(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2023년08월16일
(11) 등록번호 10-2567091
(24) 등록일자 2023년08월10일

(51) 국제특허분류(Int. Cl.)
*G06Q 10/04* (2023.01) *G06Q 20/06* (2012.01)
*H04L 65/40* (2022.01)
(52) CPC특허분류
*G06Q 10/04* (2023.01)
*G06Q 20/065* (2013.01)
(21) 출원번호 10-2021-0019754
(22) 출원일자 2021년02월15일
심사청구일자 2021년02월15일
(65) 공개번호 10-2022-0116655
(43) 공개일자 2022년08월23일
(56) 선행기술조사문헌
KR1020190070888 A*
KR1020200059136 A*
KR1020200134944 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**포항공과대학교 산학협력단**
경상북도 포항시 남구 청암로 77 (지곡동)
(72) 발명자
**박찬익**
경상북도 포항시 남구 지곡로 155, 6동 1105호
**조용래**
경상북도 포항시 남구 연일읍 유강길10번길 18-1, 101동
(74) 대리인
**특허법인이상**

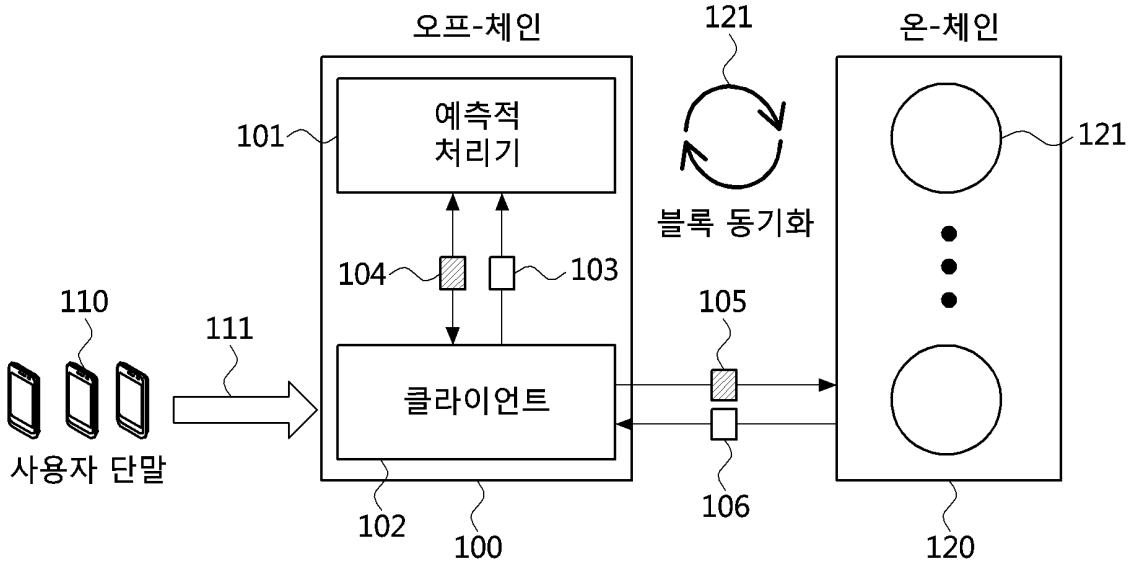
전체 청구항 수 : 총 10 항 심사관 : 박성웅

(54) 발명의 명칭 **블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템 및 방법**

## (57) 요 약

본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템은, 오프 체인 트랜잭션을 예측적 처리하고, 온 체인 트랜잭션을 후 처리하는 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템에 있어서, 서비스 사용을 위한 요청을 클라이언트에게 전달하는 사용자 단말과; 사용자 단말로부터 전달 받은 요청을 트랜잭션으로 구성하여 오프 체인의 예측적 처리기와 온 체인의 블록체인에 전달하는 오프 체인의 클라이언트; 및 데이터 구조와 연산을 활용하여 트랜잭션을 예측적 처리하고, 처리된 결과를 클라이언트에 전달하고, 클라이언트로부터 전달된 블록 데이터에 대해 후 처리를 진행하는 예측적 처리기; 를 포함한다.

*대 표 도* - 도1



(52) CPC특허분류
*H04L 67/1095* (2022.05)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711125876
과제번호 2020-0-00936-002
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 블록체인융합기술개발(R&D)
연구과제명 5G 초저지연 서비스를 위한 무선 단말용 블록체인기술 개발
기 여 율 60/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2021.01.01 ~ 2021.12.31
이 발명을 지원한 국가연구개발사업
과제고유번호 1711193875
과제번호 2021-0-00484-003
부처명 과학기술정보통신부
과제관리(전문)기관명 정보통신기획평가원
연구사업명 데이터경제를위한블록체인기술개발(R&D)
연구과제명 노드 간 메시지 전달과 합의를 위한 최적 경로 네트워크프로토콜 기술개발
기 여 율 40/100
과제수행기관명 포항공과대학교 산학협력단
연구기간 2023.01.01 ~ 2023.12.31

# 명 세 서

## 청구범위

### 청구항 1

블록체인 네트워크에 접속될 수 있는 예측적 트랜잭션 처리 시스템에 있어서,

사용자 단말로부터 서비스 이용 요청을 받아들이고, 상기 서비스 이용 요청에 관련된 트랜잭션을 예측적 처리기와 상기 블록체인 네트워크에 전달하며, 상기 블록체인 네트워크로부터 수신되는 온-체인 트랜잭션 결과를 상기 예측적 처리기에 전달하고, 상기 예측적 처리기로부터 수신되는 오프-체인 예측적 처리 결과 및 최종 결과를 상기 사용자 단말에 전달하는 서비스 클라이언트; 및

데이터 구조와 연산을 활용하여 상기 트랜잭션의 예측적 처리를 실행하여 상기 오프-체인 예측적 처리 결과를 생성해서 상기 서비스 클라이언트에 전달하고, 상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과의 동일 여부에 따른 후 처리를 진행하는 상기 예측적 처리기;

를 포함하며,

상기 후 처리는 상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과의 동일 여부에 따라 상기 오프-체인 예측적 처리 결과를 확정하는 것과, 상기 오프-체인 예측적 처리 결과의 무효화 또는 상기 예측적 처리의 재실행을 수행하는 것 중에서 어느 하나을 포함하는,

예측적 트랜잭션 처리 시스템.

### 청구항 2

청구항 1에 있어서, 상기 예측적 처리기는,

상기 서비스 클라이언트가 오프라인 상태에서 상기 블록체인 네트워크로부터 블록 데이터를 주기적으로 가져와 상기 예측적 처리기 내에 있는 상기 트랜잭션의 상태를 갱신하는 블록 동기화를 실행하는 백그라운드 블록 동기화기를 포함하는,

예측적 트랜잭션 처리 시스템.

### 청구항 3

청구항 1에 있어서, 상기 예측적 처리기는,

상기 오프-체인 예측적 처리 결과를 저장하는 예측 상태 DB;

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과가 동일함에 따른 상기 오프-체인 예측적 처리 결과의 확정 상태를 저장하는 확정 상태 DB;

상기 확정 상태에 이르기 전까지 상기 트랜잭션의 모든 상태와 실행 기록을 저장하는 히스토리 로그 DB; 및

트랜잭션간 의존성 정보를 저장하는 의존성 정보 DB;

를 포함하는 데이터베이스를 구비하는,

예측적 트랜잭션 처리 시스템.

### 청구항 4

청구항 1에 있어서, 상기 예측적 처리기는,

상기 트랜잭션을 수신하는 시점에서 준비 상태로 진입하고;

상기 예측적 처리를 실행한 후에 예비 확정 상태로 변화하고;

상기 오프-체인 예측적 처리 결과가 확정될 때 최종-확정 상태로 변화하고;

상기 준비 상태에서 상기 트랜잭션이 이전 취소된 트랜잭션과의 의존성 관계를 가지는 경우, 사전취소 상태로 변화하는,

예측적 트랜잭션 처리 시스템.

