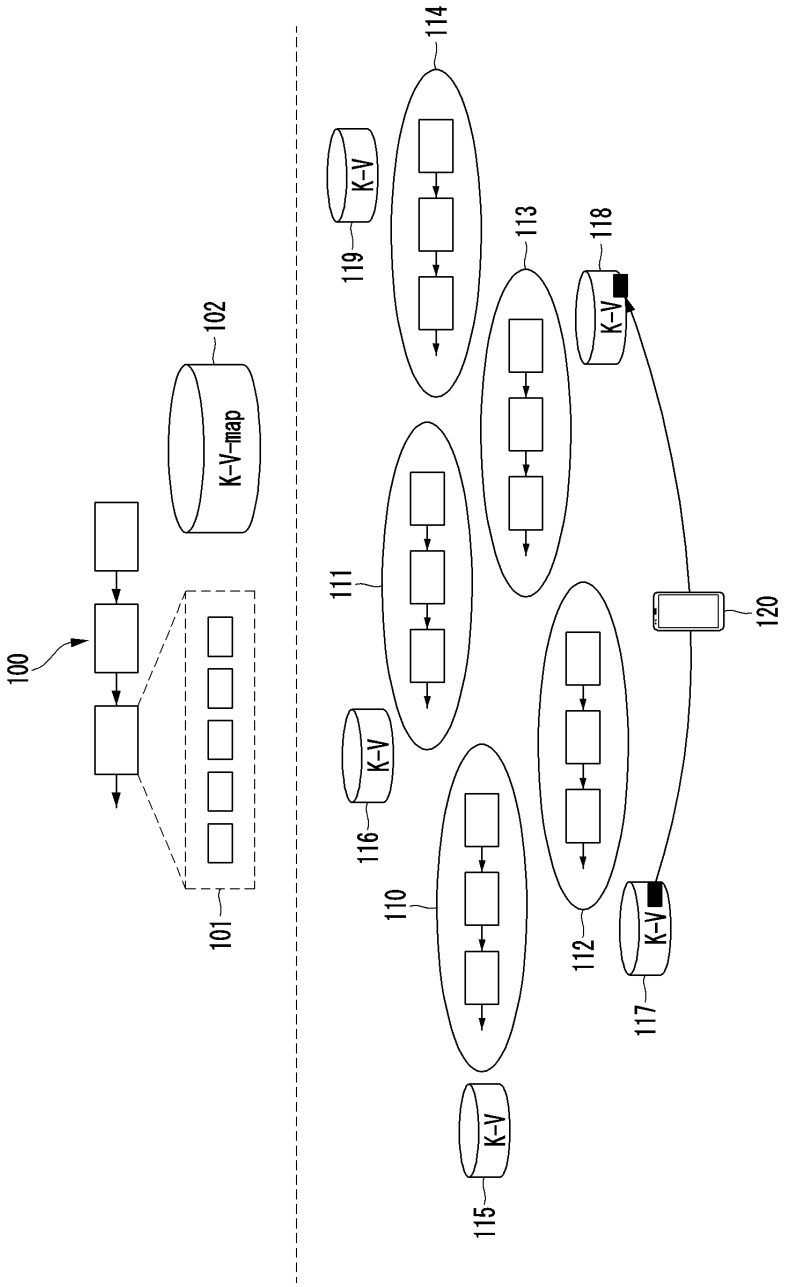
[0149] 본 발명의 일부 측면들은 장치의 문맥에서 설명되었으나, 그것은 상응하는 방법에 따른 설명 또한 나타낼 수 있고, 여기서 블록 또는 장치는 방법 단계 또는 방법 단계의 특징에 상응한다. 유사하게, 방법의 문맥에서 설명된 측면들은 또한 상응하는 블록 또는 아이템 또는 상응하는 장치의 특징으로 나타낼 수 있다. 방법 단계들의 몇몇 또는 전부는 예를 들어, 마이크로프로세서, 프로그램 가능한 컴퓨터 또는 전자 회로와 같은 하드웨어 장치에 의해(또는 이용하여) 수행될 수 있다. 몇몇의 실시 예에서, 가장 중요한 방법 단계들의 적어도 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0150] 실시 예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그래머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시 예들에서, 필드 프로그래머블 게이트 어레이(field-programmable gate array)는 여기서 설명된 방법들 중 하나를 수행하기 위한 마이크로프로세서(microprocessor)와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다.

