(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0065470
(43) 공개일자 2020년06월09일

(51) 국제특허분류(Int. Cl.)
G06Q 30/06 (2012.01) *G06Q 10/10* (2012.01)
(52) CPC특허분류
G06Q 30/06 (2013.01)
G06Q 10/10 (2013.01)
(21) 출원번호 10-2018-0151987
(22) 출원일자 2018년11월30일
심사청구일자 없음

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
인호
서울특별시 용산구 이촌로88길 15, 3동 106호 (이촌동, 왕궁아파트)
박재용
서울특별시 송파구 송이로33길 7, 301호 (문정동)
(74) 대리인
특허법인엠에이피에스

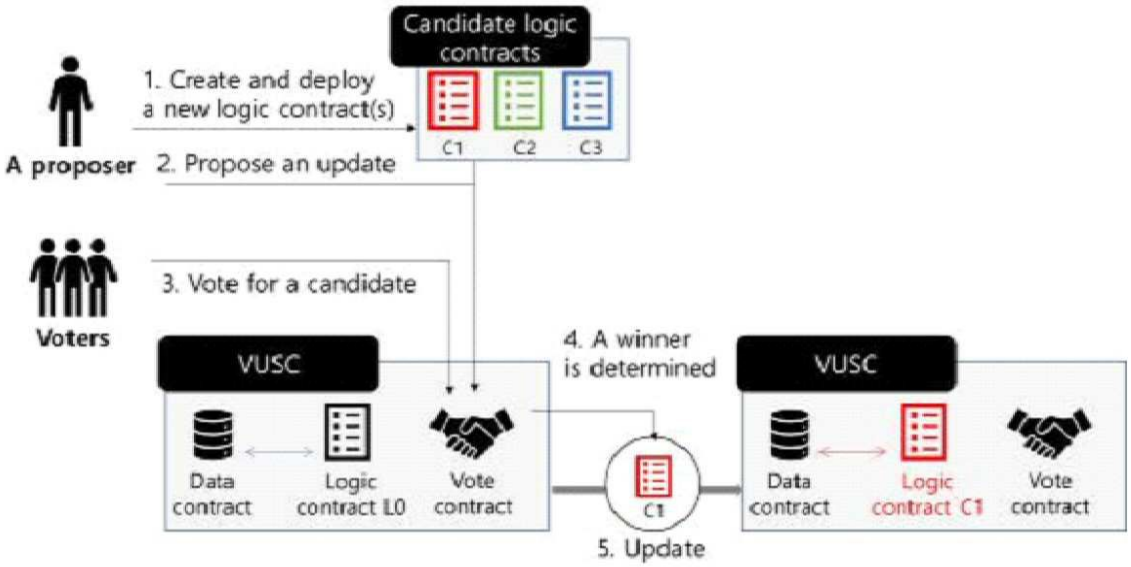
전체 청구항 수 : 총 2 항

(54) 발명의 명칭 **업그레이드 가능한 스마트 컨트랙트 방법**

(57) 요 약

본 발명은 업그레이드 가능한 스마트 컨트랙트 방법에 관한 것으로서, 이더리움에 기반하여 로직 컨트랙트의 업그레이드를 수행하는 업그레이드 가능한 스마트 컨트랙트 방법에 있어서, a) 상기 스마트 컨트랙트를 데이터 컨트랙트, 로직 컨트랙트, 투표 컨트랙트 및 프록시 컨트랙트로 분리하는 단계; b) 상기 로직 컨트랙트의 업그레이드 요청시, 네트워크 상에 사용자 단말을 통해 적어도 하나 이상의 로직 컨트랙트 후보를 배치하여 공개하는 단계; c) 적어도 하나 이상의 사용자 단말을 통해 새로운 로직 컨트랙트 후보에 대한 투표가 진행되고, 기설정된 투표 마감시간에 도달하면 득표 정보에 기초하여 업그레이드를 위한 새로운 로직 컨트랙트를 결정하는 단계; 및 d) 상기 새로운 로직 컨트랙트의 선출 시점 또는 기설정된 유예기간 이후에 이전의 로직 턴트랙트에서 새로운 로직 컨트랙트로 변경되어 로직 업그레이드를 온료하는 단계를 포함하는 것이다다.

