



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2021년12월09일  
(11) 등록번호 10-2337170  
(24) 등록일자 2021년12월03일

- (51) 국제특허분류(Int. Cl.)  
G06Q 20/38 (2012.01) G06F 16/24 (2019.01)  
G06F 16/27 (2019.01) G06Q 20/02 (2012.01)  
G06Q 20/40 (2012.01) H04L 9/06 (2006.01)  
H04L 9/32 (2006.01)
- (52) CPC특허분류  
G06Q 20/3829 (2013.01)  
G06F 16/24 (2019.01)
- (21) 출원번호 10-2020-7015438
- (22) 출원일자(국제) 2019년05월29일  
심사청구일자 2020년06월22일
- (85) 번역문제출일자 2020년05월28일
- (65) 공개번호 10-2020-0090168
- (43) 공개일자 2020년07월28일
- (86) 국제출원번호 PCT/US2019/034271
- (87) 국제공개번호 WO 2019/231965  
국제공개일자 2019년12월05일
- (30) 우선권주장  
201810532710.7 2018년05월29일 중국(CN)
- (56) 선행기술조사문헌  
US05982893 A  
US10692078 B1  
US20180315047 A1  
US20180323965 A1

- (73) 특허권자  
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.  
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
- (72) 발명자  
왕 지유안  
중국 저지앙 311121 항저우 유 향 디스트릭트 웨스트 웨이 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층  
두 후아빙  
중국 저지앙 311121 항저우 유 향 디스트릭트 웨스트 웨이 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층  
안 수에빙  
중국 저지앙 311121 항저우 유 향 디스트릭트 웨스트 웨이 이 로드 넘버 969 빌딩 3 알리바바 그룹 리갈 디파트먼트 5층
- (74) 대리인  
김태홍, 김진희

전체 청구항 수 : 총 15 항

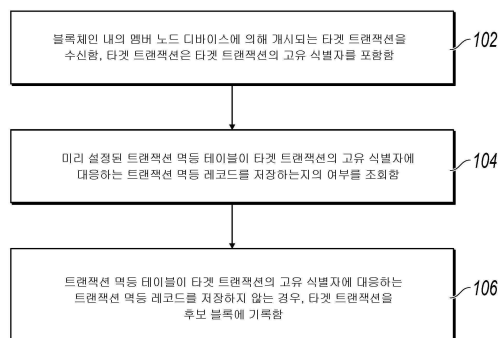
심사관 : 권태헌

(54) 발명의 명칭 **블록체인 기반 트랜잭션 프로세싱 방법 및 장치, 및 전자 디바이스**

(57) 요약

본 출원의 하나 이상의 구현에는 블록체인 기반 트랜잭션 프로세싱 방법 및 장치, 및 전자 디바이스를 제공한다. 방법은: 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 타겟 트랜잭션을 수신함, 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함함 - 을 수신하는 것을 포함할 수 있다. 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부가 조회된다. 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하지 않는 경우, 타겟 트랜잭션은 후보 블록에 기록된다.

대표도 - 도1



(52) CPC특허분류

*G06F 16/275* (2019.01)

*G06Q 20/02* (2013.01)

*G06Q 20/3825* (2013.01)

*G06Q 20/389* (2013.01)

*G06Q 20/401* (2020.05)

*G06Q 20/405* (2013.01)

*H04L 9/0643* (2013.01)

*H04L 9/3247* (2013.01)

*H04L 9/3297* (2013.01)

---

**명세서**

**청구범위**

**청구항 1**

블록체인 기반 트랜잭션을 프로세싱하기 위한 컴퓨터 구현 방법(computer-implemented method)으로서,

블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 블록체인 내의 제2 멤버 노드 디바이스가 개시한 타겟 트랜잭션 - 상기 타겟 트랜잭션은 상기 타겟 트랜잭션의 고유 식별자 및 로직 클럭의 생성 타임스탬프를 규정하는 상기 블록체인 내의 후보 블록의 블록 높이를 포함함 - 을 수신하는 단계;

상기 타겟 트랜잭션의 고유 식별자에 기초하여, 상기 타겟 트랜잭션이 트랜잭션 유효 기간 내에 수행되도록 승인된 것을 결정함으로써, 상기 타겟 트랜잭션이 유효하다는 것을 결정하는 단계 - 상기 트랜잭션 유효 기간은 연체된 트랜잭션을 유효한 트랜잭션과 구별할 수 있도록 하며 상기 후보 블록의 블록 높이와 임계값 사이의 차이에 의해 특성 묘사됨(characterized) - ;

상기 타겟 트랜잭션의 생성 타임스탬프가 상기 블록체인 내의 블록의 다른 생성 타임스탬프에 비해 단조 증가하고 있음을 검증함으로써 상기 후보 블록이 합법적인 블록이라는 것을 결정하는 단계;

상기 타겟 트랜잭션이 유효하고 상기 후보 블록이 합법적인 블록이라는 것을 결정하는 것에 응답하여, 상기 블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 타겟 트랜잭션의 고유 식별자에 기초하여 트랜잭션 멱등 테이블(transaction idempotent table)로부터 누락된 트랜잭션 멱등 레코드를 결정하기 위해 상기 블록체인 상의 상기 트랜잭션 멱등 테이블을 조회하는(querying) 단계 - 상기 트랜잭션 멱등 테이블은 상기 블록체인 내의 복수의 멤버 노드 디바이스 사이에 설정된(established) 합의 메커니즘을 사용함으로써 상기 블록체인 내의 복수의 멤버 노드 디바이스에 의해 공동으로 유지되고, 하나 이상의 결합된 트랜잭션 식별자 및 하나 이상의 개별 트랜잭션 식별자를 저장하도록 구성되고, 상기 하나 이상의 결합된 트랜잭션 식별자 각각은 트랜잭션의 레코드의 저장을 최소화하도록 결합된 복수의 기록된 단조 증가하는 트랜잭션 식별자(plurality of recorded monotonically increasing transaction identifier)를 포함함 - ;

상기 트랜잭션 멱등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하지 않았다는 것을 결정하는 것에 응답하여, 상기 블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 블록체인 상의 후보 블록 내에 상기 타겟 트랜잭션을 기록하는(recording) 단계;

상기 블록체인 상의 후보 블록 내에 상기 타겟 트랜잭션을 기록하는 것에 응답하여, 블록체인에 의해 지원되는 합의 알고리즘을 사용하여 상기 후보 블록 내의 상기 타겟 트랜잭션에 합의 프로세싱을 수행하는 단계;

상기 후보 블록이 상기 합의 프로세싱을 통과하는 것에 응답하여, 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 멱등 레코드를 생성하는 단계; 및

상기 블록체인 상의 상기 트랜잭션 멱등 테이블에, 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 멱등 레코드를 삽입하는 단계 - 상기 트랜잭션 멱등 테이블에 저장된 상기 트랜잭션 멱등 레코드는 상기 트랜잭션 멱등 레코드에 대응하는 상기 타겟 트랜잭션이 상기 블록체인의 분산형 데이터베이스에 성공적으로 기록된 것을 나타냄 -

를 포함하는, 컴퓨터 구현 방법.

**청구항 2**

제1항에 있어서,

상기 트랜잭션 멱등 테이블에 상기 타겟 트랜잭션의 고유 식별자가 삽입된 후에, 상기 트랜잭션 멱등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는 것을 결정하는 단계;

상기 트랜잭션 멱등 테이블에 상기 타겟 트랜잭션의 고유 식별자가 삽입된 후에, 상기 트랜잭션 멱등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는 것을 결정하는 것에 응답하여, 인터벌에 기초하여 상기 트랜잭션 멱등 테이블 내에 연속적인 값을 갖는 상기 복수의 단조 증가하는 트랜잭션 식별자를

기록하는 단계; 및

상기 타겟 트랜잭션의 고유 식별자가 상기 트랜잭션 먹등 테이블에 삽입된 후에, 상기 트랜잭션 먹등 테이블이 연속적인 값을 갖는 상기 복수의 단조 증가하는 트랜잭션 식별자를 포함하지 않는다는 것을 결정하는 것에 응답하여, 불연속적인 값에 기초하여 상기 트랜잭션 먹등 테이블에 상기 타겟 트랜잭션의 트랜잭션 식별자를 기록하는 단계

를 더 포함하는, 컴퓨터 구현 방법.

**청구항 3**

제1항에 있어서,

상기 타겟 트랜잭션은, 상기 타겟 트랜잭션이 트랜잭션 유효 기간 내의 유효한 트랜잭션이라는 것을 결정하는 것을 돕기 위한 타임스탬프에 기초한 기준 시간 파라미터(reference time parameter)를 더 포함하는 것인, 컴퓨터 구현 방법.

**청구항 4**

제3항에 있어서,

상기 트랜잭션 먹등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 먹등 레코드를 저장한다는 것을 결정하기 전에, 상기 기준 시간 파라미터에 기초하여 상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 단계; 및

상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 것에 응답하여, 상기 트랜잭션 먹등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 먹등 레코드를 저장한다는 것을 결정하는 단계

를 더 포함하는, 컴퓨터 구현 방법.

**청구항 5**

제4항에 있어서,

상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 단계는,

상기 기준 시간 파라미터로부터 상기 타임스탬프의 시간 윈도우 내에서 상기 타겟 트랜잭션이 발생하는 것을 결정하는 단계를 포함하고,

상기 시간 윈도우는, 상기 블록체인 상의 블록체인 트랜잭션에 대한 지속 기간 및 상기 블록체인 상의 디바이스에 대한 클록 오프셋 시간: 중 적어도 하나에 의해 특성 묘사되는 것인, 컴퓨터 구현 방법.

**청구항 6**

동작을 수행하기 위해 컴퓨터 시스템에 의해 실행 가능한 하나 이상의 명령어가 저장된 비밀시적 컴퓨터 관독 가능 매체로서, 상기 동작은,

블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 블록체인 내의 제2 멤버 노드 디바이스가 개시한 타겟 트랜잭션 - 상기 타겟 트랜잭션은 상기 타겟 트랜잭션의 고유 식별자 및 로직 클럭의 생성 타임스탬프를 규정하는 상기 블록체인 내의 후보 블록의 블록 높이를 포함함 - 을 수신하는 동작;

상기 타겟 트랜잭션의 고유 식별자에 기초하여, 상기 타겟 트랜잭션이 트랜잭션 유효 기간 내에 수행되도록 승인된 것을 결정함으로써, 상기 타겟 트랜잭션이 유효하다는 것을 결정하는 동작 - 상기 트랜잭션 유효 기간은 연체된 트랜잭션을 유효한 트랜잭션과 구별할 수 있도록 하며 상기 후보 블록의 블록 높이와 임계값 사이의 차이에 의해 특성 묘사됨(characterized) - ;

상기 타겟 트랜잭션의 생성 타임스탬프가 상기 블록체인 내의 블록의 다른 생성 타임스탬프에 비해 단조 증가하고 있음을 검증함으로써 상기 후보 블록이 합법적인 블록이라는 것을 결정하는 동작;

상기 타겟 트랜잭션이 유효하고 상기 후보 블록이 합법적인 블록이라는 것을 결정하는 것에 응답하여, 상기 블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 타겟 트랜잭션의 고유 식별자에 기초하여 트랜잭션 먹등 테

이블(transaction idempotent table)로부터 누락된 트랜잭션 멱등 레코드를 결정하기 위해 상기 블록체인 상의 상기 트랜잭션 멱등 테이블을 조회하는(querying) 동작 - 상기 트랜잭션 멱등 테이블은 상기 블록체인 내의 복수의 멤버 노드 디바이스 사이에 설정된(established) 합의 메커니즘을 사용함으로써 상기 블록체인 내의 복수의 멤버 노드 디바이스에 의해 공동으로 유지되고, 하나 이상의 결합된 트랜잭션 식별자 및 하나 이상의 개별 트랜잭션 식별자를 저장하도록 구성되고, 상기 하나 이상의 결합된 트랜잭션 식별자 각각은 트랜잭션의 레코드의 저장을 최소화하도록 결합된 복수의 기록된 단조 증가하는 트랜잭션 식별자(plurality of recorded monotonically increasing transaction identifier)를 포함함 - ;

상기 트랜잭션 멱등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하지 않았다는 것을 결정하는 것에 응답하여, 상기 블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 블록체인 상의 후보 블록 내에 상기 타겟 트랜잭션을 기록하는(recording) 동작;

상기 블록체인 상의 후보 블록 내에 상기 타겟 트랜잭션을 기록하는 것에 응답하여, 블록체인에 의해 지원되는 합의 알고리즘을 사용하여 상기 후보 블록 내의 상기 타겟 트랜잭션에 합의 프로세싱을 수행하는 동작;

상기 후보 블록이 상기 합의 프로세싱을 통과하는 것에 응답하여, 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 멱등 레코드를 생성하는 동작; 및

상기 블록체인 상의 상기 트랜잭션 멱등 테이블에, 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 멱등 레코드를 삽입하는 동작 - 상기 트랜잭션 멱등 테이블에 저장된 상기 트랜잭션 멱등 레코드는 상기 트랜잭션 멱등 레코드에 대응하는 상기 타겟 트랜잭션이 상기 블록체인의 분산형 데이터베이스에 성공적으로 기록된 것을 나타냄 -

을 포함하는 것인, 비밀시적 컴퓨터 판독 가능 매체.

**청구항 7**

제6항에 있어서, 상기 동작은,

상기 트랜잭션 멱등 테이블에 상기 타겟 트랜잭션의 고유 식별자가 삽입된 후에, 상기 트랜잭션 멱등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는 것을 결정하는 동작;

상기 트랜잭션 멱등 테이블에 상기 타겟 트랜잭션의 고유 식별자가 삽입된 후에, 상기 트랜잭션 멱등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는 것을 결정하는 것에 응답하여, 인터벌에 기초하여 상기 트랜잭션 멱등 테이블 내에 연속적인 값을 갖는 상기 복수의 단조 증가하는 트랜잭션 식별자를 기록하는 동작; 및

상기 타겟 트랜잭션의 고유 식별자가 상기 트랜잭션 멱등 테이블에 삽입된 후에, 상기 트랜잭션 멱등 테이블이 연속적인 값을 갖는 상기 복수의 단조 증가하는 트랜잭션 식별자를 포함하지 않는다는 것을 결정하는 것에 응답하여, 불연속적인 값에 기초하여 상기 트랜잭션 멱등 테이블에 상기 타겟 트랜잭션의 트랜잭션 식별자를 기록하는 동작

을 더 포함하는 것인, 비밀시적 컴퓨터 판독 가능 매체.