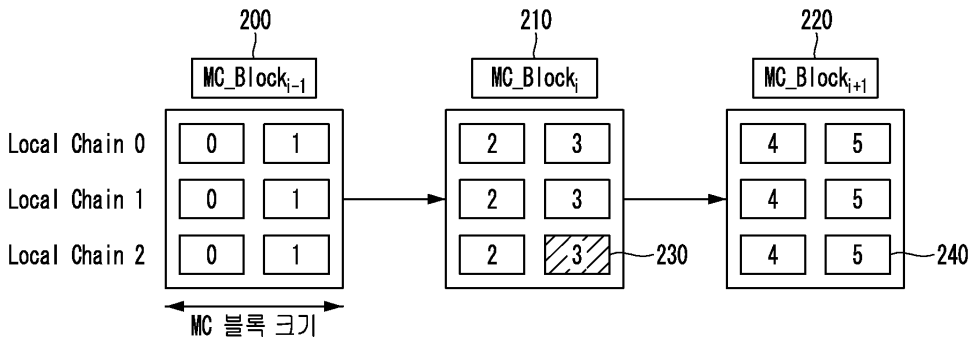
[0151] 이상 본 발명의 바람직한 실시 예를 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

도면

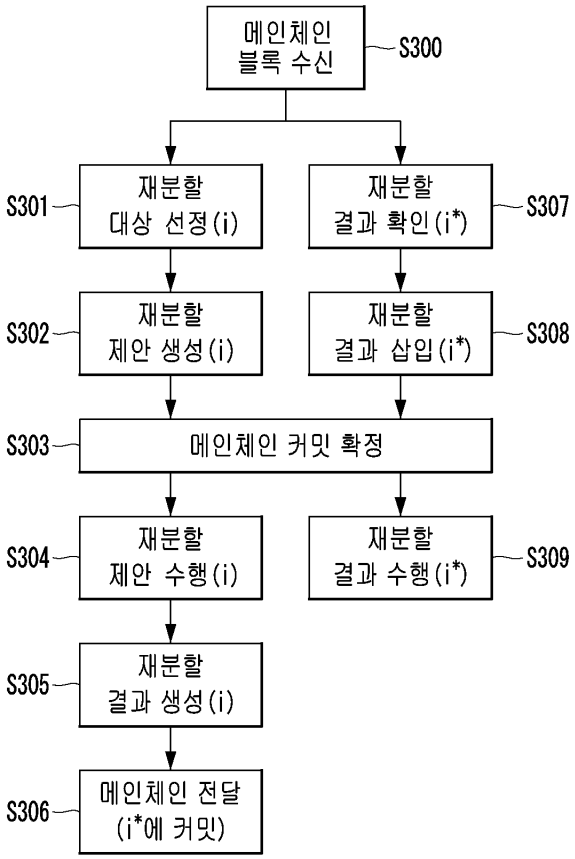
도면1


100
101
102
K-V-map
110
111
112
113
114
115
116
117
118
119
120
K-V

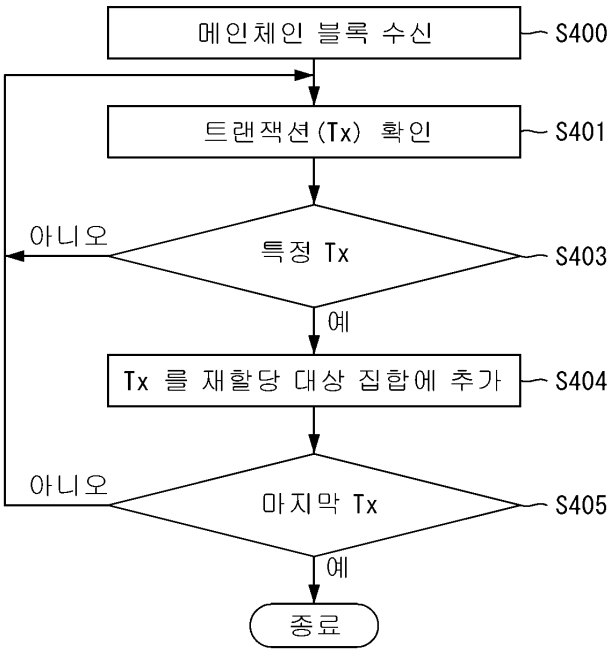
도면2


200
210
220
MC_Block$_{i-1}$
MC_Block$_i$
MC_Block$_{i+1}$
Local Chain 0
Local Chain 1
Local Chain 2
0
1
2
3
4
5
230
240
MC 블록 크기