대 표 도 - 도2



(52) CPC특허분류
H04L 9/06 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 20150009360041001
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 SW중심대학지원사업
연구과제명 SW중심대학 지원사업
기 여 율 1/1
주관기관 고려대학교 산학협력단
연구기간 2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

이더리움에 기반하여 로직 컨트랙트의 업그레이드를 수행하는 업그레이드 가능한 스마트 컨트랙트 방법에 있어서,

a) 상기 스마트 컨트랙트를 데이터 컨트랙트, 로직 컨트랙트, 투표 컨트랙트 및 프록시 컨트랙트로 분리하는 단계;

b) 상기 로직 컨트랙트의 업그레이드 요청시, 네트워크 상에 사용자 단말을 통해 적어도 하나 이상의 로직 컨트랙트 후보를 배치하여 공개하는 단계;

c) 적어도 하나 이상의 사용자 단말을 통해 새로운 로직 컨트랙트 후보에 대한 투표가 진행되고, 기설정된 투표 마감시간에 도달하면 득표 정보에 기초하여 업그레이드를 위한 새로운 로직 컨트랙트를 결정하는 단계; 및

d) 상기 새로운 로직 컨트랙트의 선출 시점 또는 기설정된 유예기간 이후에 이전의 로직 턴트랙트에서 새로운 로직 컨트랙트로 변경되어 로직 업그레이드를 온료하는 단계를 포함하는 것인, 업그레이드 가능한 스마트 컨트랙트 방법.

청구항 2

제 1 항에 있어서,

상기 c) 단계는,

사용자와 운영자간에 유권자 결정 기준, 투표 기간, 최소 득표 요구량을 포함한 투표 규칙을 결정하는 단계를 더 포함하는 것인, 업그레이드 가능한 스마트 컨트랙트 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은 사용자들간의 의사가 반영된 투표 결과에 의해 스마트 컨트랙트의 로직 업그레이드를 수행할 수 있는 업그레이드 가능한 스마트 컨트랙트 방법에 관한 것이다.

배 경 기 술

[0002] 스마트 컨트랙트(smart contract)는 블록체인 기반으로 금융거래, 부동산 계약, 공증 등 다양한 형태의 계약을 체결하고 이행하는 것으로서, 블록체인 2.0이라고도 한다. 또한, 이더리움(Ethereum)은 블록체인 기술을 기반으로 스마트 계약 기능을 구현하기 위한 분산 컴퓨팅 플랫폼이다. 이더리움이 제공하는 이더(Ether)는 비트코인과 마찬가지로 암호화폐의 일종으로 거래되고 있다.

[0003] 이더리움의 큰 특징중의 하나가 새로운 스마트 컨트랙트가 블록체인에 배포되면 해당 컨트렉트는 영구적으로 블록체인에 포함되어 변경되거나 지워지지 않는다는 점이다. 이러한 점이 이더리움의 탈중앙화된 데이터의 신뢰성을 나타내는 큰 이점이 될 수 있다. 하지만 이더리움에 서비스를 실행시키려는 개발자에게 있어서는 기능을 추가하거나 버그를 패치할 수 없는 제약이 된다.

[0004] 스마트 컨트랙트가 블록체인에 배치된 이후에 함수(logic)를 이용하여 컨트랙트의 데이터 접근 및 변경은 가능하지만, 컨트랙트의 함수 내용은 변경이 완전히 불가능하다. 이 특성 덕분에 스마트 컨트랙트에서는 신뢰할 수 없는 사용자들이 참여하여도 중재자 없이 동일한 데이터로 동일 로직을 실행할 수 있다. 즉, 탈중앙화 어플리케이션(decentralized application) 구현에 적합하지만, 함수 변경이 필요한 경우, 기존 컨트랙트를 폐기하고, 새로운 컨트랙트를 배치한 후 기존 데이터를 수동으로 다시 입력하는 방법 밖에 없다.

[0005] 업그레이드 가능한 스마트 컨트랙트는 다양한 방법으로 구현이 가능하지만, 데이터(data)와 로직(logic)을 각각 다른 컨트랙트로 분리하여 관리하는 것이다. 예를 들어, ERC20 토큰들은 컨트랙트 안에 토큰 이름, 발행량, 보

유 토큰 수 등의 데이터(data)들과, 트랜스퍼(transfer), 어푸르브(approve) 등과 같이 토큰 전송에 관여하는 함수(logic)들이 모두 같은 컨트랙트 안에 들어있다.

[0006] 그러나, 컨트랙트 내에서 함수(logic)만을 분리시킨다면, 이후 어떤 문제를 발견했을 때 문제가 발생한 함수(logic)만을 수정하여 새로 배포하는 방식으로 간단히 문제를 해결할 수 있게 된다.