**청구항 5**

블록체인 네트워크에 접속될 수 있는 서비스 클라이언트와 연동되어 동작하는 예측적 트랜잭션 처리 장치에 의해 수행되는 예측적 트랜잭션 처리 방법으로서,

사용자 단말로부터의 서비스 이용 요청에 상응한 트랜잭션을 상기 블록체인 네트워크로 전송하는 상기 서비스 클라이언트로부터, 상기 블록체인 네트워크로 전송되는 상기 트랜잭션을 받아들이는 단계;

데이터 구조와 연산을 활용하여 상기 트랜잭션의 예측적 처리를 실행하여 오프-체인 예측적 처리 결과를 생성해서 상기 서비스 클라이언트에 전달하는 단계;

상기 서비스 클라이언트를 통해서 상기 블록체인 네트워크에서 생성된 온-체인 트랜잭션 결과를 받아들이는 단계; 및

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과의 동일 여부에 따른 후 처리를 진행하는 단계;

를 포함하는,

예측적 트랜잭션 처리 방법.

**청구항 6**

청구항 5에 있어서, 상기 트랜잭션의 예측적 처리를 실행하여 오프-체인 예측적 처리 결과를 생성해서 상기 서비스 클라이언트에 전달하는 단계는,

상기 트랜잭션에 고유 순서 번호를 할당하는 단계와;

상기 트랜잭션의 상기 예측적 처리를 실행하는 단계와;

데이터베이스에 저장되어 있는 상기 오프-체인 예측적 처리 결과 및 데이터 구조를 갱신하는 단계;를 포함하는,

예측적 트랜잭션 처리 방법.

**청구항 7**

청구항 5에 있어서,

상기 후 처리 이후의 최종 처리 결과를 상기 서비스 클라이언트에 제공하는 단계;

를 더 포함하는,

예측적 트랜잭션 처리 방법.

**청구항 8**

청구항 5에 있어서, 상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과의 동일 여부에 따른 상기 후 처리를 진행하는 단계는,

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과를 비교하는 단계와;

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과가 동일한 경우, 상기 오프-체인 예측적 처리 결과를 확정하는 단계와;

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과가 동일하지 않은 경우, 상기 오프-체인 예측적 처리 결과를 무효화하는 단계;

를 포함하는,

예측적 트랜잭션 처리 방법.

**청구항 9**

청구항 8에 있어서,

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과가 동일하지 않은 경우, 상기 오프-체인 예측적 처리 결과를 무효화하는 단계는

상기 예측적 처리의 재실행을 수행하는 단계;를 포함하는,

예측적 트랜잭션 처리 방법.

**청구항 10**

청구항 8에 있어서,

상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과를 비교하는 단계는,

상기 온-체인 트랜잭션 결과를 통보 받는 단계와;

의존성 정보 관리 그래프에서 상기 온-체인 처리 완료된 트랜잭션에 상응하는 노드를 검색하고, 그 노드의 진입 간선에 연결된 노드 집합을 계산하는 단계와;

노드 집합이 공집합이거나, 노드 집합의 각 노드 상태가 모두 최종 확정인지 여부를 확인하는 단계와;

노드 집합의 각 노드 상태가 모두 최종 확정되었는지 여부에 따라 상기 오프-체인 예측적 처리 결과와 상기 온-체인 트랜잭션 결과가 동일한지 판단하는 단계; 를 포함하는,

예측적 트랜잭션 처리 방법.

**청구항 11**

삭제

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 블록체인 확장성을 높이기 위한 오프 체인 상에서의 예측적 트랜잭션 처리 시스템 및 방법에 관한 발명이다.

### *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 합의 알고리즘 개선, 암호 기법 개선, 오프 체인 트랜잭션 처리 등 다양한 기법들이 개발되고 있다. 예를 들어, 블록체인 오프 체인 트랜잭션 처리 방법은 모든 블록체인 노드들이 참여하는 온 체인 트랜잭션 처리에 비해 속도가 매우 빠르다. 그 이유는 거래 당사자들만 참여하는 작은 규모의 네트워크(즉, 오프 체인)에서 신속한 합의가 진행되기 때문이다.

[0004] 한편, 컴퓨터 프로그램의 성능 향상을 위해서, 예측적 처리 기법(Speculative execution)이 존재한다. 예측적 처리 기법은 프로그램이 실행하려는 어떤 연산이 완료되기 전에, 미리 그 결과를 예측하고, 그 예측된 결과 값을 다음 연산 실행에 활용하는 방식으로 성능을 높이는 일반적인 방법이다. 하지만, 예측적 처리 기법은 예측 결과가 실제 결과와 다를 경우, 별도의 후 처리 과정이 필요하다. 별도의 후 처리 과정으로는, 예측 실패한 연산 및 그 연산과 의존 관계를 가지는 다른 연산들의 효과를 실패 이전의 안정적인 상태로 복구하는 연산 등이 포함된다.

## *발명의 내용*

### *해결하려는 과제*

[0005] 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은, 오프 체인에서의 예측적 처리 기법을 이용하여 블록체인 트랜잭션의 신속한 처리를 지원하는 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템 및 방법을 제공하는데 있다.

## *과제의 해결 수단*

[0006] 상기 목적을 달성하기 위한 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템은, 오프 체인 트랜잭션을 예측적 처리하고, 온 체인 트랜잭션을 후 처리하는 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템에 있어서, 서비스 사용을 위한 요청을 클라이언트에게 전달하는 사용자 단말과; 사용자 단말로부터 전달 받은 요청을 트랜잭션으로 구성하여 오프 체인의 예측적 처리기와 온 체인의 블록체인에 전달하는 오프 체인의 클라이언트; 및 데이터 구조와 연산을 활용하여 트랜잭션을 예측적 처리하고, 처리된 결과를 클라이언트에 전달하고, 클라이언트로부터 전달된 블록 데이터에 대해 후 처리를 진행하는 예측적 처리기; 를 포함할 수 있다.

[0007] 예측적 처리기는, 클라이언트가 오프라인 상태인 경우에 온 체인의 블록 데이터를 주기적으로 가져와 로컬 확정 상태를 갱신하는 연산을 실행하기 위한 온 체인의 백그라운드 블록 동기화와 연동될 수 있다.

[0008] 예측적 처리기의 데이터 구조는, 오프 체인 상에서 예측적 처리 결과를 반영하는 예측 상태 정보 데이터 베이스와; 고유 순서 별 트랜잭션 및 그 상태를 저장하는 히스토리와; 트랜잭션간 의존성 정보를 관리하는 의존성 정보 관리 그래프; 및 온 체인상 트랜잭션 처리 결과를 관리하는 확정 상태 정보 데이터 베이스; 를 포함할 수 있다.

[0009] 본 발명의 다른 목적을 달성하기 위한 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 방법은, 예측적 처리기가 오프 체인 트랜잭션을 예측적 처리하는 예측 연산 수행 단계와; 온 체인 트랜잭션을 후 처리하는 후 처리 연산 수행 단계; 를 포함할 수 있다.

[0010] 예측 연산 수행 단계는, 트랜잭션에 고유 순서 번호를 할당하는 순서 단계와; 트랜잭션을 실행하는 실행 단계와; 트랜잭션간 의존성 정보 분석 및 계산하는 단계; 및 실행 결과 및 데이터 구조를 갱신하는 단계; 를 포함할 수 있다.