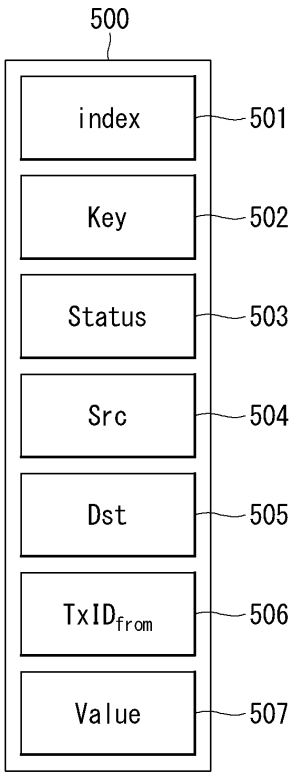
도면3


메인체인
블록 수신
S300
재분할
대상 선정(i)
S301
재분할
결과 확인(i*)
S307
재분할
제안 생성(i)
S302
재분할
결과 삽입(i*)
S308
메인체인 커밋 확정
S303
재분할
제안 수행(i)
S304
재분할
결과 수행(i*)
S309
재분할
결과 생성(i)
S305
메인체인 전달
(i*에 커밋)
S306

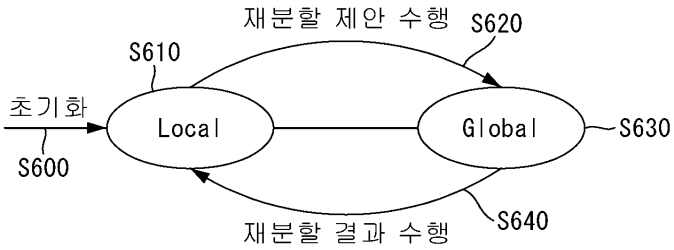
도면4


메인체인 블록 수신
S400
트랜잭션(Tx) 확인
S401
아니오
특정 Tx
S403
예
Tx 를 재할당 대상 집합에 추가
S404
아니오
마지막 Tx
S405
예
종료