**청구항 8**

제6항에 있어서,

상기 타겟 트랜잭션은, 상기 타겟 트랜잭션이 트랜잭션 유효 기간 내의 유효한 트랜잭션이라는 것을 결정하는 것을 돕기 위한 타임스탬프에 기초한 기준 시간 파라미터(reference time parameter)를 더 포함하는 것인, 비밀시적 컴퓨터 판독 가능 매체.

**청구항 9**

제8항에 있어서, 상기 동작은,

상기 트랜잭션 멱등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 멱등 레코드를 저장한다는 것을 결정하는 것을 조회하기 전에, 상기 기준 시간 파라미터에 기초하여 상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 동작; 및

상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 것에 응답하여, 상기 트랜잭션 멱등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 멱등 레코드를 저장한다는 것을 결정하는 동작

을 더 포함하는 것인, 비밀시적 컴퓨터 판독 가능 매체.

**청구항 10**

제9항에 있어서,

상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 동작은,

상기 기준 시간 파라미터로부터 상기 타임스탬프의 시간 윈도우 내에서 상기 타겟 트랜잭션이 발생하는 것을 결정하는 동작을 포함하고,

상기 시간 윈도우는, 상기 블록체인 상의 블록체인 트랜잭션에 대한 지속 기간 및 상기 블록체인 상의 디바이스에 대한 클록 오프셋 시간: 중 적어도 하나에 의해 특성 묘사되는 것인, 비밀시적 컴퓨터 판독 가능 매체.

**청구항 11**

컴퓨터 구현 시스템(computer-implemented system)으로서,

하나 이상의 컴퓨터; 및

상기 하나 이상의 컴퓨터와 상호동작 가능하게 커플링되고, 하나 이상의 명령어가 저장된 유형의(tangible) 비밀시적 기계 판독 가능 매체를 갖는 하나 이상의 컴퓨터 메모리

를 포함하고,

상기 하나 이상의 명령어는, 상기 하나 이상의 컴퓨터에 의한 실행시, 하나 이상의 동작을 수행하며, 상기 하나 이상의 동작은,

블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 블록체인 내의 제2 멤버 노드 디바이스가 개시한 타겟 트랜잭션 - 상기 타겟 트랜잭션은 상기 타겟 트랜잭션의 고유 식별자 및 로직 클럭의 생성 타임스탬프를 규정하는 상기 블록체인 내의 후보 블록의 블록 높이를 포함함 - 을 수신하는 동작;

상기 타겟 트랜잭션의 고유 식별자에 기초하여, 상기 타겟 트랜잭션이 트랜잭션 유효 기간 내에 수행되도록 승인된 것을 결정함으로써, 상기 타겟 트랜잭션이 유효하다는 것을 결정하는 동작 - 상기 트랜잭션 유효 기간은 연체된 트랜잭션을 유효한 트랜잭션과 구별할 수 있도록 하며 상기 후보 블록의 블록 높이와 임계값 사이의 차이에 의해 특성 묘사됨(characterized) - ;

상기 타겟 트랜잭션의 생성 타임스탬프가 상기 블록체인 내의 블록의 다른 생성 타임스탬프에 비해 단조 증가하고 있음을 검증함으로써 상기 후보 블록이 합법적인 블록이라는 것을 결정하는 동작;

상기 타겟 트랜잭션이 유효하고 상기 후보 블록이 합법적인 블록이라는 것을 결정하는 것에 응답하여, 상기 블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 타겟 트랜잭션의 고유 식별자에 기초하여 트랜잭션 멱등 테이블(transaction idempotent table)로부터 누락된 트랜잭션 멱등 레코드를 결정하기 위해 상기 블록체인 상의 상기 트랜잭션 멱등 테이블을 조회하는(querying) 동작 - 상기 트랜잭션 멱등 테이블은 상기 블록체인 내의 복수의 멤버 노드 디바이스 사이에 설정된(established) 합의 메커니즘을 사용함으로써 상기 블록체인 내의 복수의 멤버 노드 디바이스에 의해 공동으로 유지되고, 하나 이상의 결합된 트랜잭션 식별자 및 하나 이상의 개별 트랜잭션 식별자를 저장하도록 구성되고, 상기 하나 이상의 결합된 트랜잭션 식별자 각각은 트랜잭션의 레코드의 저장을 최소화하도록 결합된 복수의 기록된 단조 증가하는 트랜잭션 식별자(plurality of recorded monotonically increasing transaction identifier)를 포함함 - ;

상기 트랜잭션 멱등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하지 않았다는 것을 결정하는 것에 응답하여, 상기 블록체인 내의 제1 멤버 노드 디바이스에 의해, 상기 블록체인 상의 후보 블록 내에 상기 타겟 트랜잭션을 기록하는(recording) 동작;

상기 블록체인 상의 후보 블록 내에 상기 타겟 트랜잭션을 기록하는 것에 응답하여, 블록체인에 의해 지원되는 합의 알고리즘을 사용하여 상기 후보 블록 내의 상기 타겟 트랜잭션에 합의 프로세싱을 수행하는 동작;

상기 후보 블록이 상기 합의 프로세싱을 통과하는 것에 응답하여, 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 맥등 레코드를 생성하는 동작; 및

상기 블록체인 상의 상기 트랜잭션 맥등 테이블에, 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 맥등 레코드를 삽입하는 동작 - 상기 트랜잭션 맥등 테이블에 저장된 상기 트랜잭션 맥등 레코드는 상기 트랜잭션 맥등 레코드에 대응하는 상기 타겟 트랜잭션이 상기 블록체인의 분산형 데이터베이스에 성공적으로 기록된 것을 나타냄 -

을 포함하는 것인, 컴퓨터 구현 시스템.

**청구항 12**

제11항에 있어서, 상기 하나 이상의 동작은,

상기 트랜잭션 맥등 테이블에 상기 타겟 트랜잭션의 고유 식별자가 삽입된 후에, 상기 트랜잭션 맥등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는 것을 결정하는 동작;

상기 트랜잭션 맥등 테이블에 상기 타겟 트랜잭션의 고유 식별자가 삽입된 후에, 상기 트랜잭션 맥등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는 것을 결정하는 것에 응답하여, 인터벌에 기초하여 상기 트랜잭션 맥등 테이블 내에 연속적인 값을 갖는 상기 복수의 단조 증가하는 트랜잭션 식별자를 기록하는 동작; 및

상기 타겟 트랜잭션의 고유 식별자가 상기 트랜잭션 맥등 테이블에 삽입된 후에, 상기 트랜잭션 맥등 테이블이 연속적인 값을 갖는 상기 복수의 단조 증가하는 트랜잭션 식별자를 포함하지 않는다는 것을 결정하는 것에 응답하여, 불연속적인 값에 기초하여 상기 트랜잭션 맥등 테이블에 상기 타겟 트랜잭션의 트랜잭션 식별자를 기록하는 동작

을 더 포함하는 것인, 컴퓨터 구현 시스템.

**청구항 13**

제11항에 있어서,

상기 타겟 트랜잭션은, 상기 타겟 트랜잭션이 트랜잭션 유효 기간 내의 유효한 트랜잭션이라는 것을 결정하는 것을 돕기 위한 타임스탬프에 기초한 기준 시간 파라미터(reference time parameter)를 더 포함하는 것인, 컴퓨터 구현 시스템.

**청구항 14**

제13항에 있어서, 상기 하나 이상의 동작은,

상기 트랜잭션 맥등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 맥등 레코드를 저장한다는 것을 결정하기 전에, 상기 기준 시간 파라미터에 기초하여 상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 동작; 및

상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 것에 응답하여, 상기 트랜잭션 맥등 테이블이 상기 타겟 트랜잭션의 고유 식별자에 대응하는 상기 트랜잭션 맥등 레코드를 저장한다는 것을 결정하는 동작

을 더 포함하는 것인, 컴퓨터 구현 시스템.

**청구항 15**

제14항에 있어서,

상기 타겟 트랜잭션이 상기 트랜잭션 유효 기간 내의 상기 유효 트랜잭션이라는 것을 결정하는 동작은,

상기 기준 시간 파라미터로부터 상기 타임스탬프의 시간 윈도우 내에서 상기 타겟 트랜잭션이 발생하는 것을 결정하는 동작을 포함하고,

상기 시간 윈도우는, 상기 블록체인의 블록체인 트랜잭션에 대한 지속 기간 및 상기 블록체인의 디바이스

에 대한 클록 오프셋 시간: 중 적어도 하나에 의해 특성 묘사되는 것인, 컴퓨터 구현 시스템.

**발명의 설명**

**기술 분야**

[0001] [관련 출원에 대한 교차 참조] 본 출원은 2019년 5월 29일자로 출원된 중국 특허 출원 제 201810532710.7호에 대한 우선권을 주장하는데, 상기 중국 특허 출원은 참조에 의해 그 전체가 본원에 통합된다.

[0002] [기술 분야] 본 출원의 하나 이상의 구현에는 블록체인 기술의 분야에 관한 것으로, 특히 블록체인 기반 트랜잭션 프로세싱 방법 및 장치, 및 전자 디바이스에 관한 것이다.

**배경 기술**

[0003] 분산 원장 기술로 또한 칭해지는 블록체인 기술은, 몇몇 컴퓨팅 디바이스가 "어카운팅(accounting)"에 공동으로 참가하여 완전한 분산형 데이터베이스를 유지하는 새로운 기술이다. 블록체인 기술은 탈집중화(decentralization), 개방성, 및 투명성을 특징으로 한다. 각각의 컴퓨팅 디바이스는 데이터베이스에 데이터를 기록할 수 있고, 데이터는 컴퓨팅 디바이스 사이에서 빠르게 동기화될 수 있다. 따라서, 탈집중화된 시스템을 생성하기 위해 그리고 다양한 실행 프로그램을 자동 실행을 위한 블록체인의 분산형 데이터베이스에 기록하기 위해 블록체인 기술을 사용하는 것이 많은 분야에서 널리 적용되었다.

**발명의 내용**

[0004] 본 출원은 다음의 것을 포함하는 블록체인 기반 트랜잭션 프로세싱 방법을 제공한다: 블록체인 내의 멤버 노드 디바이스에 의해 게시되는 타겟 트랜잭션 - 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함함 - 을 수신하는 것; 미리 설정된 트랜잭션 멱등 테이블(idempotent table)이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하는지의 여부를 조회하는 것(querying); 및 트랜잭션 멱등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하지 않는 경우, 타겟 트랜잭션을 후보 블록에 기록하는 것.

[0005] 옵션 사항으로, 트랜잭션 멱등 테이블에서의 트랜잭션 멱등 레코드는, 트랜잭션 멱등 레코드에 대응하는 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었다는 것을 나타낸다.

[0006] 옵션 사항으로, 방법은 다음의 것을 더 포함한다: 타겟 트랜잭션이 후보 블록에 기록되고, 후보 블록이 블록체인의 분산형 데이터베이스에 성공적으로 저장되도록 합의(consensus)를 통과한 경우, 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 생성하는 것, 및 타겟 트랜잭션의 고유 식별자에 대응하는 생성된 트랜잭션 멱등 레코드를 트랜잭션 멱등 테이블에 삽입하는 것.

[0007] 옵션 사항으로, 트랜잭션 멱등 테이블에서의 트랜잭션 멱등 레코드는 트랜잭션의 고유 식별자이고, 블록체인 내의 멤버 노드 디바이스에 의해 게시되는 트랜잭션의 고유 식별자는 단조 증가하는 트랜잭션 식별자(monotonically increasing transaction identifier)이며; 방법은 다음의 것을 더 포함한다: 트랜잭션의 고유 식별자가 트랜잭션 멱등 테이블에 삽입된 이후, 트랜잭션 멱등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는지의 여부를 결정하는 것; 및 만약 그렇다면, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 인터벌의 형태로 트랜잭션 멱등 테이블에 기록하는 것; 또는 만약 그렇지 않다면, 트랜잭션의 트랜잭션 식별자를 이산 값의 형태로 트랜잭션 멱등 테이블에 기록하는 것.

[0008] 옵션 사항으로, 타겟 트랜잭션은 기준 시간 파라미터(reference time parameter)를 더 포함하고, 기준 시간 파라미터는, 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하기 위해 사용되고; 그리고 미리 설정된 트랜잭션 멱등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하는지의 여부를 조회하기 이전에, 방법은 다음의 것을 더 포함한다: 기준 시간 파라미터에 기초하여 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하는 것; 및 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션이라고 결정되는 경우, 미리 설정된 트랜잭션 멱등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 멱등 레코드를 저장하는지의 여부를 추가로 조회하는 것.

[0009] 옵션 사항으로, 블록체인은 컨소시엄 블록체인(consortium blockchain)이다.