[0011] 예측 연산 수행 단계는, 클라이언트가 사용자 단말 트랜잭션을 예측적 처리기에 전달하는 단계와; 예측적 처리 단계 진입 및 사용자 단말 트랜잭션에 대한 고유 순서 번호 할당 단계와; 복수의 파라미터로 구성된 정보를 로컬 스토리지에 로그 선행 기입하는 단계와; 사용자 단말 트랜잭션 실행 결과 값을 예측 상태 정보 데이터 베이스에 저장하는 단계와; 트랜잭션 실행 결과 값을 클라이언트에 전달하는 단계와; 파라미터 사용자 단말 트랜잭션에 대한 의존성 정보를 계산하는 단계; 및 파라미터를 예측적 처리기의 데이터 구조의 히스토리와 의존성 정보 관리 그래프에 저장하는 단계; 를 포함할 수 있다.

[0012] 후 처리 연산 수행 단계는, 오프 체인상 트랜잭션의 예측 결과와 온 체인상 트랜잭션 실행 결과간 비교하는 검사 단계와; 검사 단계의 오프 체인상 트랜잭션의 예측 결과와 온 체인상 트랜잭션 실행 결과가 동일하면 확정하는 단계와; 검사 단계의 오프 체인상 트랜잭션의 예측 결과와 온 체인상 트랜잭션 실행 결과가 틀리면 취소하는 단계와; 취소하는 단계가 실행되면 예측 상태 정보 데이터 베이스를 온 체인 블록체인과 일관된 상태로 되돌리는 되감기(rollback) 단계; 및 되감기(rollback) 단계가 실행된 트랜잭션들을 재실행(re-execution)하는 재실행 단계; 를 포함할 수 있다.

[0013] 후 처리 연산 수행 단계는, 예측적 처리기가 온 체인 처리된 트랜잭션를 전달 받고, 그와 동일한 고유 식별자를 가지는 오프 체인 처리된 트랜잭션를 검색하는 단계와; 온 체인 처리된 트랜잭션이 커밋(commit)되었는지 여부를 확정하는 단계와; 온 체인 처리된 트랜잭션이 커밋(commit)된 경우, 확정 상태 정보 데이터베이스에 온 체인 처리된 트랜잭션의 실행 결과를 반영하는 단계와; 온 체인 처리된 트랜잭션과 동일한 트랜잭션 고유 식별자를 가지며 예측적 실행되었던 트랜잭션의 순서 및 실행 결과가 서로 일치하는지 비교하는 단계와; 히스토리 자료 구조에 온 체인 처리된 트랜잭션 결과를 갱신하고, 프로그램을 종료하는 단계; 를 포함할 수 있다.

[0014] 후 처리 연산 수행 단계는, 예측적 처리기가 온 체인 처리된 트랜잭션을 전달 받고, 그와 동일한 고유 식별자를 가지는 오프 체인 처리된 트랜잭션을 검색하는 단계와; 온 체인 처리된 트랜잭션이 커밋(commit)되었는지 여부를 확정하는 단계와; 온 체인 처리된 트랜잭션이 커밋(commit)되지 않은 경우, 의존성 정보 관리 그래프상 온 체인 처리된 트랜잭션와 선행 및 후행 관계에 있는 모든 예측 상태의 트랜잭션을 계산하여 이를 집합 A 에 포함하는 단계와; 의존성 정보 관리 그래프에 집합 A가 비어 있는지 여부를 확인하는 단계를 실행하고, 집합 A가 비어 있는 경우 종료하는 단계와; 집합 A가 비어 있지 않은 경우, 의존성 정보 관리 그래프에서 집합 A를 삭제하

고, 집합 A의 각 트랜잭션의 상태를 취소(abort) 상태로 갱신하는 단계와; 예측 상태 정보 데이터 베이스를 확정 상태 정보 데이터 베이스로 되감기(rollback)하는 단계; 및 예측 상태 정보 데이터 베이스에 대해 집합 A의 각 트랜잭션을 재실행하고 프로그램을 종료하는 단계; 를 포함할 수 있다.

[0015] 예측적 처리 연산 단계는, 트랜잭션은 제출 시점에서 준비 상태로 진입하는 단계와; 예측적 실행에 의해 예비 확정 상태로 변화하는 단계와; 온 체인 처리 결과에 따라 후 처리 취소에 의한 최종 취소 상태로 변화하거나, 후 처리 확정에 의한 최종-확정 상태로 변화하는 단계와; 준비 상태로 진입하는 단계에서, 이전 취소된 트랜잭션과의 의존성 관계를 가지는 경우, 사전취소 상태로 변화하는 단계; 를 포함할 수 있다.

[0016] 온 체인 처리된 트랜잭션과 동일한 트랜잭션 고유 식별자를 가지며 예측적 실행되었던 트랜잭션의 순서 및 실행 결과가 서로 일치하는지 비교하는 단계는, 예측적 처리기가 온 체인 처리 완료된 트랜잭션을 통보 받는 단계와; 의존성 정보 관리 그래프에서 온 체인 처리 완료된 트랜잭션에 상응하는 노드를 검색하고, 그 노드의 진입 간선에 연결된 노드 집합을 계산하는 단계와; 노드 집합이 공집합이거나, 노드 집합의 각 노드 상태가 모두 최종 확정인지 여부를 확인하는 단계; 및 노드 집합의 각 노드 상태가 모두 최종 확정되었으면, "네"를 리턴하는 단계를; 노드 집합의 각 노드 상태가 모두 최종 확정되지 않았으면, "아니오"를 리턴하는 단계; 를 포함할 수 있다.

## *발명의 효과*

[0017] 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템 및 방법에 의하면, 사용자 단말에서 제출한 트랜잭션을 오프 체인상에서 예측적 처리하고 결과를 사용자에게 전송함으로써, 온체인상 높은 지연을 갖는 분산 합의가 끝나기 전에 결과를 신속하게 알 수 있다. 이를 통해 블록체인 성능 확장성뿐만 아니라 트랜잭션 지연 시간을 획기적으로 개선할 수 있는 장점을 가진다.

[0018] 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템 및 방법에 의하면, 예측 처리기는 다양한 블록체인 플랫폼의 전단계 처리 모듈로 적용할 수 있는 장점을 가진다.

## *도면의 간단한 설명*

[0019] 도 1은 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템의 구성을 나타낸 도면이다.

도 2 는 도 1의 시스템에서 예측적 처리기에 의한 트랜잭션 처리를 위해 사용되는 데이터 구조를 나타낸 도면이다.

도 3은 도 1의 시스템에서 예측적 처리기에 의한 트랜잭션 처리를 위해 진행하는 연산을 나타낸 도면이다.

도 4는 도 1의 시스템에서 예측적 처리기에 의해 정의되는 트랜잭션 상태 변화도를 나타낸 도면이다.

도 5는 도 1의 시스템에서 예측적 처리기의 클라이언트 트랜잭션에 대한 예측적 처리 단계 동작을 나타낸 도면이다.

도 6a 및 6b는 도4의 예측적 처리기의 주요 연산에서 예측적 처리기의 온 체인 트랜잭션에 대한 후 처리 단계 동작을 나타낸 도면이다.

도 7 은 도 6a 및 6b의 온 체인 트랜잭션(T')와 오프-체인 트랜잭션(T)에 대해 순서 및 실행 결과를 비교하는 단계를 나타낸 도면이다.

## *발명을 실시하기 위한 구체적인 내용*

[0020] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 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. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0021] 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는 데 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.

[0022] 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

[0023] 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, "포함하다" 또는 "가지다" 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, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0024] 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 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0025] 이하, 본 발명의 바람직한 실시예를, 첨부한 도면들을 참조하여 보다 상세하게 설명한다.

[0027] 도 1은 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템의 구성을 나타낸 도면이다.

[0028] 도 1을 참조하면, 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템은, 사용자 단말(110), 오프 체인(100)의 예측적 처리기(101) 및 클라이언트(102), 온 체인(120)을 포함한다.