[0007] 업그레이드 가능한 스마트 컨트랙트는 함수 변경을 위해 새로운 함수를 배치할 때, 기존 데이터를 새로운 로직에 자동으로 연결(승계)하게 해주는 방법이 필요하다. 이 방법에서는 데이터의 입출력 처리 함수와 같은 업그레이드가 필요 없는 함수와, 업그레이드가 자주 일어날 만한 일반 함수를 복수개의 컨트랙트들로 분리한다. 일반 로직 컨트랙트들의 주소(일종의 포인터)는 프록시 패턴이나 ENS(Ethereum Name Service)와 같은 주소 해석기(resolver)를 이용하여 관리한다. 함수를 업그레이드하기 위해 새로운 함수가 담긴 컨트랙트를 배치하면, 나머지 컨트랙트들은 자동으로 새로운 컨트랙트의 주소로 변경하게 된다.

[0008] 종래의 업그레이드가 가능한 스마트 컨트랙트 방법은 로직 업그레이드를 스마트 컨트랙트의 운영자(혹은 소유자)에 의해 수행되는데, 이는 탈중앙화 어플리케이션 구현에 부적합할 뿐만 아니라, 함수 업그레이드의 방향이 중앙에 의존적이고, 스마트 컨트랙트가 사유화될 여지가 있다는 문제점이 있다.

[0009] 또한, 스마트 컨트랙트는 암호화폐와 같은 디지털 자산이나 중요한 데이터를 보관하는데 많이 쓰이는데, 기존의 업그레이드 가능한 스마트 컨트랙트 방법에서는 운영자가 이를 노리는 악의적인 함수 업그레이드를 할 여지가 있다는 문제점이 있다.

[0010] 이를 해결하기 위해서, 업그레이드가 가능한 스마트 컨트랙트 방법은 운영자의 단독 결정에 의해서가 아닌 사용자들의 의견과 의사가 반영되는 함수 업그레이드 방법이 필요하다.

발명의 내용

해결하려는 과제

[0011] 본 발명은 전술한 문제점을 해결하기 위하여, 본 발명의 일 실시예에 따라 스마트 컨트랙트의 로직 업그레이드 수행시 중앙 제어, 즉 운영자의 단독 결정에 의해서 수행되는 것이 아니라 이해 관계자들의 합의를 통해 결정 및 변경할 수 있도록 하는 업그레이드 가능한 스마트 컨트랙트 방법을 제공하는 것에 목적이 있다.

[0012] 다만, 본 실시예가 이루고자 하는 기술적 과제는 상기된 바와 같은 기술적 과제로 한정되지 않으며, 또 다른 기술적 과제들이 존재할 수 있다.

과제의 해결 수단

[0013] 상기한 기술적 과제를 달성하기 위한 기술적 수단으로서 본 발명의 일 실시예에 따른 업그레이드 가능한 스마트 컨트랙트 방법은, 이더리움에 기반하여 로직 컨트랙트의 업그레이드를 수행하는 업그레이드 가능한 스마트 컨트랙트 방법에 있어서, a) 상기 스마트 컨트랙트를 데이터 컨트랙트, 로직 컨트랙트, 투표 컨트랙트 및 프록시 컨트랙트로 분리하는 단계; b) 상기 로직 컨트랙트의 업그레이드 요청시, 네트워크 상에 사용자 단말을 통해 적어도 하나 이상의 로직 컨트랙트 후보를 배치하여 공개하는 단계; c) 적어도 하나 이상의 사용자 단말을 통해 새로운 로직 컨트랙트 후보에 대한 투표가 진행되고, 기설정된 투표 마감시간에 도달하면 득표 정보에 기초하여 업그레이드를 위한 새로운 로직 컨트랙트를 결정하는 단계; 및 d) 상기 새로운 로직 컨트랙트의 선출 시점 또는 기설정된 유예기간 이후에 이전의 로직 턴트랙트에서 새로운 로직 컨트랙트로 변경되어 로직 업그레이드를 온료하는 단계를 포함하는 것이다.

발명의 효과

[0014] 전술한 본 발명의 과제 해결 수단에 의하면, 스마트 컨트랙트의 로직 업그레이드가 중앙 제어(운영자)에 의해 결정되는 것이 아니라 스마트 컨트랙트 이해관계자, 즉 사용자와 운영자들의 의사가 반영된 투표의 결과에 의해 이루어도록 함으로써 로직 업그레이드가 가능할 뿐만 아니라 스마트 컨트랙트의 탈중앙성 특징을 유지할 수 있다.