- [0010] 본 출원은 또한 다음의 것을 포함하는 블록체인 기반 트랜잭션 프로세싱 장치를 제공한다: 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 타겟 트랜잭션 - 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함함 - 을 수신하도록 구성되는 수신 모듈; 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 조회하도록 구성되는 조회 모듈; 및 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하지 않는 경우, 타겟 트랜잭션을 후보 블록에 기록하도록 구성되는 기록 모듈.
- [0011] 옵션 사항으로, 트랜잭션 먹등 테이블에서의 트랜잭션 먹등 레코드는, 트랜잭션 먹등 레코드에 대응하는 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었다는 것을 나타낸다.
- [0012] 옵션 사항으로, 기록 모듈은 또한: 타겟 트랜잭션이 후보 블록에 기록되고, 후보 블록이 블록체인의 분산형 데이터베이스에 성공적으로 저장되도록 합의를 통과한 경우, 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 생성하도록, 그리고 타겟 트랜잭션의 고유 식별자에 대응하는 생성된 트랜잭션 먹등 레코드를 트랜잭션 먹등 테이블에 삽입하도록 구성된다.
- [0013] 옵션 사항으로, 트랜잭션 먹등 테이블에서의 트랜잭션 먹등 레코드는 트랜잭션의 고유 식별자이고, 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 트랜잭션의 고유 식별자는 단조 증가하는 트랜잭션 식별자이며; 기록 모듈은 또한, 트랜잭션의 고유 식별자가 트랜잭션 먹등 테이블에 삽입된 이후, 트랜잭션 먹등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는지의 여부를 결정하도록; 그리고 만약 그렇다면, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 인터벌의 형태로 트랜잭션 먹등 테이블에 기록하도록; 또는 만약 그렇지 않다면, 트랜잭션의 트랜잭션 식별자를 이산 값의 형태로 트랜잭션 먹등 테이블에 기록하도록 구성된다.
- [0014] 옵션 사항으로, 타겟 트랜잭션은 기준 시간 파라미터를 더 포함하고, 기준 시간 파라미터는, 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하기 위해 사용되고; 장치는 다음의 것: 결정 모듈을 더 포함하되, 결정 모듈은; 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부가 조회되기 이전에, 기준 시간 파라미터에 기초하여 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하도록; 그리고 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션이라고 결정되는 경우, 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 추가로 조회하도록 구성된다.
- [0015] 옵션 사항으로, 블록체인은 컨소시엄 블록체인이다.
- [0016] 본 출원은 또한 전자 디바이스를 제공하는데, 전자 디바이스는 다음의 것: 프로세서; 및 머신 실행 가능 명령어를 저장하도록 구성되는 메모리를 을 포함하되, 메모리에 저장되며 블록체인 기반 트랜잭션 프로세싱의 제어 로직에 대응하는 머신 실행 가능 명령어를 판독 및 실행하는 것에 의해, 프로세서는, 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 타겟 트랜잭션 - 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함함 - 을 수신하도록; 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 조회하도록; 그리고 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하지 않는 경우, 타겟 트랜잭션을 후보 블록에 기록하도록 구성된다.

**도면의 간단한 설명**

- [0017] 도 1은, 예시적인 구현예에 따른, 블록체인 기반 트랜잭션 프로세싱 방법을 나타내는 플로우차트이다;
- 도 2는, 예시적인 구현예에 따른, 전자 디바이스를 예시하는 구조도이다;
- 도 3은, 예시적인 구현예에 따른, 블록체인 기반 트랜잭션 프로세싱 장치를 예시하는 블록도이다; 그리고
- 도 4는, 본 개시의 구현예에 따른, 블록체인 기반 트랜잭션을 프로세싱하기 위한 컴퓨터 구현 방법의 예를 예시하는 플로우차트이다.

**발명을 실시하기 위한 구체적인 내용**

- [0018] 본 출원은, 블록체인에서 수신된 트랜잭션에 대해 먹등 프로세싱을 수행하기 위해, 생성된 트랜잭션 먹등 테이블이 사용되는 기술적 솔루션을 제공하고, 그 결과, 비합법적인 노드는 인터셉트된 기한이 지난 트랜잭션을 사용하는 것에 의해 재전송 공격(replay attack)을 개시할 수 없다.

- [0019] 구현 동안, 블록체인에서 어카운팅 노드로서 역할을 할 수 있는 노드 디바이스는 트랜잭션 맥등 테이블을 공동으로 유지할 수 있다. 예를 들면, 어카운팅 노드 역할을 하는 노드 디바이스는 블록체인에서의 현존하는 합의 메커니즘을 사용하는 것에 의해 합의 트랜잭션 맥등 테이블을 공동으로 유지할 수 있다.
- [0020] 트랜잭션 맥등 테이블에서의 트랜잭션 맥등 레코드는, 트랜잭션 맥등 레코드에 대응하는 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었다는 것을 나타낸다.
- [0021] 유저가 클라이언트 측 상에서 트랜잭션을 생성할 때, 클라이언트 측은 트랜잭션에 대한 고유 식별자를 생성하고 고유 식별자를 트랜잭션에 추가할 수 있고, 그 다음, 클라이언트 측에 연결되는 노드 디바이스가 블록체인에서 트랜잭션을 발행한다(publish).
- [0022] 블록체인 내의 다른 노드 디바이스가 그 트랜잭션을 수신하고 트랜잭션이 유효하다는 것을 검증한 이후, 노드 디바이스는, 트랜잭션 맥등 테이블이 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장하는지의 여부를 결정하기 위해 트랜잭션 맥등 테이블에게 추가로 조회할 수 있다.
- [0023] 트랜잭션 맥등 테이블이 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장하지 않는 경우, 그것은, 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되지 않았다는 것을 나타낸다. 이 경우, 트랜잭션은 후보 블록에 기록될 수 있다. 반대로, 트랜잭션 맥등 테이블이 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장하는 경우, 그것은, 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었으며, 블록체인에서 프로세싱되고 실행된 트랜잭션이라는 것을 나타낸다. 이 경우, 트랜잭션은 프로세싱되지 않고 바로 폐기될 수 있다.
- [0024] 이전의 기술적 솔루션에 따르면, 트랜잭션은, 트랜잭션에 관련되는 트랜잭션 맥등 레코드가 트랜잭션 맥등 테이블에 저장되어 있는 경우에만 유효 트랜잭션으로서 후보 블록에 기록될 수 있다. 그와 같이, 블록체인 내의 비합법적인 노드 디바이스는, 인터셉트된 기한이 지난 트랜잭션을 사용하는 것에 의해 블록체인에서 재전송 공격을 개시할 수 없고, 그에 의해, 블록체인의 트랜잭션 보안 레벨을 증가시킨다.
- [0025] 다음은 특정한 적용 시나리오에 기초한 특정한 구현예를 사용하는 것에 의해 본 명세서를 설명한다.
- [0026] 도 1은, 본 출원의 구현예에 따른 블록체인 기반 트랜잭션 프로세싱 방법을 도시한다. 방법은 블록체인의 임의의 노드 디바이스에 적용되며, 다음의 단계를 포함한다:
- [0027] 단계(102): 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 타겟 트랜잭션 - 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함함 - 을 수신함.
- [0028] 단계(104): 미리 설정된 트랜잭션 맥등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장하는지의 여부를 조회함.
- [0029] 단계(106): 트랜잭션 맥등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장하지 않는 경우, 타겟 트랜잭션을 후보 블록에 기록함.
- [0030] 본 출원에서 설명되는 블록체인은, 프라이빗 블록체인, 퍼블릭 블록체인, 컨소시엄 블록체인, 등등을 포함할 수 있으며, 구현예는 본 출원에서 제한되지 않는다.
- [0031] 예를 들면, 한 시나리오에서, 블록체인은 다음의 멤버 디바이스: 제3자 지불 플랫폼(third-party payment platform)의 서버, 국내 은행 서버, 해외 은행 서버, 및 몇몇 유저 노드 디바이스를 포함하는 컨소시엄 블록체인일 수 있다. 컨소시엄 블록체인 오퍼레이터는 컨소시엄 블록체인에 따라 국가간 양도(cross-border transfer) 및 자산 양도(asset transfer)와 같은 컨소시엄 블록체인 기반 온라인 서비스를 배치할 수 있다.
- [0032] 본 출원에서 설명되는 트랜잭션(양도)은, 블록체인의 클라이언트 측의 유저에 의해 생성되며, 최종적으로 블록체인의 분산형 데이터베이스에 발행될 필요가 있다.
- [0033] 블록체인에서의 트랜잭션은 좁은 의미의 트랜잭션 및 넓은 의미의 트랜잭션을 포함한다. 좁은 의미의 트랜잭션은 블록체인에서 유저에 의해 발행되는 가치 양도(value transfer)이다. 예를 들면, 종래의 비트 코인 블록체인 네트워크에서, 트랜잭션은 블록체인에서 유저에 의해 개시되는 양도일 수 있다. 넓은 의미의 트랜잭션은 블록체인에서 유저에 의해 발행되는 서비스 지향 서비스 데이터이다. 예를 들면, 오퍼레이터는 실제 서비스 요건에 기초하여 컨소시엄 블록체인을 생성하고, 컨소시엄 블록체인에 따른 가치 양도에 관련되지 않는 어떤 다른 타입의 온라인 서비스(예를 들면, 임차권(tenancy) 서비스, 차량 예약(vehicle scheduling) 서비스, 보험 청구 서비스, 신용 서비스 및 의료 서비스)를 배치할 수 있다. 그러한 컨소시엄 블록체인에서, 트랜잭션은 컨소시엄 블록체인

에서 유저에 의해 발행되는 서비스 지향 서비스 메시지 또는 메시지 요청일 수 있다.

- [0034] 타겟 트랜잭션은, 블록체인에서 어카운팅 노드로서 역할을 하는 노드 디바이스가 패킹하여(pack) 후보 블록에 포함시킬 필요가 있는 후보 트랜잭션이다. 후보 트랜잭션은, 다른 멤버 노드 디바이스에 의해 발행되고 검증된 수집된 트랜잭션으로부터 노드 디바이스에 의해 선택된다.
- [0035] 본 출원에서, 클라이언트 측의 유저에 의해 생성되는 트랜잭션은 유저에 의해 유지되는 개인 키에 기초하여 서명될 수 있고, 클라이언트 측에 연결되는 노드 디바이스에 의해 블록체인의 P2P 네트워크에서 브로드캐스팅된다. 어카운팅 노드로서 역할을 하는 노드 디바이스는 다른 노드 디바이스에 의해 브로드캐스팅되는 트랜잭션을 수집하고, 수집된 트랜잭션을 확인 응답되지 않은 트랜잭션(unacknowledged transaction)으로서 로컬 트랜잭션 풀(메모리 풀로 또한 칭해짐)에 저장할 수 있다.
- [0036] 게다가, 어카운팅 노드로서 역할을 하는 노드 디바이스는 현재의 어카운팅 기간에 후보 블록을 생성할 수 있고, 트랜잭션 풀 내의 트랜잭션에 대한 유효성 검증을 수행할 수 있고, 그 다음, 검증된 트랜잭션을 후보 트랜잭션으로서 생성된 후보 블록에 기록할 수 있다.
- [0037] 실제 애플리케이션에서, 트랜잭션 풀 내의 트랜잭션에 대한 검증을 수행하는 것은, 트랜잭션의 발행자의 신원(identity)에 대한 검증 및 트랜잭션 콘텐츠에 대한 검증을 수행하는 것을 포함할 수 있다. 트랜잭션 콘텐츠에 대한 검증은 트랜잭션 콘텐츠에 대한 무결성 검증을 더 포함할 수 있다.
- [0038] 구현 동안, 서명되는 경우, 트랜잭션은 콘텐츠 다이제스트(content digest)(예를 들면, 해시 값)를 획득하기 위해 일반적으로 계산될 수 있고, 그 다음, 콘텐츠 다이제스트는 유지된 개인 키에 기초하여 암호화되어 디지털 서명을 획득한다. 서명된 트랜잭션을 수신한 이후, 어카운팅 노드로서 역할을 하는 노드 디바이스는 트랜잭션에 서명하기 위해 사용되는 개인 키에 기초하여 디지털 서명을 암호 해제할 수 있다. 암호 해제가 성공하면, 그것은, 트랜잭션의 발행자의 신원이 검증되고, 트랜잭션이 유저에 의해 발행되는 합법적인 트랜잭션이라는 것을 나타낸다.
- [0039] 그 다음, 어카운팅 노드로서 역할을 하는 노드 디바이스는 또한, 트랜잭션을 재계산하여 콘텐츠 다이제스트를 획득하고, 재계산된 콘텐츠 다이제스트 및 디지털 서명을 암호 해제하는 것에 의해 획득되는 원래의 콘텐츠 다이제스트를 매칭시킬 수 있다. 두 개의 콘텐츠 다이제스트가 서로 매치하면, 그것은, 트랜잭션 콘텐츠에 대한 무결성 검증이 통과되었고, 트랜잭션의 트랜잭션 콘텐츠가 트랜잭션 송신 프로세스에서 불법적으로 무단 변경되지 않았다는 것을 나타낸다.
- [0040] 본 명세서에서, 트랜잭션 풀 내의 트랜잭션의 발행자의 신원에 대한 검증 및 트랜잭션 콘텐츠에 대한 검증에 더하여, 트랜잭션에 포함되는 기준 시간 파라미터에 기초하여, 트랜잭션 풀 내의 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부가 추가로 검증될 수 있다.
- [0041] 트랜잭션 유효 기간은, 블록체인에서 발행되는 트랜잭션에 대해 블록체인의 오퍼레이터에 의해 설정되는 유효 기간이다. 유효 기간 이내의 트랜잭션은, 합법적인 트랜잭션으로서 후보 블록에 추가될 수 있는 유효 트랜잭션으로 간주된다. 반대로, 유효 기간을 넘어서게 되는 트랜잭션은, 후보 블록에 추가될 수 없는 무효한 트랜잭션으로 간주된다.
- [0042] 트랜잭션 유효 기간은, 현재의 어카운팅 기간에 생성되는 후보 블록의 생성 시간을 기준으로 사용하는 것에 의해 블록체인에서 어카운팅 노드 디바이스에 의해 설정되는 시간 인터벌일 수 있다. 예를 들면, 트랜잭션 유효 기간은, 후보 블록의 생성 시간 이전의 시간의 기간일 수 있거나, 또는 후보 블록의 생성 시간 이후의 시간의 기간일 수 있다. 블록체인 내의 다른 노드 디바이스에 의해 발행되는 많은 트랜잭션을 수집할 때, 어카운팅 노드는, 트랜잭션 유효 기간을 사용하는 것에 의해, 생성된 후보 블록에 합법적인 트랜잭션으로서 어떤 트랜잭션이 추가될 수 있는지를 결정할 수 있다.
- [0043] 기준 시간 파라미터는, 트랜잭션에 추가되며 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하기 위해 사용되는 시간 파라미터일 수 있다. 수집된 트랜잭션에 대한 검증을 수행할 때, 블록체인 내의 어카운팅 노드는, 트랜잭션에 포함되는 기준 시간 파라미터에 의해 나타내어지는 시간에 기초하여 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정할 수 있다.
- [0044] 기준 시간 파라미터는 물리적 클록일 수 있거나, 또는 논리적 클록일 수 있다.
- [0045] 물리적 클록은, 시스템 또는 제3자 클록 서버로부터 관독되는 시스템 타임스탬프이다. 논리적 클록은 논리적 타임스탬프이다. 분산형 시스템에서, 이벤트(예를 들면, 트랜잭션) 발생 순서를 나타낼 수 있는 임의의 자체 증가

하는 값이 논리적 클록으로서 사용될 수 있다.