[0029] 사용자 단말(110)은 블록체인 기반 서비스 사용자로 간주될 수 있으며, 서비스 사용을 위한 요청(111)을 클라이언트(102)에게 전달한다. 클라이언트(102)는 전달 받은 요청을 트랜잭션(104)으로 구성하여 오프 체인(100)의 예측적 처리기(101)와 온 체인(120) 블록체인에 동시 전달한다. 온 체인(120)의 트랜잭션 처리가 진행되는 동안, 오프 체인(100)의 예측적 처리기(101)는 데이터 구조와 주요 연산을 활용하여 트랜잭션을 예측적 처리(speculative execution)한다.

[0030] 예측적 처리기(101)는 처리된 결과를 클라이언트(102)에 전달하고 클라이언트(102)는 사용자 단말(110)에 최종 결과를 전달한다. 그리고 온 체인(120) 트랜잭션 결과가 블록 형태(106)로 송신되어 클라이언트(102)가 수신하면, 클라이언트(102)는 이를 예측적 처리기(101)에 전달(103)한다.

[0031] 전달받은 블록 데이터(103)에 대해 예측적 처리기(101)는 후 처리 단계를 진행하며, 여기에는 오프 체인(100)상 예측한 트랜잭션 결과와 온 체인(120)상 트랜잭션 결과를 비교하는 단계, 그리고 결과 동일 유무에 따른 트랜잭션 상태 최종 확정 또는 트랜잭션 취소, 상태 되감기(rollback), 트랜잭션 재실행하는 단계가 포함된다.

[0032] 또한, 백그라운드 블록 동기화(121)는, 클라이언트(102)가 오프라인 상태일 때는 예측적 처리기(101)가 클라이언트(102) 도움 없이 온 체인(120) 블록 데이터를 주기적으로 가져와 로컬 확정 상태를 갱신하는 연산이다.

[0034] 도 2 는 도 1의 시스템에서 예측적 처리기에 의한 트랜잭션 처리를 위해 사용되는 데이터 구조를 나타낸 블록도이다.

[0035] 도 2를 참조하면, 예측적 처리기(101)가 예측적 처리 및 후 처리에 사용하는 데이터 구조는 예측 상태 정보 데이터 베이스(DB)(131)와, 확정 상태 정보 데이터 베이스(DB)(134)와, 히스토리(132)와, 의존성 정보 관리 그래프(133)를 포함한다.

[0036] 예측 상태 정보 데이터 베이스(131)는 오프 체인(100) 상에서 예측적 처리 결과를 반영한다.

[0037] 확정 상태 정보 데이터 베이스(134)는 온 체인(120)상 트랜잭션 처리 결과를 관리한다.

[0038] 히스토리(132)는 고유 순서 별 트랜잭션 및 그 상태를 저장한다.

[0039] 의존성 정보 관리 그래프(133)는 트랜잭션간 의존성 정보를 관리한다.

[0041] 도 3은 도 1의 시스템에서 예측적 처리기(101)가 트랜잭션 처리를 위해 진행하는 연산을 도시한 흐름도이다.

[0042] 도 3을 참조하면, 예측적 처리 연산 단계(S141)를 구성하는 단계는, 각 트랜잭션 별 고유 순서 번호를 할당하는 단계(S110), 트랜잭션을 실행하는 단계(S120), 트랜잭션간 의존성 정보 분석 및 계산하는 단계(S130), 실행 결과 및 데이터 구조를 갱신하는 단계(S140)를 포함한다.

[0043] 후 처리 단계(S142)를 구성하는 단계는, 오프 체인(100)상 트랜잭션의 예측 결과와 온 체인(120)상 트랜잭션 실행 결과간 비교하는 검사 단계(S210), 그 결과가 옳다면 확정하는 단계(S220), 틀리면 취소하는 단계(S230), 취소된 경우에는 예측 상태 정보 데이터 베이스(DB)를 온 체인 블록체인과 일관된 상태로 되돌리는 되감기(rollback) 단계(S240), 되감기 된 트랜잭션들을 재실행(re-execution)하는 단계(S250)를 포함한다.

[0045] 도 4는 도 1의 시스템에서 예측적 처리 연산 단계(S141)에 의해 정의되는 트랜잭션 상태 변화도를 도시한 흐름도이다.

[0046] 도4를 참조하면, 트랜잭션은 제출 시점에서 준비 상태(S501)로 진입한다.

[0047] 다음으로, 예측적 실행(S506)에 의해 예비 확정 상태(S502)로 변화한다.

[0048] 온 체인 처리 결과에 따라 후 처리 취소(S507)에 의한 최종 취소 상태(S503) 또는 후 처리 확정(S509)에 의한 최종 확정 상태(S505)로 변화한다.

[0049] 또한, 준비 단계에서 이전 취소된 트랜잭션과의 의존성 관계를 가지는 경우(S508), 사전 취소 상태(S504)로 변화한다.

[0051] 도 5는 도 1의 시스템에서 예측적 처리기의 클라이언트 트랜잭션에 대한 예측적 처리 단계 동작을 나타낸 흐름도이다.

[0052] 도 5를 참조하면, 본 실시예에 따른 예측적 처리 방법의 예측적 처리 연산 단계(S141)는 S201 내지 S207의 일련의 단계들로 구성된다.

[0053] 먼저, 클라이언트가 사용자 단말 트랜잭션(T)을 예측적 처리기(101)에 전달하는 단계(S201)가 실행된다.

[0054] 다음으로, 예측적 처리 단계 진입 및 사용자 단말 트랜잭션(T)에 대한 고유 순서 번호(S) 할당 단계(S202)가 실행된다.

[0055] 그리고, 3개의 파라미터로 구성된 정보(S, T, I)를 로컬 스토리지에 로그 선행 기입하는 단계(S203)가 실행된다.

[0056] 그리고, 사용자 단말 트랜잭션 T 실행 결과 값(R)을 예측 상태 정보 데이터 베이스(DB)에 저장하는 단계(S204)가 실행된다.

[0057] 여기서, 결과 값(R)을 클라이언트에 전달하는 단계(S205)와, 파라미터 사용자 단말 트랜잭션(T)에 대한 의존성 정보(D)를 계산하는 단계(S206) 및 파라미터(T, S, D)를 데이터 구조 히스토리와 의존성 정보 관리 그래프에 저장하는 단계(S207)가 실행된다.

[0059] 도 6a 및 6b는 도4의 예측적 처리기(101)의 주요 연산에서 예측적 처리기(101)의 온 체인(120) 트랜잭션에 대한 후 처리 단계(S142)의 동작을 나타낸 흐름도이다.

[0060] 도 6a 및 6b를 참조하면, 본 실시예에 따른 온 체인(120) 처리 결과에 대한 예측적 처리기(101)의 후 처리 방법은 S300 내지 S314의 일련의 단계들로 구성된다.

[0061] 예측적 처리기(101)는 온 체인 처리된 트랜잭션(T')를 전달 받고, 그와 동일한 고유 식별자(ID)를 가지는 과거 오프 체인 처리된 트랜잭션(T)를 검색하여(S300), 그 확정 유무를 판단(S301)한다. 그리고 그 유무에 따라 실행 경로가 S302과 S310의 제1 실행 경로와 제2 실행 경로의 두 가지 경로로 나뉜다.

[0063] S301이후 제1 실행 경로로, 온 체인 처리된 트랜잭션(T')가 확정된 경우, 확정 상태 정보 데이터베이스(134)에 온 체인(120) 처리된 트랜잭션(T')의 실행 결과를 반영한다(S302).

[0064] 그리고 온 체인 처리된 트랜잭션(T')와 동일한 트랜잭션 고유 식별자를 가지며 과거 예측적 실행되었던 트랜잭션(T)의 순서 및 실행 결과가 서로 일치하는지를 비교한다(S303).