[0015] 또한, 본 발명은 처음부터 스마트 컨트랙트의 업그레이드를 설정할 필요 없이 필요시 이해관계자들의 합의를 통해 결정 및 변경할 수 있고, 운영자에 의한 스마트 컨트랙트의 사유화나 악의적인 로직 업그레이드를 방지할 수 있다.

도면의 간단한 설명

[0016] 도 1은 일반적인 스마트 컨트랙트 방법을 설명하는 도면이다.

도 2는 본 발명의 일 실시예에 따른 업그레이드 가능한 스마트 컨트랙트 방법을 구현하는 시스템 구조를 나타낸 도면이다.

도 3은 도 2의 스마트 콘트랙트의 세부 구성을 설명하는 도면이다.

발명을 실시하기 위한 구체적인 내용

[0017] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0018] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미하며, 하나 또는 그 이상의 다른 특징이나 숫자, 단계, 동작, 구성요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0019] 이하의 실시예는 본 발명의 이해를 돕기 위한 상세한 설명이며, 본 발명의 권리 범위를 제한하는 것이 아니다. 따라서 본 발명과 동일한 기능을 수행하는 동일 범위의 발명 역시 본 발명의 권리 범위에 속할 것이다.

[0020] 이하 첨부된 도면을 참고하여 본 발명의 일 실시예를 상세히 설명하기로 한다.

[0021] 도 1은 일반적인 스마트 컨트랙트 방법을 설명하는 도면이고, 도 2는 본 발명의 일 실시예에 따른 업그레이드 가능한 스마트 컨트랙트 방법을 구현하는 시스템 구조를 나타낸 도면이며, 도 3은 도 2의 스마트 콘트랙트의 세부 구성을 설명하는 도면이다.

[0022] 도 1 내지 도 3을 참조하면, 본 발명의 일 실시예에 따른 업그레이드 가능한 스마트 컨트랙트 방법은, 기존의 업그레이드 가능한 스마트 컨트랙트 방법에서 도 1에 도시된 바와 같이 컨트랙트를 로직 컨트랙트와 데이터 컨트랙트로 분리하였지만, 여기에 추가적으로 투표 컨트랙트와 프록시 컨트랙트를 추가한 것이다.

[0023] 도 3에 도시된 바와 같이, 투표 기반의 업그레이드 가능한 스마트 컨트랙트(Vote-based upgradeable smart contract, VUSC) 는 데이터 컨트랙트, 로직 컨트랙트, 투표 컨트랙트, 프록시 컨트랙트로 구분될 수 있고, 투표 컨트랙트는 로직 업그레이드에 대한 투표를 관리하고, 로직 컨트랙트는 old Logic, new Logic으로 나뉘어진다.

[0024] 또한, 업그레이드 가능한 컨트랙트 구조는 새로운 로직 컨트랙트가 배포되면 사용자 프로그램에서 실행하는 로직 컨트랙트의 주소도 변경된 주소로 실행해야 한다. 하지만 모든 사용자 프로그램내 설정된 컨트랙트의 주소를 변경하는 것은 쉬운 일이 아니다. 모든 사용자가 변경되기까지 배포 시간도 오래 걸릴 것이며, 그 전까지 기존 컨트랙트를 통한 사용자의 접근도 생기게 되기 때문에 두 가지의 로직 컨트랙트의 동작이 유지되게 해야만 한다.

[0025] 이를 해결하기 위해, 프록시 컨트랙트는 로직 컨트랙트를 프록시(Proxy) 형태로 변경한다. 따라서, 프록시 컨트랙트는 사용자가 실행시킨 함수 call을 그대로 로직 컨트랙트에 전달하는 역할을 수행한다.

[0026] 다시 도 2를 참조하면, 로직 업그레이드가 필요한 경우, 이해관계자가 하나 이상의 새로 대체할 로직 컨트랙트 후보를 네트워크에 배치하여 공개하고 (1. Create and deploy), 투표 컨트랙트를 통해 이에 대한 업그레이드를 제안한 후 투표를 시작한다(2. New logic contract).

[0027] 투표는 일정 마감시간까지 진행되며, 이해관계자들은 제안된 새로운 로직들 중에서 업그레이드 되기를 원하는 로직 컨트랙트 후보에 투표할 수 있고, 원하는 로직 컨트랙트 후보가 없다면 투표에 참여하지 않는다(3. Vote for candidate).

[0028] 투표는 이해관계자들의 합의에 따라 자율적으로 만들어진 투표 규칙을 따르는데, 투표 규칙은 유권자를 결정하는 기준, 투표 기간, 최소 득표 요구량 등이 포함될 수 있다.