- [0046] 한 구현예에서, 예를 들면, 기준 시간 파라미터는 물리적 클록이다. 기준 시간 파라미터는 트랜잭션에 추가되는 기준 타임스탬프일 수 있다. 상응하여, 이 경우, 트랜잭션 유효 기간은 후보 블록의 생성 시간에 대응하는 생성 타임스탬프와 제1 임계치 사이의 차이(제1 값) 및 블록의 생성 타임스탬프와 제2 임계치의 합(제2 값)에 의해 형성되는 수치 인터벌일 수 있다.
- [0047] 예를 들면, 후보 블록의 생성 타임스탬프는  $B_{ts}$ 로 표기되고, 제1 임계치는  $K1$ 로 표기되고, 제2 임계치는  $K2$ 로 표기된다. 이 경우, 트랜잭션 유효 기간은 수치 인터벌  $[B_{ts} - K1, B_{ts} + K2]$ 에 의해 표현될 수 있다.
- [0048] 그들 중, 제1 임계치는 트랜잭션 유효 기간의 설정 동안 예약되는 트랜잭션 유효 지속 기간을 나타낸다. 제2 임계치는, 트랜잭션을 발행하는 노드 디바이스의 시스템 타임스탬프와 후보 블록을 생성하는 노드 디바이스의 시스템 타임스탬프 사이의 클록 오프셋을 나타낸다. 실제 애플리케이션에서, 블록체인 네트워크에서 허용될 수 있는 클록 오프셋은 일반적으로 상대적으로 작다. 따라서, 트랜잭션 유효 기간의 설정 동안, 제2 임계치는 크기의 순서에서 제1 임계치보다 더 작은 임계치로 설정될 수 있다.
- [0049] 예를 들면, 제1 임계치는 5 일로 설정될 수 있고, 제2 임계치는 5 분으로 설정될 수 있다. 이 경우, 후보 블록의 생성 시간 이전 5일 이내에 발행되는 트랜잭션과 후보 블록의 생성 시간 이후 5 분 이내에 발행되는 트랜잭션 둘 모두는 트랜잭션 유효 기간 이내의 유효 트랜잭션이다.
- [0050] 기준 타임스탬프는, 사용자가 클라이언트 측 상에서 트랜잭션을 생성할 때 유저에 의해 수동으로 명시될 수 있거나, 또는 클라이언트 측 상에서 자동적으로 추가될 수 있다는 것을 주목할 가치가 있다.
- [0051] 예를 들면, 하나의 상황에서, 사용자가 클라이언트 측 상에서 트랜잭션을 생성할 때, 클라이언트 측은 시스템으로부터 트랜잭션의 생성 시간을 관독할 수 있고, 그 다음, 생성 시간에 대응하는 타임스탬프를, 기준 타임스탬프로서, 생성된 트랜잭션에 자동적으로 추가할 수 있다. 다른 상황에서, 유저는 필요에 따라 트랜잭션 유효 기간 이내의 시간을 명시할 수 있고, 그 다음, 그 시간에 대응하는 타임스탬프를, 기준 타임스탬프로서, 생성된 트랜잭션에 수동으로 추가할 수 있다.
- [0052] 확실히, 실제 적용에서, 트랜잭션 유효 기간의 설정 동안, 트랜잭션을 발행하는 노드 디바이스의 시스템 타임스탬프와 후보 블록을 생성하는 노드 디바이스의 시스템 타임스탬프 사이의 클록 오프셋은 고려되지 않을 수도 있다. 이 경우에, 트랜잭션 유효 기간은, 후보 블록의 생성 시간에 대응하는 생성 타임스탬프와 제1 임계치 사이의 차이(제1 값) 및 후보 블록의 생성 타임스탬프에 의해 형성되는 수치 인터벌일 수 있다.
- [0053] 예를 들면, 후보 블록의 생성 타임스탬프는  $B_{ts}$ 로 표기되고, 제1 임계치는  $K1$ 로 표기된다. 이 경우, 트랜잭션 유효 기간은 수치 인터벌  $[B_{ts} - K1, B_{ts}]$ 에 의해 표현될 수 있다.
- [0054] 다른 구현예에서, 예를 들면, 기준 시간 파라미터는 논리적 클록이다. 블록체인에 대응하는 P2P 네트워크에서, 블록체인에서의 블록의 블록 높이는 논리적 클록으로서 사용될 수 있다. 이 경우, 기준 시간 파라미터는 트랜잭션에 추가되는 기준 블록 높이일 수 있다. 트랜잭션 유효 기간은 블록체인에서의 후보 블록의 블록 높이 및 블록체인에서의 후보 블록의 블록 높이와 제3 임계치 사이의 차이(제3 값)에 의해 형성되는 수치 인터벌일 수 있다.
- [0055] 예를 들면, 블록체인에서의 후보 블록의 블록 높이는  $B_h$ 로 표기되고, 제3 임계치는  $K3$ 으로 표기된다. 이 경우, 트랜잭션 유효 기간은 수치 인터벌  $[B_h - K3, B_h]$ 에 의해 표현될 수 있다.
- [0056] 제1 임계치과 같이, 제3 임계치는 트랜잭션 유효 기간의 설정 동안 예약되는 트랜잭션 유효 지속 기간을 나타낸다. 블록 높이가 트랜잭션 유효 기간을 나타내기 위한 논리적 클록으로서 사용되는 경우, 트랜잭션을 발행하는 노드 디바이스의 시스템 타임스탬프와 후보 블록을 생성하는 노드 디바이스의 시스템 타임스탬프 사이의 클록 오프셋은 고려되지 않을 수도 있다. 따라서, 이전 표현의 우측 부분의 증가하는 인터벌과 클록 오프셋을 나타내는 임계치가 추가되지 않을 수도 있다.
- [0057] 기준 블록 높이는, 사용자가 클라이언트 측 상에서 트랜잭션을 생성할 때 유저에 의해 수동으로 명시될 수 있거나, 또는 클라이언트 측 상에서 자동적으로 추가될 수 있다는 것을 주목할 가치가 있다.
- [0058] 예를 들면, 하나의 상황에서, 사용자가 클라이언트 측 상에서 트랜잭션을 생성할 때, 클라이언트 측은 시스템으로부터 트랜잭션의 생성 시간을 관독할 수 있고, 그 다음, 생성 시간에 블록체인에서의 최대 블록 높이를 추가로

조회할 수 있고, 그 최대 블록 높이를, 생성된 트랜잭션에 자동적으로 추가할 수 있다. 다른 상황에서, 유저는 필요에 따라 트랜잭션 유효 기간 이내에 블록 높이를 명시할 수 있고, 그 다음, 블록 높이에 대응하는 값을, 기준 블록 높이로서, 생성된 트랜잭션에 수동으로 추가할 수 있다.

- [0059] 확실히, 실제 적용에서, 블록체인에서의 블록의 블록 높이에 추가하여, 트랜잭션 발생 순서를 설명하기 위해 사용될 수 있는 다른 타입의 증가하는 값이 논리적 클록으로서 사용될 수 있다. 구현예가 본 명세서에서 나열되지 않는다.
- [0060] 한 구현예에서, 기준 시간 파라미터가 트랜잭션에 추가되는 기준 타임스탬프이고  $T_{ts}$ 로 표기된다는 것을 가정하면, 트랜잭션 유효 기간은, 후보 블록의 생성 시간에 대응하는 생성 타임스탬프( $B_{ts}$ )와 제1 임계치( $K1$ ) 사이의 차이 및 후보 블록의 생성 타임스탬프( $B_{ts}$ )와 제2 임계치( $K2$ )의 합에 의해 형성되는 수치 인터벌 [ $B_{ts} - K1, B_{ts} + K2$ ]이다.
- [0061] 이 경우에, 어카운팅 노드로서 역할을 하는 노드 디바이스는, 먼저, 생성된 후보 블록의 생성 타임스탬프에 대해 단조 증가 체크를 수행하여, 생성된 후보 블록의 생성 타임스탬프( $B_{ts}$ )가 블록체인에서의 최신 블록의 생성 타임스탬프보다 더 큰지의 여부를 체크할 수 있다. 만약 그렇다면, 그것은, 블록체인에서의 블록의 생성 타임스탬프가 단조롭게 증가하고 있다는 특성을 후보 블록이 충족하고, 후보 블록이 합법적인 블록이라는 것을 나타낸다.
- [0062] 후보 블록이 단조 증가 체크를 통과한 이후, 어카운팅 노드로서 역할을 하는 노드 디바이스는 트랜잭션으로부터 타임스탬프( $T_{ts}$ )를 추가로 판독하고,  $B_{ts} - K1$  및  $B_{ts} + K2$ 로 판독되는 기준 타임스탬프( $T_{ts}$ )를 개별적으로 비교할 수 있다.  $T_{ts}$ 가  $B_{ts} - K1$ 보다 더 크고  $B_{ts} + K2$ 보다 더 작은 경우, 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션이라고 결정될 수 있다.
- [0063] 한 구현예에서, 기준 시간 파라미터가 트랜잭션에 추가되는 기준 블록 높이이고  $T_h$ 로 표기된다는 것을 가정하면, 트랜잭션 유효 기간은, 블록체인에서의 후보 블록의 블록 높이( $B_h$ )와 제3 임계치( $K3$ ) 사이의 차이 및 블록체인에서의 후보 블록의 블록 높이( $B_h$ )에 의해 형성되는 수치 인터벌 [ $B_h - K3, B_h$ ]이다.
- [0064] 이 경우, 어카운팅 노드로서 역할을 하는 노드 디바이스는, 먼저, 생성된 후보 블록의 블록 번호에 대한 단조 증가 체크를 수행하여, 생성된 후보 블록의 블록 수가 블록체인에서의 최신 블록의 블록 수보다 더 큰지의 여부를 체크할 수 있다. 만약 그렇다면, 그것은, 블록체인에서의 블록의 블록 수가 단조롭게 증가하고 있다는 특성을 후보 블록이 충족하고, 후보 블록이 합법적인 블록이라는 것을 나타낸다.
- [0065] 후보 블록이 단조 증가 체크를 통과한 이후, 어카운팅 노드로서 역할을 하는 노드 디바이스는 트랜잭션으로부터 기준 블록 높이( $T_h$ )를 추가로 판독하고,  $B_h - K3$  및  $B_h$ 로 판독되는 기준 블록 높이( $T_h$ )를 개별적으로 비교할 수 있다.  $T_h$ 가  $B_h - K3$ 보다 더 크고  $B_h$ 보다 더 작은 경우, 트랜잭션은 트랜잭션 유효 기간 이내의 유효 트랜잭션이라고 결정될 수 있다.
- [0066] 본 출원에서, 발행자의 신원에 대한 검증, 트랜잭션 콘텐츠에 대한 검증, 트랜잭션의 유효성 검증, 등등에서 성공하는 트랜잭션 풀 내의 트랜잭션은 후보 트랜잭션으로서 사용될 수 있고, 생성된 후보 블록에 패키징되어 포함될 수 있다.
- [0067] 예를 들면, 어카운팅 노드로서 역할을 하는 노드 디바이스는 유효성 검증에 성공하는 트랜잭션을 후보 블록에 추가할 수 있거나, 또는 규칙에 기초한(예를 들면, 트랜잭션 우선 순위에 기초한) 유효성 검증에서 성공하는 트랜잭션 중 일부를 선택할 수 있고, 그 트랜잭션을 후보 블록에 추가할 수 있다.
- [0068] 따라서, 트랜잭션 유효 기간 이내의 유효 트랜잭션만이 합법적인 트랜잭션으로서 후보 블록에 기록될 수 있다. 장기간의 시간 이전에 몇몇 기한이 지난 트랜잭션은 후속하는 트랜잭션 실행을 위한 후보 블록에 기록될 수 없다. 그와 같이, 블록체인에서의 비합법적인 노드 디바이스는, 인터셉트된 기한이 지난 트랜잭션을 장기간의 시간 이전에 사용하는 것에 의해 블록체인에서 재전송 공격을 개시할 수 없고, 그에 의해, 블록체인의 트랜잭션 보안 레벨을 증가시킨다.
- [0069] 본 명세서에서, 어카운팅 노드로서 역할을 하는 노드 디바이스의 트랜잭션 실행 환경은 다중 인스턴스 실행 환경일 수 있고, 다중 인스턴스 실행 환경에서, 동일한 트랜잭션은 상이한 인스턴스에 의해 반복적으로 제출될 수

있다. 따라서, 블록체인에서의 트랜잭션 실행 동안 멱등성(idempotence)이 발생할 수 있다. 멱등성은, 동일한 트랜잭션이 반복적으로 실행된 이후 사용자가 부정적인 영향을 받게 된다는 것을 의미한다.