[0065] S303 단계에서 온 체인 처리된 트랜잭션(T')와 동일한 트랜잭션 고유 식별자를 가지며 과거 예측적 실행되었던 트랜잭션(T)의 순서 및 실행 결과가 서로 일치한다면, 히스토리(132) 자료구조에 온 체인 처리된 트랜잭션(T') 결과를 갱신하며(S304), 프로그램은 종료된다.

[0066] 하지만, S303 단계에서 온 체인 처리된 트랜잭션(T')와 동일한 트랜잭션 고유 식별자를 가지며 과거 예측적 실행되었던 트랜잭션(T)의 순서 및 실행 결과가 서로 일치하지 않는다면, 의존성 정보 관리 그래프(G) 상 온 체인 처리된 트랜잭션(T')와 선행 및 후행 관계에 있는 모든 예측 상태의 트랜잭션을 계산하여 이를 집합 A 에 포함

한다.

[0068] S301이후의 제2 실행 경로로, 온 체인 처리된 트랜잭션(T')가 확정되지 않은 경우, 의존성 정보 관리 그래프(G) 상 온 체인 처리된 트랜잭션(T')와 후행 관계에 있는 모든 예측 상태의 트랜잭션을 계산하여 이를 집합 A 에 포함한다(S310).

[0070] S301 이후의 제1 실행 경로 및 제2 실행 경로에서 집합 A 가 계산된 경우, 의존성 정보 관리 그래프(G)(133) 에서 집합 A가 비어 있는 지 여부를 확인한다(S311).

[0071] 만일, 의존성 정보 관리 그래프(G)(133)에서 집합 A가 비어 있지 않으면, 의존성 정보 관리 그래프(G)(133)에서 집합 A를 삭제하고, H에서 집합 A 의 각 트랜잭션의 상태를 취소(abort) 상태로 갱신한다(S312)하고, 의존성 정보 관리 그래프(G)(133)에서 집합 A가 비어 있으면 프로그램을 종료한다.

[0072] 그 후 예측 상태 정보 데이터 베이스(131)를 확정 상태 정보 데이터 베이스(134)로 되감기(rollback)한다(S313).

[0073] 마지막으로, 예측 상태 정보 데이터 베이스(131)에 대해 집합 A 의 각 트랜잭션을 재실행하고(S314), 프로그램은 종료된다.

[0075] 도 7 은 도 6a 및 6b의 온 체인 처리된 트랜잭션(T')와 오프-체인 처리된 트랜잭션(T)에 대한 순서 및 실행 결과를 비교하는 단계(S303)를 보다 구체적으로 나타낸 도면이다.

[0076] 도 7을 참조하면, 예측적 처리기(101)는 온 체인 처리 완료된 트랜잭션(T')를 통보 받는다(S401).

[0077] 의존성 정보 관리 그래프(G)에서 온 체인 처리 완료된 트랜잭션(T')에 상응하는 노드를 검색하고, 그 노드의 진입 간선에 연결된 노드 집합(N)을 계산한다(S402).

[0078] 노드 집합(N)이 공집합이거나, 노드 집합(N)의 각 노드 상태가 모두 최종 확정되었는지 유무를 확인한다(S403).

[0079] 노드 집합(N)의 각 노드 상태가 모두 최종 확정되었으면, "네"를 리턴하고(S404), 노드 집합(N)의 각 노드 상태가 모두 최종 확정되지 않았으면, "아니오"를 리턴한다(S405).

[0080]

[0081] 본 발명의 블록체인 확장성을 위한 예측적 트랜잭션 처리 시스템을 구현하기 위한 방법으로, 예측적 처리기(Speculator) 모듈을 정의한다.

[0082] 예측적 처리기는 클라이언트가 제출한 트랜잭션을 블록체인상 분산 합의를 거치기 전, 이를 예측적으로(speculative) 처리함으로써, 신속하게 클라이언트에게 응답을 전달하며, 이를 통해 초저지연 트랜잭션을 지원한다. 이때 블록체인상 분산 합의와는 비동기적으로 진행되며, 블록체인상 분산 합의 결과에 따라 예측 처리기는 예측적으로 처리한 결과에 대해 최종적으로 확정(commit) 또는 취소(abort)에 대하여 사후 처리(post-processing)를 한다.

[0083] 예측 처리기에서 유지 관리하는 데이터 구조는, 예측적으로 실행하는 트랜잭션 결과, 즉 예측(Speculation) 상태를 저장하는 예측 상태 데이터 베이스(DB), 블록체인 분산 합의에 따른 확정(Commit) 상태를 저장하는 확정 상태 데이터 베이스(DB), 확정 상태 전까지 모든 예측 트랜잭션 상태 및 그 실행 기록을 포함하는 히스토리 로그, 예측 실행 트랜잭션간 읽기/쓰기 집합(read/write set) 의존성 관계를 나타내는 방향 비순환 그래프(Directed Acyclic Graph, DAG) 구조의 의존성 정보 등으로 구성된다.

[0084] 예측 처리기의 트랜잭션 처리 과정은, 트랜잭션의 예측적 실행을 진행하는 오프-체인상 예측적 처리 단계와 온 체인상 합의 결과를 기반으로 하는 후 처리 단계를 포함한다.

[0085] 일 실시예에서, 예측적 처리 단계는, 클라이언트로부터 전달 받은 트랜잭션에 대해 실행 순서 번호 할당하는 단계(order), 트랜잭션을 스마트 컨트랙트 로직에 따라 실행하는 단계(execute), 트랜잭션에 실행 결과에 대한 읽기/쓰기 집합 (read/write set) 의존성 정보를 분석하는 단계(build), 그리고 관련 데이터구조를 갱신하는 단계(update)로 진행된다.

[0086] 일 실시예에서, 후 처리 단계에서는, 온 체인상에서 합의되는 블록 정보를 기반으로 진행되며, 예측적 처리기는 각 블록 내부에 저장되어 있는 트랜잭션들에 대해서 후 처리를 진행한다. 후 처리 단계에는, 블록내 트랜잭션별 예측 결과를 비교하는 검사 단계(check), 검사 결과에 따라, 예측 결과와 온 체인 확정 결과가 같으면 확정(commit) 하는 단계, 또는 그렇지 않으면 취소(abort) 하는 단계로 구성된다. 취소되는 경우, 취소된 트랜잭션

에 의한 상태 갱신을 무효화시키는 되감기(rollback) 단계가 진행되고, 되감기된 트랜잭션들에 대해 클라이언트에게 알림(notification) 전달하고 재실행 단계(re-execute) 단계가 진행된다.

[0087] 일 실시예에서, 예측 처리기는 트랜잭션의 예측적 실행을 위해, 스마트 컨트랙트(smart contract) 유지, 최신 데이터 상태 정보 관리, 그리고 온 체인 확정 결과를 검증하기 위한 온 체인 장부 데이터(ledger) 유지와 온 체인 블록 동기화 등의 기능을 지원한다.

[0088] 일 실시예에서, 예측 처리기 소프트웨어는 클라이언트와 같은 머신상에서 동작한다.

[0089] 일 실시예에서, 예측 처리의 트랜잭션간 비교의 의미는 방향 비순환 그래프 구조를 갖는 의존성 정보 관리 그래프상 트랜잭션에 상응하는 그래프 노드의 전/후 간선 관계 비교 및 트랜잭션 실행 결과 비교를 나타낸다.

[0090] 본 발명에 의하면, 사용자 단말에서 제출한 트랜잭션을 오프 체인상에서 예측적 처리하고 결과를 사용자에게 전송함으로써, 온체인상 높은 지연을 갖는 분산 합의가 끝나기 전에 결과를 신속하게 알 수 있다. 이를 통해 블록체인 성능 확장성뿐만 아니라 트랜잭션 지연 시간을 획기적으로 개선할 수 있는 장점을 가진다.