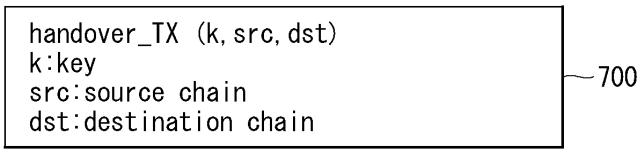
도면5


500
index
501
Key
502
Status
503
Src
504
Dst
505
TxID$_{from}$
506
Value
507

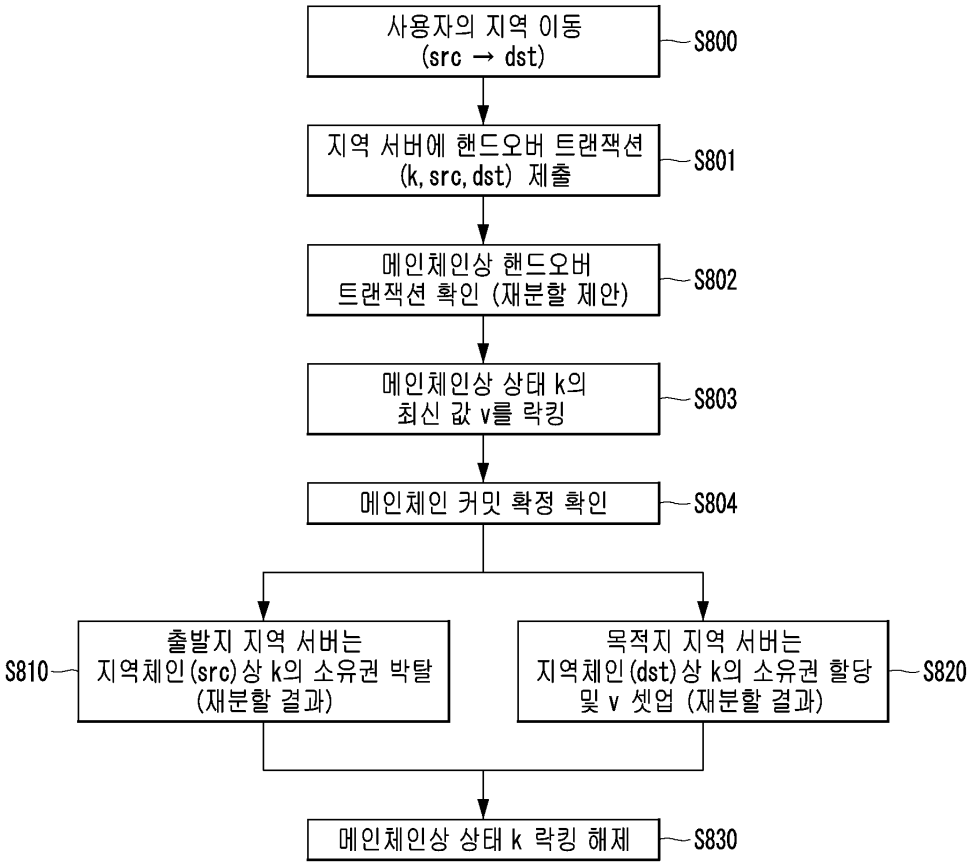
도면6


재분할 제안 수행
S620
S610
초기화
Local
Global
S630
S600
S640
재분할 결과 수행

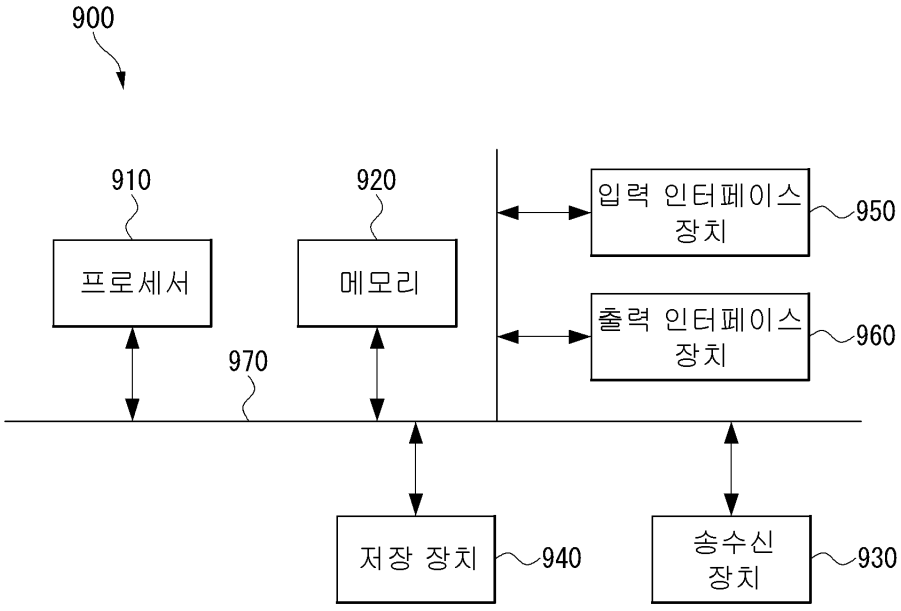
도면7


handover_TX (k, src, dst)
k:key
src:source chain
dst:destination chain
700

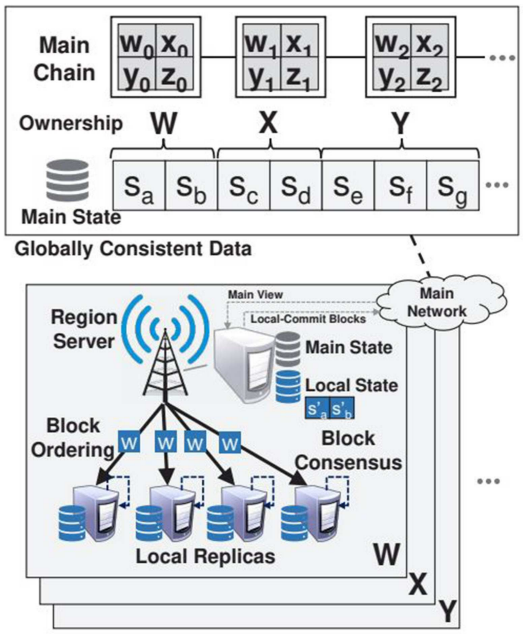
도면8


사용자의 지역 이동
(src → dst)
S800
지역 서버에 핸드오버 트랜잭션
(k, src, dst) 제출
S801
메인체인상 핸드오버
트랜잭션 확인 (재분할 제안)
S802
메인체인상 상태 k의
최신 값 v를 락킹
S803
메인체인 커밋 확정 확인
S804
S810
출발지 지역 서버는
지역체인(src)상 k의 소유권 박탈
(재분할 결과)
목적지 지역 서버는
지역체인(dst)상 k의 소유권 할당
및 v 셋업 (재분할 결과)
S820
메인체인상 상태 k 락킹 해제
S830

도면9


900
910
프로세서
920
메모리
970
입력 인터페이스
장치
950
출력 인터페이스
장치
960
저장 장치
940
송수신
장치
930

도면10


Main Chain
Ownership
W
X
Y
Main State
Globally Consistent Data
Region Server
Main View
Local-Commit Blocks
Main Network
Main State
Local State
Block Ordering
Block Consensus
Local Replicas