- [0070] 예를 들면, 비트 코인 네트워크에서 "이중 지출" 문제가 통상적인 "멱등성" 문제이다. 유저의 개인 키를 사용하는 것에 의해 수행되는 서명 검증이 성공한 이후 비합법적인 트랜잭션 노드에 의해 양도 트랜잭션(transfer transaction)이 인터셉트된다는 것을 가정한다. 트랜잭션이 실행된 이후, 비합법적인 노드는 인터셉트된 트랜잭션에 기초하여 재전송 공격을 개시할 수 있고, 블록체인에서 트랜잭션을 반복적으로 실행하여, 동일한 자본으로 하여금 복수 회 양도되게 하고 유저에게 재정적 손실을 야기할 수 있다.
- [0071] 따라서, 다중 인스턴스 실행 환경에서 트랜잭션의 반복된 실행을 감소시키기 위해, 블록체인에서 어카운팅 노드로서 역할을 할 수 있는 노드 디바이스는 트랜잭션 멱등 테이블을 공동으로 유지할 수 있다.
- [0072] 예를 들면, 어카운팅 노드로서 역할을 하는 노드 디바이스는 블록체인에서 현존하는 합의 메커니즘을 사용하는 것에 의해 합의를 통과하는 트랜잭션 멱등 테이블을 공동으로 유지할 수 있다.
- [0073] 트랜잭션 멱등 테이블은, 트랜잭션 유효 기간 이내의 유효 트랜잭션에 기초하여 블록체인의 분산형 데이터베이스에 성공적으로 기록되는 저장 레코드(즉, 블록 레코드)에 대해 생성되는 인덱스 레코드 테이블이다. 트랜잭션 멱등 테이블은, 블록체인의 분산형 데이터베이스에 성공적으로 기록되는 유효 트랜잭션에 대응하는 트랜잭션 멱등 레코드를 저장하기 위해 사용된다.
- [0074] 구체적으로, 트랜잭션 멱등 테이블에 저장되는 트랜잭션 멱등 레코드는, 트랜잭션 멱등 레코드에 대응하는 트랜잭션이 후보 블록에 성공적으로 캡슐화되었고, 후보 블록이 합의를 통과하여, 블록체인에서의 최신 블록으로서, 블록체인의 분산형 데이터베이스(즉, 분산 원장)에 성공적으로 추가되었다는 것을 나타내기 위해 사용된다.
- [0075] 후보 블록에 유효 트랜잭션을 기록하기 이전에, 어카운팅 노드로서 역할을 하는 노드 디바이스는 트랜잭션 멱등 테이블에 기초하여 트랜잭션에 대해 멱등성 체크를 수행하여, 트랜잭션이 블록체인의 데이터베이스에 성공적으로 기록된 트랜잭션인지의 여부를 결정할 수 있다.
- [0076] 한 구현예에서, 클라이언트 측 상에서 유저에 의해 생성되는 트랜잭션은, 이전 기준 시간 파라미터에 추가하여, 트랜잭션을 위해 클라이언트 측 상에서 생성되는 고유 식별자를 포함할 수 있다.
- [0077] 트랜잭션에 대해 클라이언트 측 상에서 생성되는 고유 식별자는 단조 증가하는 트랜잭션 식별자일 수 있다. 트랜잭션 식별자의 특정한 형태는 본 명세서에서 제한되지 않는다.
- [0078] 한 구현예에서, 트랜잭션에 포함되는 트랜잭션의 고유 식별자는, 트랜잭션에 대해 클라이언트 측 상에서 생성되는 고유의 단조 증가하는 트랜잭션 번호일 수 있다.
- [0079] 예를 들면, 실제 적용에서, 블록체인 내의 노드 디바이스는 복수의 인스턴스로 구성되는 노드 디바이스일 수 있고, 각각의 인스턴스는 고유의 인스턴스 ID를 갖는다. 이 경우, 트랜잭션 번호는, 인스턴스 ID 및 생성된 난수를 포함하는 고유의 트랜잭션 번호일 수 있다.
- [0080] 다른 예를 들면, 블록체인 내의 노드 디바이스는 복수의 디바이스를 포함하는 분산형 디바이스이고, 각각의 디바이스는 고유의 디바이스 식별자(예를 들면, 디바이스 ID 또는 디바이스의 IP 어드레스)를 갖는다. 이 경우, 트랜잭션 번호는, 디바이스 식별자 및 생성된 난수를 포함하는 고유의 트랜잭션 번호일 수 있다.
- [0081] 확실히, 이전 예에서 설명되는 트랜잭션 번호 생성 방법은 단지 예에 불과하다. 기술 분야의 숙련된 자는 또한, 본 출원에서의 기술적 솔루션을 구현하는 동안 다른 트랜잭션 번호 생성 방법을 유연하게 사용할 수 있다. 다른 트랜잭션 번호 생성 방법은 본 출원에서 열거되지 않는다.
- [0082] 다른 구현예에서, 트랜잭션에 포함되는 트랜잭션의 고유 식별자는 생성된 트랜잭션에 클라이언트 측 상에서 추가되는 고유의 단조 증가하는 난스(nonce) 값일 수 있다.
- [0083] 난스 값은 트랜잭션에 추가되는 단조 증가하는 난수 또는 의사 난수일 수 있고 단지 한 번만 하나의 트랜잭션에 의해 사용될 수 있다.
- [0084] 종래의 이더리움(Ethereum) 블록체인 플랫폼이 예로서 사용된다. 이더리움에서, 각각의 계정 오브젝트(account object)에 대해 초기 난스 값이 구성되며 난스 값은 0에서부터 카운팅된다. 난스 값은, 계정 오브젝트가 트랜잭션을 전송할 때마다 1만큼 상응하여 증가되고, 계정 오브젝트에 의해 전송되는 각각의 트랜잭션은 계정 오브젝트의 현재의 난스 값(즉, 트랜잭션의 생성 동안의 계정 오브젝트의 난스 값)을 포함한다. 트랜잭션을 수신한 이

후, 어카운팅 노드로서 역할을 하는 노드 디바이스는 년스 값의 카운팅 순서에 기초하여 유저로부터 트랜잭션을 엄격하게 실행할 수 있다. 년스 값이 계정 오브젝트에 의해 이전에 전송된 트랜잭션에서 사용되는 년스 값보다 더 큰지의 여부를 결정하기 위해, 트랜잭션에 포함되는 년스 값이 체크될 수 있다. 트랜잭션에 포함되는 년스 값이 계정 오브젝트의 트랜잭션에 의해 이전에 사용된 최대 년스 값보다 더 작으면, 그것은 트랜잭션이 중복 트랜잭션이며 바로 거절된다는 것을 나타낸다. 트랜잭션에 포함되는 년스 값이 계정 오브젝트의 트랜잭션에 의해 이전에 사용된 최대 년스 값보다 훨씬 더 큰 경우, 트랜잭션은, 트랜잭션에 포함되는 년스 값에 선행하는 년스 값에 대응하는 트랜잭션이 프로세싱된 이후에만 프로세싱되어 후보 블록에 기록될 수 있다. 상응하여, 트랜잭션에 포함되는 년스 값이 계정 오브젝트의 트랜잭션에 의해 사용되는 최대 년스 값의 다음 카운트 값과 일치하면, 트랜잭션은 즉시 프로세싱될 수 있고, 트랜잭션은 후보 블록에서 기록된다. 본 출원에서, 트랜잭션에 포함되는 트랜잭션의 고유 식별자는 이더넷에서의 년스 값일 수 있는데, 세부 사항은 본 출원에서 생략된다.

- [0085] 수집되는 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션이라는 것을 결정한 이후, 어카운팅 노드로서 역할을 하는 노드 디바이스는, 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드가 트랜잭션 맥등 테이블에 저장되는지의 여부를 추가로 조회할 수 있다.
- [0086] 트랜잭션 맥등 레코드가 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장한 경우, 그것은, 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었고, 트랜잭션이 중복 트랜잭션이며, 트랜잭션이 바로 폐기될 수 있다는 것을 나타낸다.
- [0087] 또한, 트랜잭션 맥등 테이블이 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 저장하지 않았다면, 그것은 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되지 않았고, 노드 디바이스가 후보 블록에 트랜잭션을 기록할 수 있다는 것을 나타낸다.
- [0088] 본 출원에서, 후보 블록을 생성한 이후, 어카운팅 노드로서 역할을 하는 노드 디바이스는 생성된 후보 블록을 블록체인에서 추가로 브로드캐스팅할 수 있고, 어카운팅 허가(accounting permission)를 경쟁하기 위해, 블록체인에 의해 지원되는 합의 알고리즘에 기초하여 블록체인 내의 후보 블록에 기록되는 트랜잭션에 대해 합의 프로세싱을 수행할 수 있다.
- [0089] 블록체인에 의해 지원되는 특정한 타입의 합의 알고리즘은 본 출원에서 제한되지 않는다. 실제 적용에서, 작업 증명 알고리즘(proof-of-work algorithm) 또는 PBFT 알고리즘과 같은 표준 합의 알고리즘이 사용될 수 있거나, 또는 합의 알고리즘은 실제 서비스 요건에 기초하여 블록체인의 오퍼레이터에 의해 커스터마이징될 수 있다.
- [0090] 후보 블록이 합의를 통과하고, 어카운팅 노드로서 역할을 하는 노드 디바이스가 어카운팅 허가를 획득한 이후, 다음이 구현될 수 있다.
- [0091] 후보 블록은 블록체인에서의 최신 블록으로서 블록체인의 분산형 데이터베이스(즉, 분산 원장)에 추가될 수 있다. 이 경우, 후보 블록은 블록체인 내의 블록으로서 블록체인에 영구적으로 저장된다.
- [0092] 또한, 노드 디바이스는, 트랜잭션에 포함되는 트랜잭션 콘텐츠에 기초하여, 후보 블록에 기록되는 트랜잭션 통과 합의(transaction passing consensus)를, 노드 디바이스의 트랜잭션 실행 환경에서 실행되도록 트리거할 수 있다. 예를 들면, 트랜잭션은 블록체인에서 발행된 스마트 계약의 입력으로서 사용될 수 있고, 트랜잭션은, 스마트 계약에서 지정되는 트랜잭션 실행 프로그램 코드를 실행하는 것(예를 들면, 트랜잭션 실행에 관련되는 어떤 기능을 호출함)에 의해 노드 디바이스의 트랜잭션 실행 환경에서 실행된다.
- [0093] 한 구현예에서, 타겟 트랜잭션이 후보 블록에 성공적으로 기록되고, 후보 블록이 블록체인의 최신 블록으로서 블록체인의 분산형 데이터베이스에 최종적으로 저장되도록 합의를 통과한 이후, 타겟 트랜잭션은 블록체인의 분산형 데이터베이스에 성공적으로 저장되었다(다시 말하면, 트랜잭션이 성공적으로 온체인된다(onchain)). 이 경우, 어카운팅 노드로서 역할을 하는 노드 디바이스는 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 추가로 생성할 수 있고, 그 다음 트랜잭션 맥등 레코드를 트랜잭션 맥등 테이블에 삽입할 수 있다.
- [0094] 트랜잭션 맥등 레코드의 특정한 포맷은 본 출원에서 제한되지 않는다.
- [0095] 한 구현예에서, 트랜잭션 맥등 레코드가 상대적으로 큰 저장 공간을 점유하는 것을 방지하기 위해, 트랜잭션의 고유 식별자는 트랜잭션 맥등 레코드로서 트랜잭션 맥등 테이블에 직접적으로 삽입될 수 있다. 확실히, 실제 적용에서, 트랜잭션 맥등 레코드는 트랜잭션의 고유 식별자를 포함하는 데이터 레코드일 수 있다. 다음의 구현예는 트랜잭션 맥등 테이블에서의 트랜잭션 맥등 레코드가 트랜잭션의 고유 식별자인 예를 사용하는 것에 의해 설명된다.

- [0096] 트랜잭션 먹등 테이블에서의 트랜잭션 먹등 레코드는 트랜잭션 유효 기간 이내의 유효 트랜잭션의 트랜잭션 먹등 레코드만을 포함하고, 트랜잭션 유효 기간 이전의 이력 트랜잭션의 트랜잭션 먹등 레코드는 저장될 필요가 없다. 따라서, 트랜잭션 먹등 테이블의 저장 공간 소비가 과도하게 크지 않으며, 트랜잭션 먹등 테이블의 저장 공간 소비가 과도하게 큰 것 때문에 조회 성능 문제는 존재하지 않는다.
- [0097] 예를 들면, 어카운팅 노드로서 역할을 할 수 있는 임의의 노드 디바이스의 경우, 트랜잭션 먹등 테이블에 의해 점유되는 저장 공간이 상대적으로 작기 때문에, 트랜잭션 먹등 테이블은 디바이스 메모리에 직접적으로 로딩되어 유지될 수 있고, 트랜잭션 먹등 테이블은 제3자 스토리지 디스크를 사용하는 것에 의해 저장될 필요가 없다. 따라서, 트랜잭션 먹등 테이블에서의 조회가 메모리에서 직접적으로 수행될 수 있고, 조회 성능이 크게 향상될 수 있다.
- [0098] 또한, 유효 트랜잭션 중에서, 트랜잭션 먹등 테이블에 트랜잭션 먹등 레코드가 존재하지 않는 트랜잭션만이 후보 블록에 성공적으로 기록될 수 있다. 따라서, 블록체인에서의 트랜잭션 실행 동안 발생하는 "먹등성" 문제는 감소될 수 있으며, 비합법적인 노드는, 트랜잭션 유효 기간 내에 인터셉트된 유효 트랜잭션을 사용하는 것에 의해 재전송 공격을 개시할 수 없다. 그와 같이, 동일한 유효 트랜잭션은 반복적으로 실행될 수 없다.
- [0099] 또한, 블록체인 내의 노드 디바이스에 대해 복수의 인스턴스가 구성되거나, 또는 노드 디바이스가 분산형 디바이스인 경우, 다음의 문제점이 효과적으로 감소될 수 있다: 동일한 유효 트랜잭션이 분산형 디바이스에서의 상이한 인스턴스 또는 상이한 하위 디바이스(subdevice)에 의해 병렬로 발행되기 때문에, 동일한 유효 트랜잭션은 반복적으로 실행된다.
- [0100] 한 구현예에서, 트랜잭션 먹등 테이블에 기록되는 트랜잭션 식별자가 연속적인 값을 갖는 단조 증가하는 트랜잭션 식별자이기 때문에, 트랜잭션 먹등 레코드를 트랜잭션 먹등 테이블에 삽입하는 프로세스에서, 연속적인 값을 갖는 복수의 기록된 단조 증가하는 트랜잭션 식별자는 트랜잭션 먹등 테이블에 의해 점유되는 저장 공간을 추가로 감소시키기 위해 결합될 수 있다.
- [0101] 구체적으로, 타겟 트랜잭션의 트랜잭션 식별자를 트랜잭션 먹등 레코드로서 트랜잭션 먹등 테이블에 삽입할 때, 어카운팅 노드로서 역할을 하는 노드 디바이스는, 타겟 트랜잭션의 트랜잭션 식별자가 트랜잭션 먹등 테이블에 삽입된 이후, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 트랜잭션 먹등 테이블이 포함하는지의 여부를 결정할 수 있다. 만약 그렇다면, 노드 디바이스는 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 인터벌의 형태로 트랜잭션 먹등 테이블에 기록할 수 있다. 만약 그렇지 않다면, 노드 디바이스는 타겟 트랜잭션의 트랜잭션 식별자를 이산 값의 형태로 트랜잭션 먹등 테이블에 기록할 수 있다.
- [0102] 예를 들면, 타겟 트랜잭션의 트랜잭션 식별자는 년스 값이다. 타겟 트랜잭션에 포함되는 년스 값이 2이고, 년스 값 1, 3, 및 5가 트랜잭션 먹등 테이블에 기록되었다는 것을 가정한다. 이 경우, 타겟 트랜잭션에 포함되는 년스 값 2가 트랜잭션 먹등 레코드로서 트랜잭션 먹등 테이블에 삽입된 이후, 트랜잭션 먹등 테이블에 기록된 년스 값 2 및 년스 값 1 및 3은 단조 증가하는 연속적인 값이다. 따라서, 년스 값 1, 2, 및 3은 인터벌 [1, 3]의 형태로 트랜잭션 먹등 테이블에 기록될 수 있다. 대안적으로, 인터벌의 최대 값은 인터벌을 나타내기 위해 사용될 수 있고, 인터벌 [1, 3]은, 트랜잭션 먹등 테이블에 년스 값을 기록하기 위해 3으로 표현되어, 트랜잭션 먹등 레코드의 저장 공간을 추가로 절약한다.
- [0103] 다른 예를 들면, 타겟 트랜잭션에 포함되는 년스 값은 9이고, 년스 값 [1, 3] 및 5가 트랜잭션 먹등 테이블에 기록되었다. 타겟 트랜잭션에 포함되는 년스 값 9가 트랜잭션 먹등 레코드로서 트랜잭션 먹등 테이블에 삽입된 이후, 트랜잭션 먹등 테이블은 복수의 단조 증가하는 연속적인 년스 값을 포함하지 않는다. 이 경우, 년스 값 9는 이산 값의 형태로 트랜잭션 먹등 테이블에 기록될 수 있다. 이 경우, 업데이트된 트랜잭션 먹등 테이블에서의 년스 값은 [1, 3], 5 및 9이다.
- [0104] 그와 같이, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자가 인터벌의 형태로 트랜잭션 먹등 테이블에 기록될 수 있다. 그것은, 대규모 트랜잭션 프로세싱 시나리오에서, 트랜잭션 먹등 테이블의 저장 공간의 점유를 상당히 감소시킬 수 있다.
- [0105] 확실히, 트랜잭션 먹등 테이블에 트랜잭션 먹등 레코드를 삽입하는 프로세스에서, 트랜잭션 먹등 테이블에서 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자가 결합된다. 실제 적용에서, 설명된 결합 프로세스는 미리 설정된 결합 기간에 기초하여 주기적으로 완료될 수 있다. 예를 들면, 트랜잭션 먹등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는지의 여부는, 미리 설정된 결합 기간에 기초하여 주기적으로 체크된다. 만약 그렇다면, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자는 인터벌의