[0091] 본 발명에 의하면, 예측 처리기는 다양한 블록체인 플랫폼의 전단계 처리 모듈로 적용할 수 있는 장점을 가진다.

[0093] 본 발명의 실시예들에 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 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산 방식으로 컴퓨터로 읽을 수 있 는 프로그램 또는 코드가 저장되고 실행될 수 있다.

[0094] 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 만 들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터(interpreter) 등을 사용해서 컴퓨터에 의해 실행될 수 있는 고급 언어 코드를 포함할 수 있다. 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. 몇 몇의 실시예에서, 가장 중요한 방법 단계들의 하나 이상은 이와 같은 장치에 의해 수행될 수 있다.

[0095] 실시예들에서, 프로그램 가능한 로직 장치(예를 들어, 필드 프로그래머블 게이트 어레이)가 여기서 설명된 방법들의 기능의 일부 또는 전부를 수행하기 위해 사용될 수 있다. 실시예들에서, 필드 프로그머블 게이트 어레이는 여기서 설명된 방 법들 중 하나를 수행하기 위한 마이크로프로세서와 함께 작동할 수 있다. 일반적으로, 방법들은 어떤 하드웨어 장치에 의해 수행되는 것이 바람직하다. 이상 본 발명의 바람직한 실시예를 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.

## *부호의 설명*

[0096] 100 : 오프 체인

101 : 예측적 처리기

102 : 클라이언트

110 : 사용자 단말

120 : 온 체인

131 : 예측 상태 정보 데이터 베이스

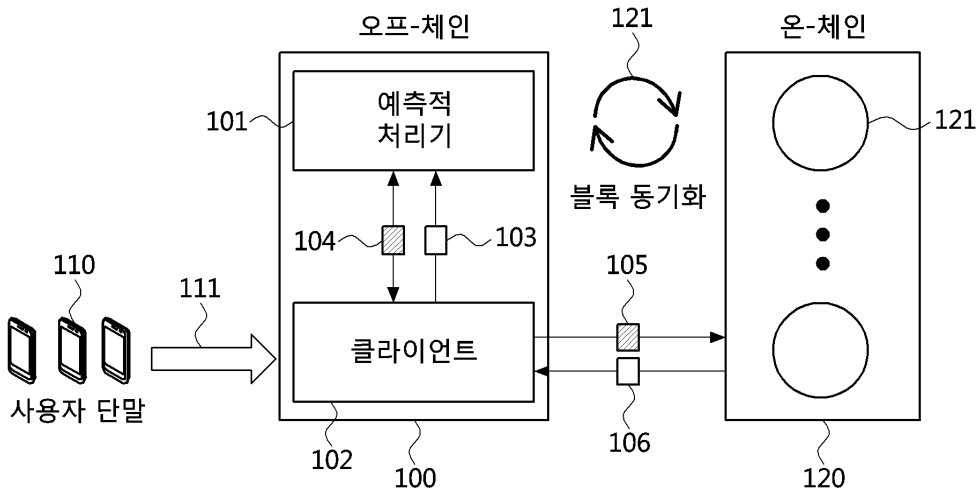
132 : 히스토리

133 : 의존성 정보 관리 그래프

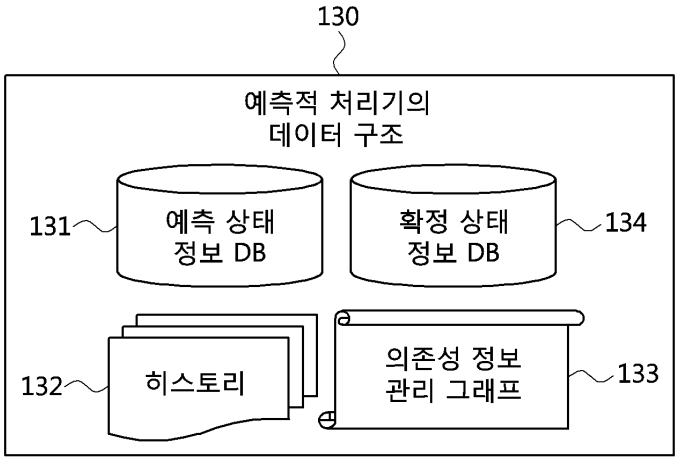
134 : 확정 상태 정보 데이터 베이스

도면

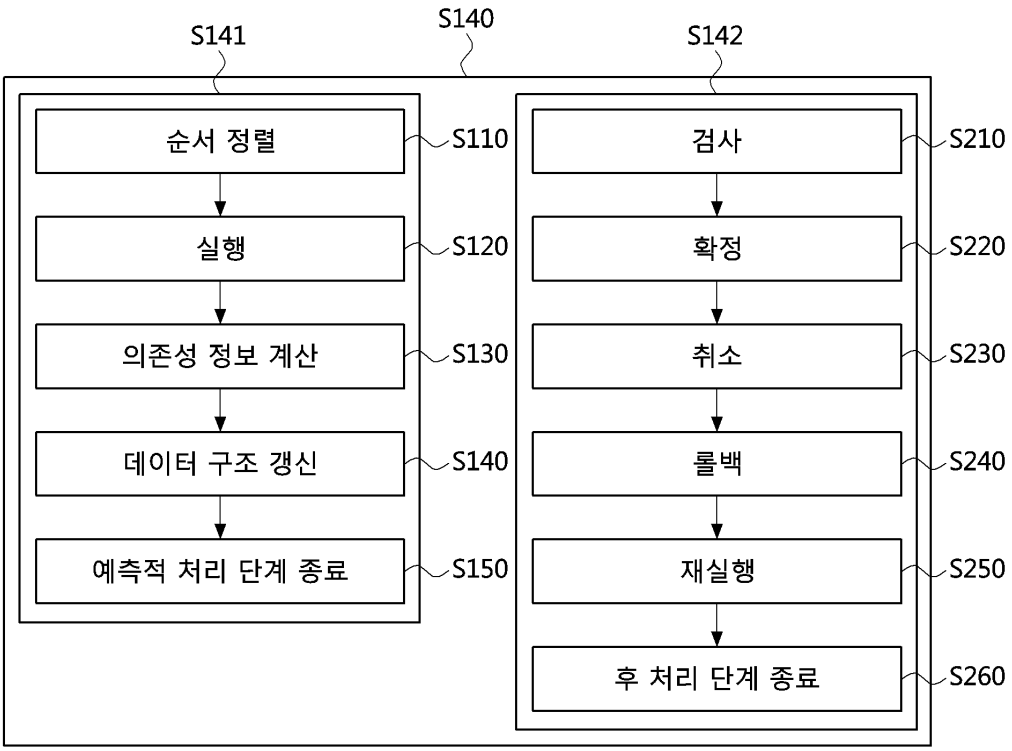
도면1


오프-체인
121
온-체인
101
예측적
처리기
121
블록 동기화
104
103
110
111
105
클라이언트
사용자 단말
106
102
100
120