[0029] 투표가 마감된 후, 특정한 로직 컨트랙트 후보가 선출된다(4.A winner is determined). 이때, 이해 관계자들이 합의에 따라 사전에 결정된 투표 규칙에 따라 로직 컨트랙트 후보가 선출되지 않을 수도 있다. 이 경우에는 로직 업그레이드가 취소된다.

[0030] 로직 컨트랙트는 후보 선출 시점 또는 후보 선출 시점부터 일정 유예기간 후에 선출된 로직 컨트랙트로 대체된다 (5. Update). 즉, 로직 컨트랙트의 주소 값이 원래의 로직 컨트랙트 주소(L0)에서 새 로직 컨트랙트의 주소(C1)로 바뀌면서 로직 업그레이드가 완료된다.

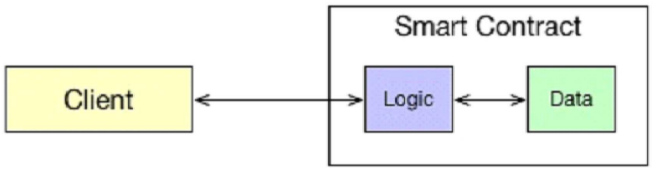
[0031] 이상에서 설명한 본 발명의 실시예에 따른 업그레이드 가능한 스마트 컨트랙트 방법은, 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 이러한 기록 매체는 컴퓨터 판독 가능 매체를 포함하며, 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체를 포함하며, 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다.

[0032] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

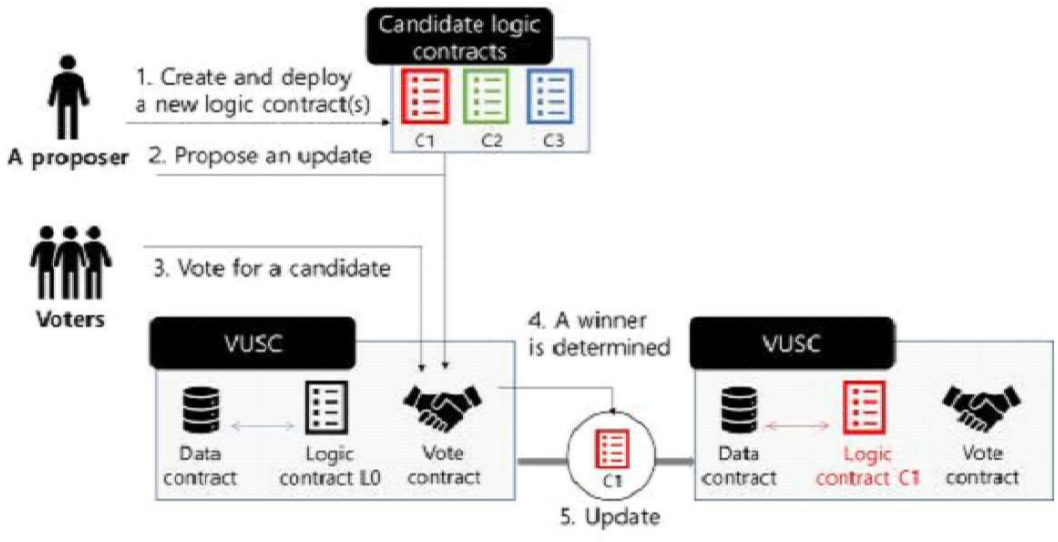
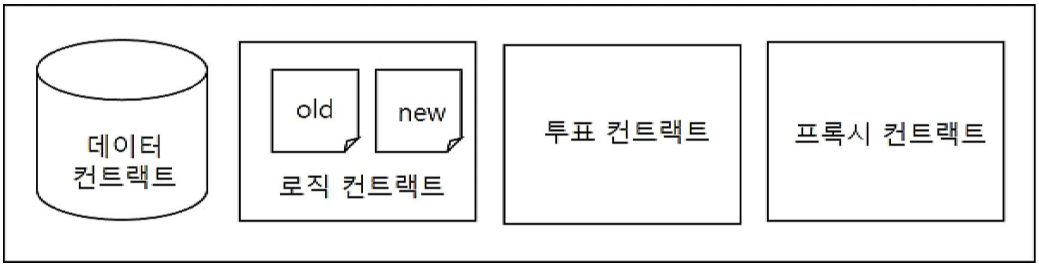
[0033] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면

도면1



도면2



도면3