형태로 트랜잭션 맥등 테이블에 기록될 수 있다.

- [0106] 본 출원에서, 후보 블록을 생성한 이후, 어카운팅 노드로서 역할을 하는 노드 디바이스는 생성된 후보 블록을 블록체인에서 추가로 브로드캐스팅할 수 있고, 어카운팅 허가를 경쟁하기 위해, 블록체인에 의해 지원되는 합의 알고리즘에 기초하여 블록체인 내의 후보 블록에 기록되는 트랜잭션에 대해 합의 프로세싱을 수행할 수 있다.
- [0107] 블록체인에 의해 지원되는 특정한 타입의 합의 알고리즘은 본 출원에서 제한되지 않는다. 실제 적용에서, 작업 증명 알고리즘 또는 PBFT 알고리즘과 같은 표준 합의 알고리즘이 사용될 수 있거나, 또는 합의 알고리즘은 실제 서비스 요건에 기초하여 블록체인의 오퍼레이터에 의해 커스터마이징될 수 있다.
- [0108] 후보 블록이 합의를 통과하고, 어카운팅 노드로서 역할을 하는 노드 디바이스가 어카운팅 허가를 획득한 이후, 다음이 구현될 수 있다.
- [0109] 후보 블록은 블록체인에서의 최신 블록으로서 블록체인의 분산형 데이터베이스(즉, 분산 원장)에 추가될 수 있다. 이 경우, 후보 블록은 블록체인 내의 블록으로서 블록체인에 영구적으로 저장된다.
- [0110] 또한, 노드 디바이스는, 트랜잭션에 포함되는 트랜잭션 콘텐츠에 기초하여, 후보 블록에 기록되는 트랜잭션 통과 합의를, 노드 디바이스의 트랜잭션 실행 환경에서 실행되도록 트리거할 수 있다. 예를 들면, 트랜잭션은 블록체인에서 발행된 스마트 계약의 입력으로서 사용될 수 있고, 트랜잭션은, 스마트 계약에서 지정되는 트랜잭션 실행 프로그램 코드를 실행하는 것(예를 들면, 트랜잭션 실행에 관련되는 어떤 기능을 호출함)에 의해 노드 디바이스의 트랜잭션 실행 환경에서 실행된다.
- [0111] 한 구현예에서, 타겟 트랜잭션이 후보 블록에 성공적으로 기록되고, 후보 블록이 블록체인의 최신 블록으로서 블록체인의 분산형 데이터베이스에 최종적으로 저장되도록 합의를 통과한 이후, 타겟 트랜잭션은 블록체인의 분산형 데이터베이스에 성공적으로 저장되었다(다시 말하면, 트랜잭션이 성공적으로 온체인된다). 이 경우, 어카운팅 노드로서 역할을 하는 노드 디바이스는 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 맥등 레코드를 추가로 생성할 수 있고, 그 다음 트랜잭션 맥등 레코드를 트랜잭션 맥등 테이블에 삽입할 수 있다.
- [0112] 본 출원에서, 트랜잭션 맥등 테이블은 트랜잭션 유효 기간 이내의 유효 트랜잭션에 대응하는 트랜잭션 맥등 레코드를 유지하기 위해 사용된다. 따라서, 실제 적용에서, 트랜잭션 맥등 테이블을 공동으로 유지하는 멤버 노드 디바이스는, 시간적으로 트랜잭션 맥등 테이블에서의 트랜잭션 유효 기간을 넘어서게 되는 트랜잭션의 트랜잭션 맥등 레코드를 주기적으로 지울 수 있다.
- [0113] 예를 들면, 트랜잭션 유효 기간은, 현재의 어카운팅 기간에 생성되는 후보 블록의 생성 시간을 기준으로 하여 사용하는 것에 의해 블록체인에서 어카운팅 노드 디바이스에 의해 설정되는 시간 인터벌일 수 있다. 후보 블록이 주기적으로 생성되기 때문에, 트랜잭션 유효 기간도 또한 주기적이고 동적인 시간 기간이다. 이 경우, 노드 디바이스는 다음 번 어카운팅 기간에 새로운 후보 블록이 생성될 때 트랜잭션 유효 기간을 다시 결정할 수 있고, 그 다음, 다시 결정되는 트랜잭션 유효 기간을 넘어서게 되는 트랜잭션의 트랜잭션 맥등 레코드에 대해 트랜잭션 맥등 테이블을 능동적으로 검색할 수 있다. 예를 들면, 트랜잭션에서 기준 시간 파라미터를 사용하는 것에 의해 트랜잭션이 다시 결정된 트랜잭션 유효 기간을 여전히 넘어서게 되는지의 여부가 결정될 수 있다. 특정한 구현 프로세스가 생략된다.
- [0114] 게다가, 이들 식별된 트랜잭션 맥등 레코드는 트랜잭션 맥등 테이블에서 유지되는 트랜잭션 맥등 레코드를 동적으로 업데이트하고 유지하기 위해 삭제될 수 있다. 그와 같이, 트랜잭션 맥등 테이블에서의 트랜잭션 맥등 레코드는 현재 트랜잭션 유효 기간 이내의 유효 트랜잭션에 대응하는 트랜잭션 맥등 레코드이다.
- [0115] 본 출원은 또한 기술한 방법 구현예에 대응하는 블록체인 기반 트랜잭션 프로세싱 장치의 구현예를 제공한다. 본 출원에서의 블록체인 기반 트랜잭션 프로세싱 장치의 구현예는 전자 디바이스에 적용될 수 있다. 장치 구현예는 소프트웨어, 하드웨어, 또는 하드웨어와 소프트웨어의 조합에 의해 구현될 수 있다. 소프트웨어 구현예가 예로서 사용된다. 장치가 위치되는 전자 디바이스의 프로세서는 불휘발성 메모리로부터 메모리로 대응하는 컴퓨터 프로그램 명령어를 판독하고, 컴퓨터 프로그램 명령어는 논리적 장치를 형성하도록 실행된다. 하드웨어 구현예의 관점에서, 도 2는 본 출원에 따라 블록체인 기반 트랜잭션 프로세싱 장치가 위치되는 전자 디바이스의 하드웨어를 예시하는 구조도이다. 도 2에서 도시되는 프로세서, 메모리, 네트워크 인터페이스, 및 불휘발성 메모리에 더하여, 이 구현에서 장치가 위치되는 전자 디바이스는 일반적으로 전자 디바이스의 실제 기능에 기초하여 다른 하드웨어를 포함할 수 있다. 세부 사항은 생략된다.
- [0116] 도 3은, 본 출원의 예시적인 구현예에 따른, 블록체인 기반 트랜잭션 프로세싱 장치를 예시하는 블록도이다.

- [0117] 도 3을 참조하면, 블록체인 기반 트랜잭션 프로세싱 장치(30)는 도 2에서 도시되는 전자 디바이스에 적용될 수 있고, 수신 모듈(301), 조회 모듈(302), 및 기록 모듈(303)을 포함한다.
- [0118] 수신 모듈(301)은 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 타겟 트랜잭션을 수신하도록 구성되는데, 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함한다.
- [0119] 조회 모듈(302)은, 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 조회하도록 구성된다.
- [0120] 기록 모듈(303)은, 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하지 않는 경우, 타겟 트랜잭션을 후보 블록에 기록하도록 구성된다.
- [0121] 이 구현예에서, 트랜잭션 먹등 테이블에서의 트랜잭션 먹등 레코드는, 트랜잭션 먹등 레코드에 대응하는 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었다는 것을 나타낸다.
- [0122] 이 구현예에서, 기록 모듈(303)은 또한: 타겟 트랜잭션이 후보 블록에 기록되고, 후보 블록이 블록체인의 분산형 데이터베이스에 성공적으로 저장되도록 합의를 통과한 경우, 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 생성하도록, 그리고 타겟 트랜잭션의 고유 식별자에 대응하는 생성된 트랜잭션 먹등 레코드를 트랜잭션 먹등 테이블에 삽입하도록 구성된다.
- [0123] 이 구현예에서, 트랜잭션 먹등 테이블에서의 트랜잭션 먹등 레코드는 트랜잭션의 고유 식별자이고, 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 트랜잭션의 고유 식별자는 단조 증가하는 트랜잭션 식별자이다.
- [0124] 기록 모듈(303)은 또한: 트랜잭션의 고유 식별자가 트랜잭션 먹등 테이블에 삽입된 이후, 트랜잭션 먹등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는지의 여부를 결정하도록; 그리고 만약 그렇다면, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 인터벌의 형태로 트랜잭션 먹등 테이블에 기록하도록; 또는 만약 그렇지 않다면, 트랜잭션의 트랜잭션 식별자를 이산 값의 형태로 트랜잭션 먹등 테이블에 기록하도록 구성된다.
- [0125] 이 구현예에서, 타겟 트랜잭션은 기준 시간 파라미터를 더 포함하고, 기준 시간 파라미터는, 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하기 위해 사용된다.
- [0126] 장치(30)는 다음의 것: (도 3에서 도시되지 않은) 결정 모듈(304)을 더 포함하는데, 결정 모듈(304)은, 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부가 조회되기 이전에, 기준 시간 파라미터에 기초하여 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하도록; 그리고 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션이라고 결정되는 경우, 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 추가로 조회하도록 구성된다.
- [0127] 이 구현예에서, 블록체인은 컨소시엄 블록체인이다. 장치 내의 각각의 모듈의 기능 및 역할의 구현 프로세스에 대해서는, 이전 방법에서의 대응하는 단계의 구현 프로세스를 참조한다. 세부 사항은 여기서는 생략되지 않는다.
- [0128] 장치 구현예가 기본적으로 방법 구현예에 대응하기 때문에, 관련 부분에 대해서는, 방법 구현예에서의 관련된 설명에 대한 참조가 이루어질 수 있다. 앞서 설명된 장치 구현예는 예에 불과하다. 분리된 부분으로서 설명되는 모듈은 물리적으로 분리될 수도 있거나 또는 분리되지 않을 수도 있고, 모듈로서 디스플레이 되는 부분은 물리적 모듈일 수도 있거나 또는 아닐 수도 있고, 하나의 위치에 위치될 수 있거나, 또는 복수의 네트워크 모듈 상에 분산될 수 있다. 모듈 중 몇몇 또는 전체는 본 출원의 솔루션의 목적을 달성하기 위한 실제 요구에 기초하여 선택될 수 있다. 기술 분야에서 통상의 기술을 가진 자는 창의적인 노력 없이 본 출원의 구현예를 이해하고 구현할 수 있다.
- [0129] 이전 구현예에서 예시되는 시스템, 장치, 또는 모듈은 컴퓨터 칩 또는 엔티티를 사용하는 것에 의해 구현될 수 있거나, 또는 소정의 기능을 갖는 제품을 사용하는 것에 의해 구현될 수 있다. 통상적인 구현 디바이스는 컴퓨터이고, 컴퓨터는, 퍼스널 컴퓨터, 랩탑 컴퓨터, 셀룰러 전화, 카메라 폰, 스마트폰, 개인 휴대형 정보 단말(personal digital assistant), 미디어 플레이어, 내비게이션 디바이스, 전자 메일 수신 및 전송 디바이스, 게임 콘솔, 태블릿, 웨어러블 디바이스, 또는 이들 디바이스의 임의의 조합일 수 있다.
- [0130] 본 출원은 또한 이전 방법 구현예에 대응하는 전자 디바이스의 구현예를 제공한다. 전자 디바이스는 머신 실행

가능 명령어를 저장하도록 구성되는 프로세서 및 메모리를 포함한다. 프로세서 및 메모리는 일반적으로 내부 버스를 사용하는 것에 의해 서로 연결된다. 다른 가능한 구현예에서, 디바이스는 외부 인터페이스를 더 포함할 수 있고, 그 결과, 디바이스는 다른 디바이스 또는 컴포넌트와 통신할 수 있다.