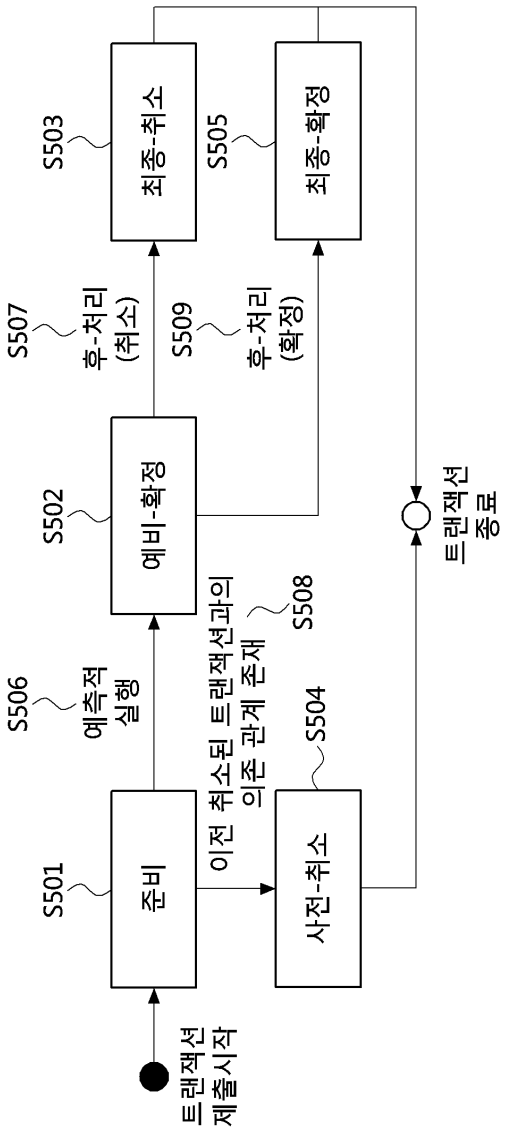
도면2


130
예측적 처리기의
데이터 구조
131
예측 상태
정보 DB
확정 상태
정보 DB
134
132
히스토리
의존성 정보
관리 그래프
133

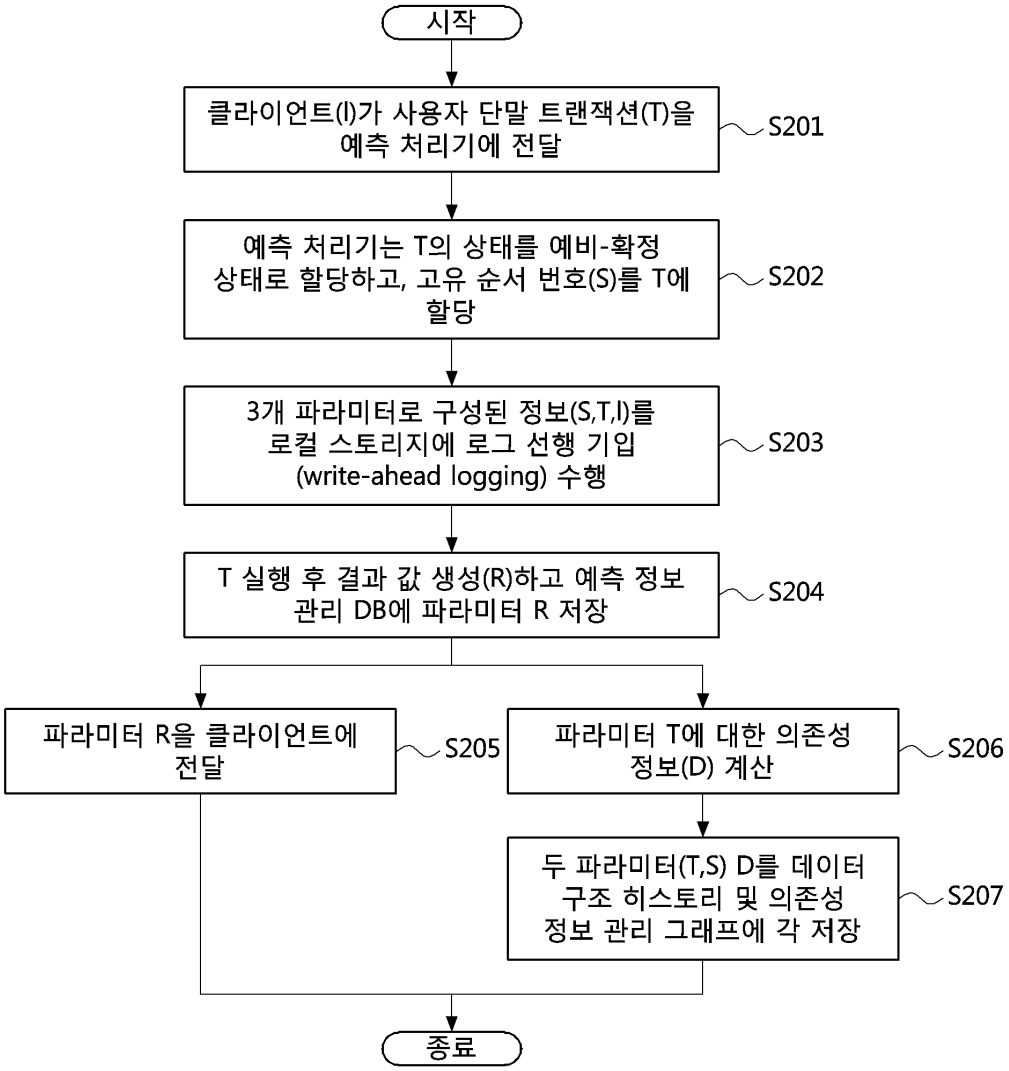
도면3


S141
S140
S142
순서 정렬
S110
실행
S120
의존성 정보 계산
S130
데이터 구조 갱신
S140
예측적 처리 단계 종료
S150
검사
S210
확정
S220
취소
S230
롤백
S240
재실행
S250
후 처리 단계 종료
S260

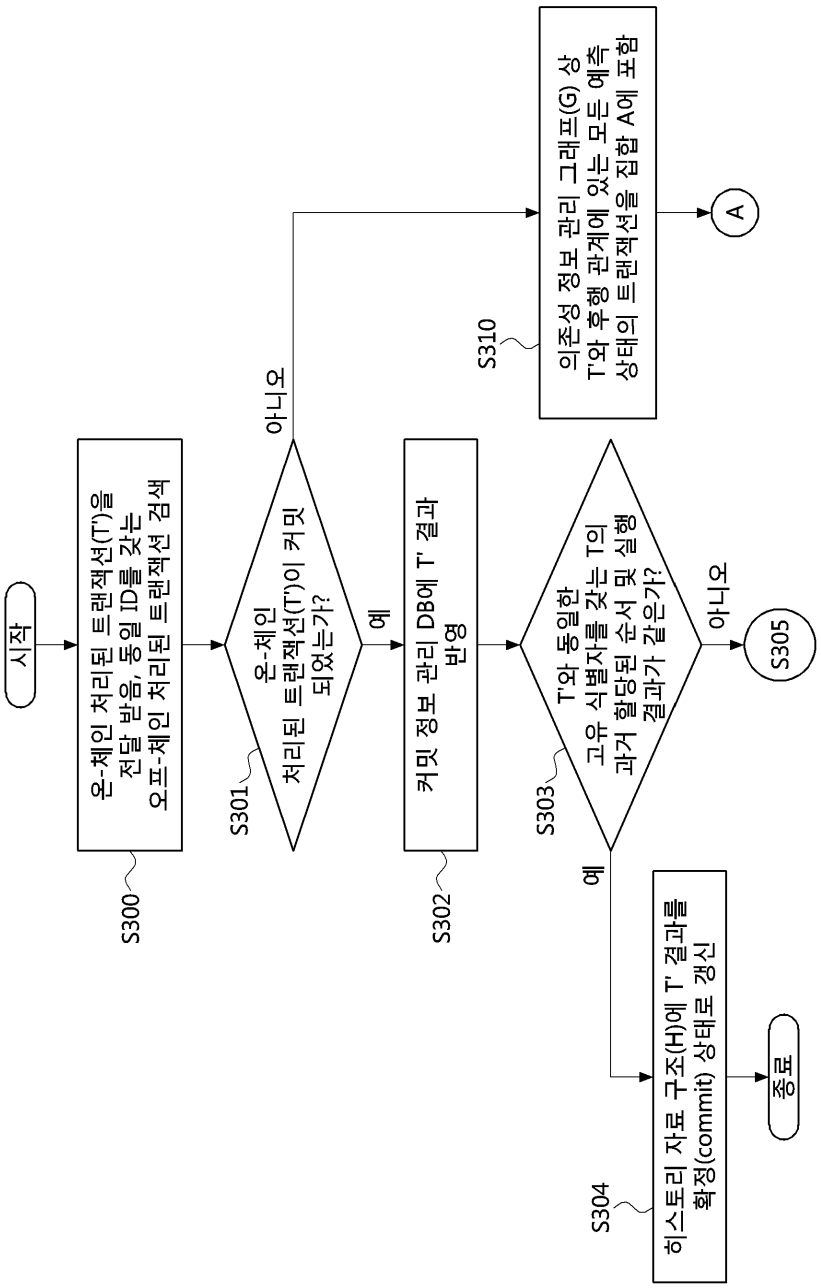
도면4


트랜잭션
제출시작
S501
준비
S506
예측적
실행
S502
예비-확정
S507
후-처리
(취소)
S503
최종-취소
S509
후-처리
(확정)
S505
최종-확정
이전 취소된 트랜잭션과의
의존 관계 존재
S508
S504
사전-취소
트랜잭션
종료