[0131] 이 구현예에서, 메모리에 저장되며 블록체인 기반 트랜잭션 프로세싱의 제어 로직에 대응하는 머신 실행 가능 명령어를 판독 및 실행하는 것에 의해, 프로세서는, 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 타겟 트랜잭션 - 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함함 - 을 수신하도록; 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 조회하도록; 그리고 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하지 않는 경우, 타겟 트랜잭션을 후보 블록에 기록하도록 구성된다.

[0132] 이 구현예에서, 메모리에 저장되며 블록체인 기반 트랜잭션 프로세싱의 제어 로직에 대응하는 머신 실행 가능 명령어를 판독 및 실행하는 것에 의해, 프로세서는: 타겟 트랜잭션이 후보 블록에 기록되고, 후보 블록이 블록체인의 분산형 데이터베이스에 성공적으로 저장되도록 합의를 통과한 경우, 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 생성하도록, 그리고 타겟 트랜잭션의 고유 식별자에 대응하는 생성된 트랜잭션 먹등 레코드를 트랜잭션 먹등 테이블에 삽입하도록 구성된다.

[0133] 이 구현예에서, 트랜잭션 먹등 테이블에서의 트랜잭션 먹등 레코드는 트랜잭션의 고유 식별자이고, 블록체인 내의 멤버 노드 디바이스에 의해 개시되는 트랜잭션의 고유 식별자는 단조 증가하는 트랜잭션 식별자이다.

[0134] 메모리에 저장되며 블록체인 기반 트랜잭션 프로세싱의 제어 로직에 대응하는 머신 실행 가능 명령어를 판독 및 실행하는 것에 의해, 프로세서는, 트랜잭션의 고유 식별자가 트랜잭션 먹등 테이블에 삽입된 이후, 트랜잭션 먹등 테이블이 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 포함하는지의 여부를 결정하도록; 그리고 만약 그렇다면, 연속적인 값을 갖는 복수의 단조 증가하는 트랜잭션 식별자를 인터벌의 형태로 트랜잭션 먹등 테이블에 기록하도록; 또는 만약 그렇지 않다면, 트랜잭션의 트랜잭션 식별자를 이산 값의 형태로 트랜잭션 먹등 테이블에 기록하도록 구성된다.

[0135] 이 구현예에서, 타겟 트랜잭션은 기준 시간 파라미터를 더 포함하고, 기준 시간 파라미터는, 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하기 위해 사용된다.

[0136] 메모리에 저장되며 블록체인 기반 트랜잭션 프로세싱의 제어 로직에 대응하는 머신 실행 가능 명령어를 판독 및 실행하는 것에 의해, 프로세서는, 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부가 조회되기 이전에, 기준 시간 파라미터에 기초하여 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션인지의 여부를 결정하도록; 그리고 타겟 트랜잭션이 트랜잭션 유효 기간 이내의 유효 트랜잭션이라고 결정되는 경우, 미리 설정된 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하는지의 여부를 추가로 조회하도록 구성된다.

[0137] 기술 분야의 숙련된 자는, 본 출원을 검토하고 여기에서 본 개시를 실시한 이후 본 출원의 다른 구현예를 용이하게 알아낼 수 있다. 본 출원은 본 출원의 임의의 변형예, 사용예 또는 적용예를 포괄하도록 의도되며, 이들 변형예, 사용예 또는 적용예는 본 출원의 일반적인 원리를 따르며 본 출원의 기술 분야에서 공개되지 않은 통상적인 기술 또는 종래의 기술을 포함한다. 본 명세서 및 구현예는 단지 예로서 간주되며, 본 출원의 실제 범위 및 취지는 다음의 청구범위에 의해 지시된다.

[0138] 본 출원은 상기에서 설명되며 첨부 도면에서 도시되는 정확한 구조체로 제한되지 않으며, 본 출원의 범위를 벗어나지 않으면서 다양한 수정 및 변경이 이루어질 수 있다는 것이 이해되어야 한다. 본 출원의 범위는 오로지 첨부된 청구범위에 의해서만 제한된다.

[0139] 앞선 설명은 본 출원의 바람직한 구현예에 불과하며, 본 출원을 제한하도록 의도되는 것은 아니다. 본 출원의 취지 및 원리를 벗어나지 않으면서 이루어지는 임의의 수정, 등가적 대체, 또는 개선은 본 출원의 보호 범위 내에 속할 것이다.

[0140] 상기 맥락에서, 도 4는, 본 개시의 구현예에 따른, 블록체인 기반 트랜잭션을 프로세싱하기 위한 컴퓨터 구현 방법(400)의 예를 예시하는 플로우차트이다. 제시의 명확성을 위해, 이하의 설명은, 이 설명의 다른 도면의 맥락에서 방법(400)을 일반적으로 설명한다. 그러나, 방법(400)은, 예를 들면, 임의의 시스템, 환경, 소프트웨어, 및 하드웨어에 의해 또는 시스템, 환경, 소프트웨어, 및 하드웨어의 조합에 의해 적절하게 수행될 수 있다는 것이 이해될 것이다. 몇몇 구현예에서, 방법(400)의 다양한 단계는 병렬로, 조합하여, 루프에서, 또는 임의의 순

서로 실행될 수 있다.

- [0141] 402에서, 블록체인은 멤버 노드 디바이스에 의해 게시되는 타겟 트랜잭션을 수신한다. 타겟 트랜잭션은 타겟 트랜잭션의 고유 식별자를 포함할 수 있다. 하나의 예에서, 고유 식별자는 년스 값에 대응한다. 타겟 트랜잭션은 기준 시간 파라미터를 더 포함할 수 있다. 하나의 예에서, 기준 시간 파라미터는 타임스탬프를 포함한다. 402로부터, 방법(400)은 404로 진행한다.
- [0142] 404에서, 방법은 타겟 트랜잭션이 트랜잭션 유효 기간 내에서 유효한지의 여부를 결정하도록 진행한다. 맥락에서, 타겟 트랜잭션은 블록체인 상의 멤버 노드 디바이스에 의해 연속적인 방식으로 게시될 수도 있다. 각각의 타겟 트랜잭션은 유한한 유효 기간을 갖는다. 예를 들면, 타겟 트랜잭션의 기준 시간 파라미터는, 기준 시간 파라미터에 기초하여 타겟 트랜잭션이 트랜잭션 유효 기간 내에 있는지의 여부를 결정하기 위해 검증될 수 있다. 하나의 예에서, 트랜잭션 유효 기간은, 블록체인 상에서의 블록체인 트랜잭션의 만료 기간, 또는 블록체인 상의 디바이스에 대한 클록 오프셋에 의해 특성 묘사되는 시간 윈도우에 대응한다. 타겟 트랜잭션이 유효성 시간 기간(406) 내에 있다는 것을 결정하는 것에 응답하여, 방법(400)은 408로 진행한다. 그렇지 않으면, 타겟 트랜잭션은 드랍될 수도 있다.
- [0143] 408에서, 방법(400)은, 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하였는지의 여부를 결정하기 위해 블록체인 상의 트랜잭션 먹등 테이블을 조회하도록 진행한다. 트랜잭션 먹등 테이블에 저장되는 트랜잭션 먹등 레코드는, 트랜잭션 먹등 레코드에 대응하는 트랜잭션이 블록체인의 분산형 데이터베이스에 성공적으로 기록되었다는 것을 나타낸다. 트랜잭션 먹등 레코드는, 초기 적용을 넘게 결과를 변경하지 않으면서 다수 회 적용될 수 있는 트랜잭션 레코드를 나타낸다. 408에서, 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하였는지의 여부에 관한 결정이 이루어진다. 408로부터, 방법(400)은 410으로 진행한다.
- [0144] 410에서, 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하였는지의 여부에 관한 결정이 이루어진다. 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하였다는 것을 결정하는 것에 응답하여, 방법(400)은 타겟 트랜잭션이 성공적으로 기록되었다는 것을 결정하는 412로 진행한다. 트랜잭션 먹등 테이블이 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 저장하였다는 것을 결정하는 것에 응답하여, 방법(400)은 블록체인 상의 후보 블록에 타겟 트랜잭션을 기록하는 414로 진행한다. 414로부터, 방법(400)은 416으로 진행한다.
- [0145] 416에서, 방법(400)은 블록체인에 의해 지원되는 합의 알고리즘을 사용하여 후보 블록 내의 타겟 트랜잭션에 대해 합의 프로세싱을 수행하여 블록체인의 분산형 데이터베이스에 후보 블록을 저장할지의 여부를 결정한다. 후보 블록이 합의 프로세싱을 통과하는 것에 응답하여, 방법(400)은 타겟 트랜잭션의 고유 식별자에 대응하는 트랜잭션 먹등 레코드를 생성하도록 진행한다(418). 후속하여, 방법(400)은 타겟 트랜잭션의 고유 식별자에 대응하는 생성된 트랜잭션 먹등 레코드를 블록체인 상의 트랜잭션 먹등 테이블에 삽입하도록 진행한다(420).
- [0146] 본 명세서에서 게시되는 구현에는 블록체인 트랜잭션을 핸들링하기 위한 기술적 솔루션을 제공한다. 하나의 양태에서, 블록체인에서의 수신된 트랜잭션에 대한 먹등 프로세싱을 강제하기 위해 트랜잭션 먹등 테이블이 생성된다. 먹등 프로세싱은 초기 적용을 넘게 결과를 변경하지 않으면서 다수 회 적용될 수 있다. 그와 같이, 비합법적인 노드는 인터셉트된 기한이 지난 트랜잭션을 사용하는 것에 의해 재전송 공격을 개시할 수 없다. 다른 양태에서, 타겟 트랜잭션은 타임스탬프에 기초하여 블록체인 상에서 게시된다. 타겟 트랜잭션의 적시의(timely) 프로세싱은 유효성 시간 기간 내에 발생할 것으로 예상된다. 각각의 타겟 트랜잭션에 대해 시간 윈도우를 시행하는 것에 의해, 어카운팅 노드는, 재전송(replay)과 같은, 유효성 시간 윈도우 밖에 있는 타겟 트랜잭션이 비합법적인 것으로 취급될 수도 있도록, 타겟 트랜잭션의 적시성을 식별할 수 있다.
- [0147] 본 명세서에서 설명되는 실시형태 및 동작은, 디지털 전자 회로부(circuitry)에서, 또는, 본 명세서에서 게시되는 구조체를 비롯한 컴퓨터 소프트웨어, 펌웨어, 또는 하드웨어로, 또는 이들 중 하나 이상의 조합으로 구현될 수 있다. 동작은, 하나 이상의 컴퓨터 판독 가능 스토리지 디바이스 상에 저장되는 또는 다른 소스로부터 수신되는 데이터에 대한 데이터 프로세싱 장치에 의해 수행되는 동작으로서 구현될 수 있다. 데이터 프로세싱 장치, 컴퓨터, 또는 컴퓨팅 디바이스는, 예로서, 프로그래머블 프로세서, 컴퓨터, 시스템 온 칩, 또는 전술한 것 중 다수의 것, 또는 전술한 것의 조합을 비롯한, 데이터를 프로세싱하기 위한 장치, 디바이스, 및 머신을 포괄할 수도 있다. 장치는, 특수 목적의 논리 회로부, 예를 들면, 중앙 프로세싱 유닛(central processing unit; CPU), 필드 프로그래머블 게이트 어레이(field programmable gate array; FPGA) 또는 주문형 집적 회로(application-specific integrated circuit; ASIC)를 포함할 수 있다. 장치는 또한, 문제의 컴퓨터 프로그램에

대한 실행 환경을 생성하는 코드, 예를 들면, 프로세서 펌웨어, 프로토콜 스택, 데이터베이스 관리 시스템, 오퍼레이팅 시스템(예를 들면, 오퍼레이팅 시스템 또는 오퍼레이팅 시스템의 조합), 크로스 플랫폼 런타임 환경, 가상 머신, 또는 그들 중 하나 이상의 조합을 구성하는 코드를 포함할 수 있다. 장치 및 실행 환경은, 웹 서비스, 분산 컴퓨팅 및 그리드 컴퓨팅 인프라와 같은, 여러 가지 상이한 컴퓨팅 모델 인프라를 실현할 수 있다.

[0148] 컴퓨터 프로그램(예를 들면, 프로그램, 소프트웨어, 소프트웨어 애플리케이션, 소프트웨어 모듈, 소프트웨어 유닛, 스크립트, 또는 코드로서 또한 알려짐)은, 컴파일식 언어(compiled language) 또는 인터프리트식 언어(interpreted language), 선언적 언어(declarative language) 또는 절차적 언어(procedural language)를 비롯한, 임의의 형태의 프로그래밍 언어로 작성될 수 있고, 그것은, 독립형 프로그램으로서 또는 모듈, 컴포넌트, 서브루틴, 객체, 또는 컴퓨팅 환경에서 사용하기에 적절한 다른 유닛으로서 배치되는 것을 비롯한, 임의의 형태로 배치될 수 있다. 프로그램은, 다른 프로그램 또는 데이터를 유지하는 파일의 부분(예를 들면, 마크업 언어 문서에 저장되는 하나 이상의 스크립트)에, 문제가 되는 프로그램에 전용되는 단일의 파일에, 또는 다수의 협력 파일(coordinated file)(예를 들면, 하나 이상의 모듈, 서브 프로그램, 또는 코드의 일부를 저장하는 파일)에 저장될 수 있다. 컴퓨터 프로그램은, 하나의 컴퓨터 상에서 또는 하나의 사이트에 위치되는 또는 다수의 사이트에 걸쳐 분산되며 통신 네트워크에 의해 인터커넥트되는 다수의 컴퓨터 상에서 실행될 수 있다.