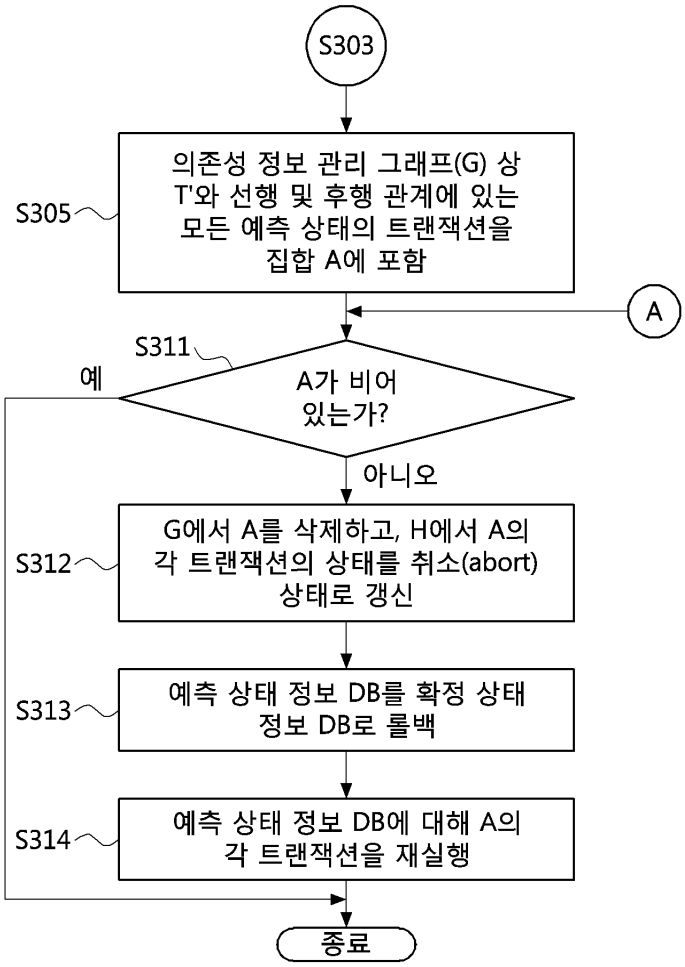
도면5


시작
클라이언트(I)가 사용자 단말 트랜잭션(T)을 예측 처리기에 전달
S201
예측 처리기는 T의 상태를 예비-확정 상태로 할당하고, 고유 순서 번호(S)를 T에 할당
S202
3개 파라미터로 구성된 정보(S,T,I)를 로컬 스토리지에 로그 선행 기입 (write-ahead logging) 수행
S203
T 실행 후 결과 값 생성(R)하고 예측 정보 관리 DB에 파라미터 R 저장
S204
파라미터 R을 클라이언트에 전달
S205
파라미터 T에 대한 의존성 정보(D) 계산
S206
두 파라미터(T,S) D를 데이터 구조 히스토리 및 의존성 정보 관리 그래프에 각 저장
S207
종료

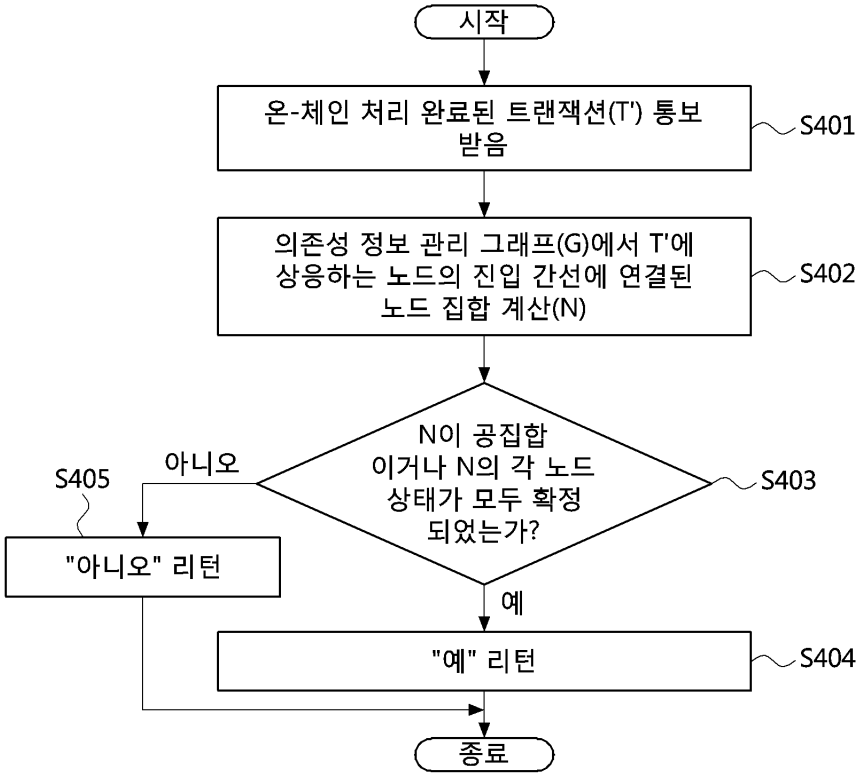
도면6a


시작
온-체인 처리된 트랜잭션(T')을 전달 받음, 동일 ID를 갖는 오프-체인 처리된 트랜잭션 검색
S300
온-체인 처리된 트랜잭션(T')이 커밋 되었는가?
S301
아니오
예
의존성 정보 관리 그래프(G) 상 T'와 후행 관계에 있는 모든 예측 상태의 트랜잭션을 집합 A에 포함
S310
A
커밋 정보 관리 DB에 T' 결과 반영
S302
T'와 동일한 고유 식별자를 갖는 T의 과거 할당된 순서 및 실행 결과가 같은가?
S303
아니오
S305
예
히스토리 자료 구조(H)에 T' 결과를 확정(commit) 상태로 갱신
S304
종료

도면6b


S303
S305
의존성 정보 관리 그래프(G) 상 T'와 선행 및 후행 관계에 있는 모든 예측 상태의 트랜잭션을 집합 A에 포함
A
S311
예
A가 비어 있는가?
아니오
S312
G에서 A를 삭제하고, H에서 A의 각 트랜잭션의 상태를 취소(abort) 상태로 갱신
S313
예측 상태 정보 DB를 확정 상태 정보 DB로 롤백
S314
예측 상태 정보 DB에 대해 A의 각 트랜잭션을 재실행
종료

도면7


시작
온-체인 처리 완료된 트랜잭션(T') 통보 받음
S401
의존성 정보 관리 그래프(G)에서 T'에 상응하는 노드의 진입 간선에 연결된 노드 집합 계산(N)
S402
N이 공집합 이거나 N의 각 노드 상태가 모두 확정 되었는가?
S403
아니오
S405
"아니오" 리턴
예
"예" 리턴
S404
종료