[0149] 컴퓨터 프로그램의 실행을 위한 프로세서는, 예로서, 범용 및 특수 목적 마이크로프로세서, 및 임의의 종류의 디지털 컴퓨터의 임의의 하나 이상의 프로세서 둘 모두를 포함한다. 일반적으로, 프로세서는 리드 온리 메모리 또는 랜덤 액세스 메모리 또는 둘 모두로부터 명령어 및 데이터를 수신할 것이다. 컴퓨터의 필수 엘리먼트는, 명령어에 따라 동작을 수행하기 위한 프로세서 및 명령어 및 데이터를 저장하기 위한 하나 이상의 메모리 디바이스이다. 일반적으로, 컴퓨터는 또한, 데이터를 저장하기 위한 하나 이상의 대용량 스토리지 디바이스를 포함할 것이고, 하나 이상의 대용량 스토리지 디바이스로부터 데이터를 수신하도록 그리고 하나 이상의 대용량 스토리지 디바이스로 데이터를 전송하도록, 또는 둘 모두를 하도록 동작 가능하게 커플링될 것이다. 컴퓨터는, 다른 디바이스, 예를 들면, 모바일 디바이스, 개인 휴대형 정보 단말(personal digital assistant; PDA), 게임 콘솔, 전지구 위치 결정 시스템(global positioning system; GPS) 수신기, 또는 휴대용 스토리지 디바이스에 임베딩될 수 있다. 컴퓨터 프로그램 명령어 및 데이터를 저장하기에 적절한 디바이스는, 예로서, 반도체 메모리 디바이스, 자기 디스크, 및 광자기 디스크(magneto-optical disk)를 비롯한, 불휘발성 메모리, 매체, 및 메모리 디바이스를 포함한다. 프로세서 및 메모리는 특수 목적의 논리 회로부에 의해 보충될 수 있거나, 또는 특수 목적의 논리 회로부에 통합될 수 있다.

[0150] 모바일 디바이스는 핸드셋, 유저 기기(user equipment; UE), 이동 전화(예를 들면, 스마트폰), 태블릿, 웨어러블 디바이스(예를 들면, 스마트워치 및 스마트 안경), 인체 내부의 이식 디바이스(예를 들면, 바이오 센서, 달팽이관 임플란트), 또는 다른 타입의 모바일 디바이스를 포함할 수 있다. 모바일 디바이스는, 다양한 통신 네트워크(이하에서 설명됨)에 무선으로(예를 들면, 무선 주파수(RF) 신호를 사용하여) 통신할 수 있다. 모바일 디바이스는, 모바일 디바이스의 현재 환경의 특성을 결정하기 위한 센서를 포함할 수 있다. 센서는, 카메라, 마이크, 근접 센서, GPS 센서, 모션 센서, 가속도계, 주변 광 센서, 습도 센서, 자이로스코프, 콤팩스, 기압계, 지문 센서, 얼굴 인식 시스템, RF 센서(예를 들면, Wi-Fi 및 셀룰러 무선), 열 센서, 또는 다른 타입의 센서를 포함할 수 있다. 예를 들면, 카메라는, 이동식 또는 고정식 렌즈를 갖는 전방 대향 또는 후방 대향 카메라, 플래시, 이미지 센서, 및 이미지 프로세서를 포함할 수 있다. 카메라는, 얼굴 및/또는 홍채(iris) 인식을 위한 세부 사항(detail)을 캡처할 수 있는 메가 픽셀 카메라일 수 있다. 카메라는, 메모리에 저장되는 또는 원격으로 액세스되는 데이터 프로세서 및 인증 정보와 함께, 얼굴 인식 시스템을 형성할 수 있다. 얼굴 인식 시스템 또는 하나 이상의 센서, 예를 들면, 마이크, 모션 센서, 가속도계, GPS 센서, 또는 RF 센서는 유저 인증을 위해 사용될 수 있다.

[0151] 유저와의 상호 작용을 제공하기 위해, 실시형태는, 디스플레이 디바이스 및 입력 디바이스, 예를 들면, 정보를 유저에게 디스플레이하기 위한 액정 디스플레이(liquid crystal display; LCD) 또는 유기 발광 다이오드(organic light-emitting diode; OLED)/가상 현실(virtual-reality; VR)/증강 현실(augmented-reality; AR) 디스플레이 및 유저가 컴퓨터에게 입력을 제공할 수 있게 하는 터치스크린, 키보드, 및 포인팅 디바이스를 구비하는 컴퓨터 상에서 구현될 수 있다. 유저와의 상호 작용을 제공하기 위해 다른 종류의 디바이스가 또한 사용될 수 있다; 예를 들면, 유저에게 제공되는 피드백은 임의의 형태의 감각 피드백(sensory feedback), 예를 들면, 시각적 피드백, 청각 피드백, 또는 촉각 피드백일 수 있으며; 그리고 유저로부터의 입력은, 음향, 음성, 또는 촉각 입력을 비롯한, 임의의 형태로 수신될 수 있다. 또한, 컴퓨터는, 유저에 의해 사용되는 디바이스로 문서를 전송하는 것 및 유저에 의해 사용되는 디바이스로부터 문서를 수신하는 것에 의해; 예를 들면, 웹 브라우저로부

터 수신되는 요청에 응답하여 유저의 클라이언트 디바이스 상의 웹 브라우저에 웹 페이지를 전송하는 것에 의해, 유저와 상호 작용할 수 있다.

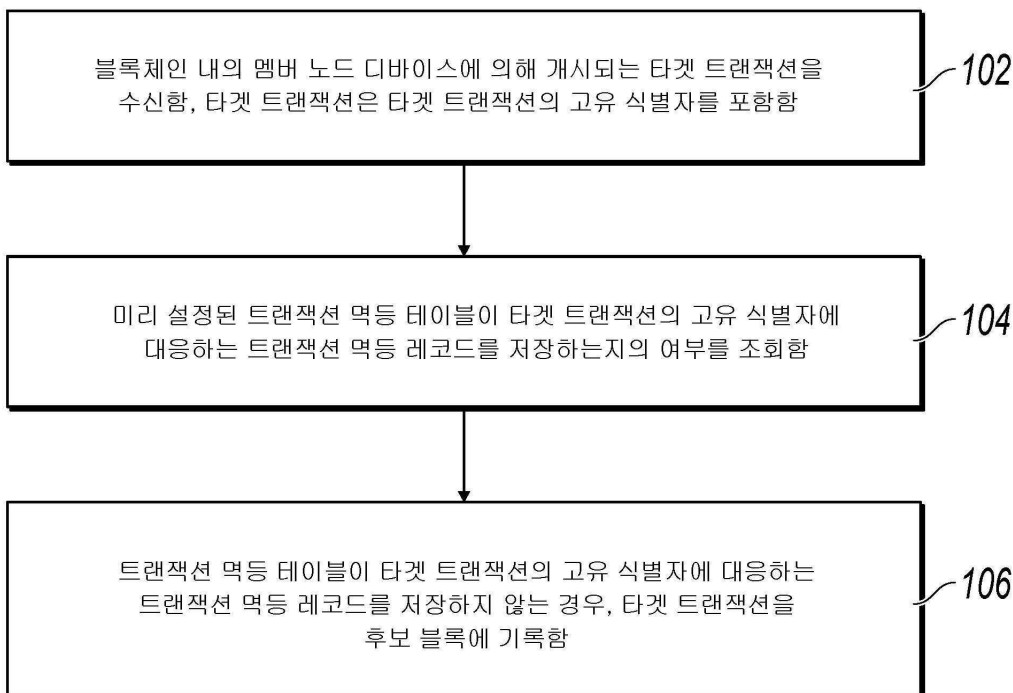
[0152] 실시형태는, 임의의 형태 또는 매체의 유선 또는 무선 디지털 데이터 통신(또는 이들의 조합), 예를 들면, 통신 네트워크에 의해 인터커넥트되는 컴퓨팅 디바이스를 사용하여 구현될 수 있다. 인터커넥트된 디바이스의 예는, 통상적으로 통신 네트워크를 통해 상호 작용하는, 일반적으로 서로 멀리 떨어진 클라이언트 및 서버이다. 클라이언트, 예를 들면, 모바일 디바이스는, 그 자체로, 서버와 함께, 또는 서버를 통해 트랜잭션을 수행할 수 있는데, 예를 들면, 구매, 판매, 지불, 제공, 전송, 또는 대여 트랜잭션을 수행할 수 있거나, 또는 이들을 인가할 수 있다. 그러한 트랜잭션은, 액션 및 응답이 시간적으로 근접하도록 실시간일 수도 있다; 예를 들면, 개인은 액션 및 응답을 실질적으로 동시에 발생하는 것으로 인식하며, 개인의 액션에 후속하는 응답에 대한 시간 차이는 1 밀리초(ms) 미만 또는 1 초(s) 미만이거나, 또는 응답은, 시스템의 프로세싱 한계를 고려하여 의도적인 지연을 갖지 않는다.

[0153] 통신 네트워크의 예는, 근거리 통신망(local area network; LAN), 무선 액세스 네트워크(Radio Access Network; RAN), 도시권 통신망(Metropolitan Area Network; MAN) 및 광역 통신망(wide area network; WAN)을 포함한다. 통신 네트워크는, 인터넷의 전체 또는 일부, 다른 통신 네트워크, 또는 통신 네트워크의 조합을 포함할 수 있다. 정보는, 롱 텀 에볼루션(long term evolution; LTE), 5G, IEEE 802, 인터넷 프로토콜(Internet Protocol; IP), 또는 다른 프로토콜 또는 프로토콜의 조합을 비롯한, 다양한 프로토콜 및 표준에 따라 통신 네트워크 상에서 송신될 수 있다. 통신 네트워크는, 연결된 컴퓨팅 디바이스 사이에서, 음성, 비디오, 생체 인식, 또는 인증 데이터, 또는 다른 정보를 송신할 수 있다.

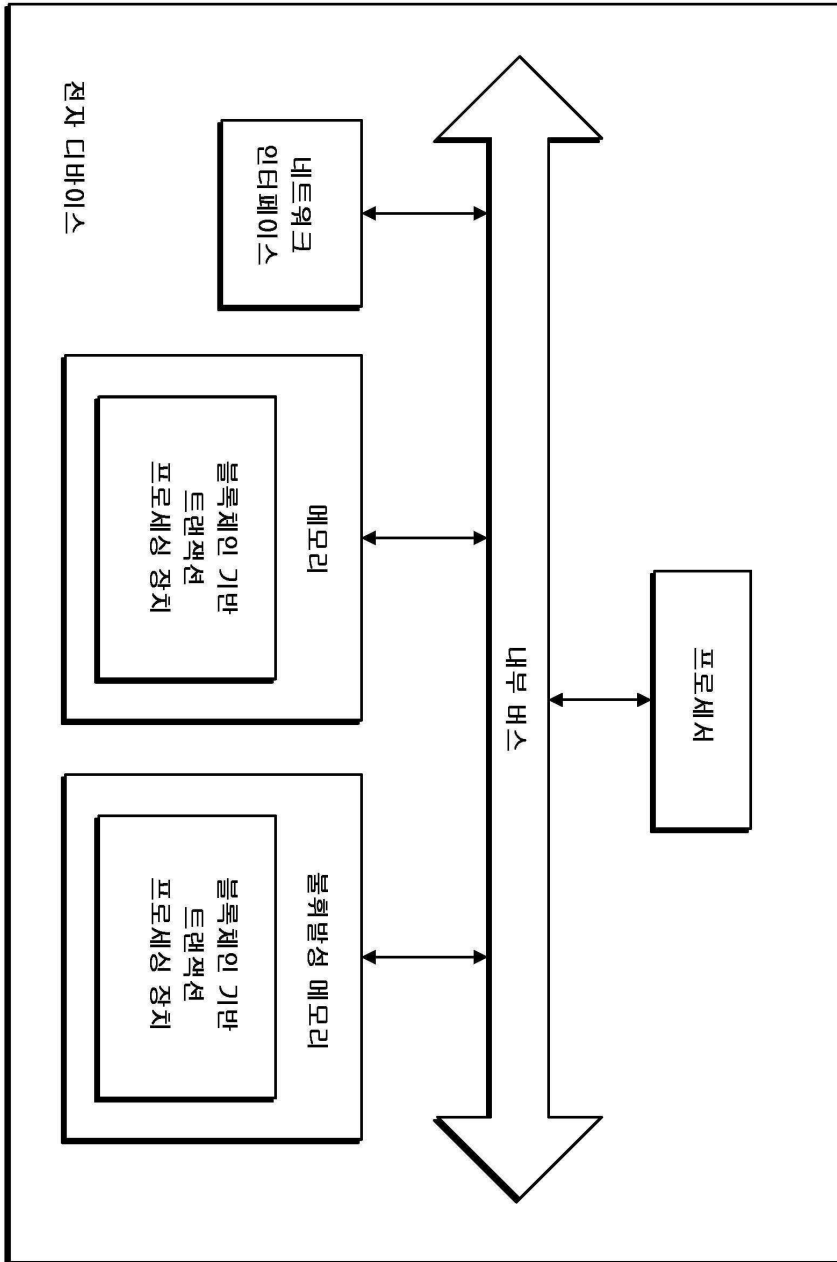
[0154] 별개의 구현예로서 설명되는 피처는, 조합하여, 단일의 구현예에서 구현될 수도 있고, 한편, 단일의 구현예로서 설명되는 피처는 다수의 구현예에서, 개별적으로, 또는 임의의 적절한 하위 조합으로 구현될 수도 있다. 특정한 순서로 설명되고 주장된 동작은 그 특정한 순서를 요구하는 것으로 이해되지 않아야 하고, 모든 예시된 동작이 수행되어야 한다는 것을 규정하는 것으로도 이해되지 않아야 한다(몇몇 동작은 옵션 사항일 수 있음). 적절히, 멀티태스킹 또는 병렬 프로세싱(또는 멀티태스킹과 병렬 프로세싱의 조합)이 수행될 수 있다.

**도면**

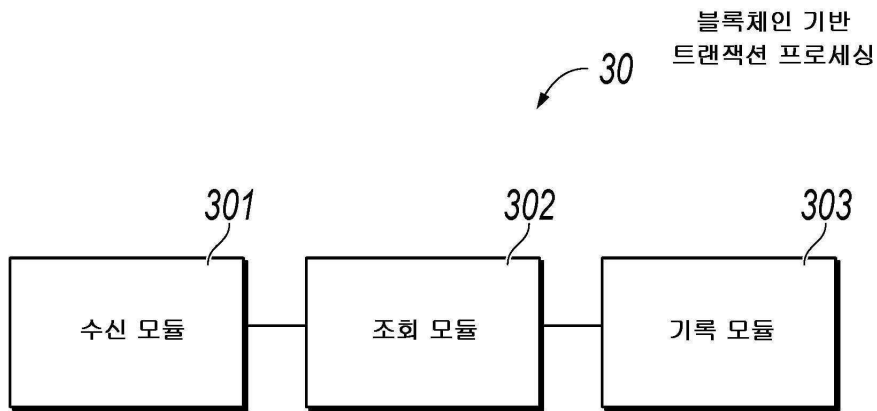
**도면1**



도면2



도면3



도면4

