(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0090369
(43) 공개일자 2020년07월29일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06K 19/06* (2006.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
G06K 19/06037 (2013.01)
(21) 출원번호 10-2019-0007310
(22) 출원일자 2019년01월21일
심사청구일자 2019년01월21일

(71) 출원인
주식회사 머니브레인
서울특별시 강남구 테헤란로8길 44, 5층 (역삼동)
(72) 발명자
이정대
서울특별시 송파구 송이로17길 46-20, 301호(가락동)
(74) 대리인
특허법인 신우

전체 청구항 수 : 총 8 항

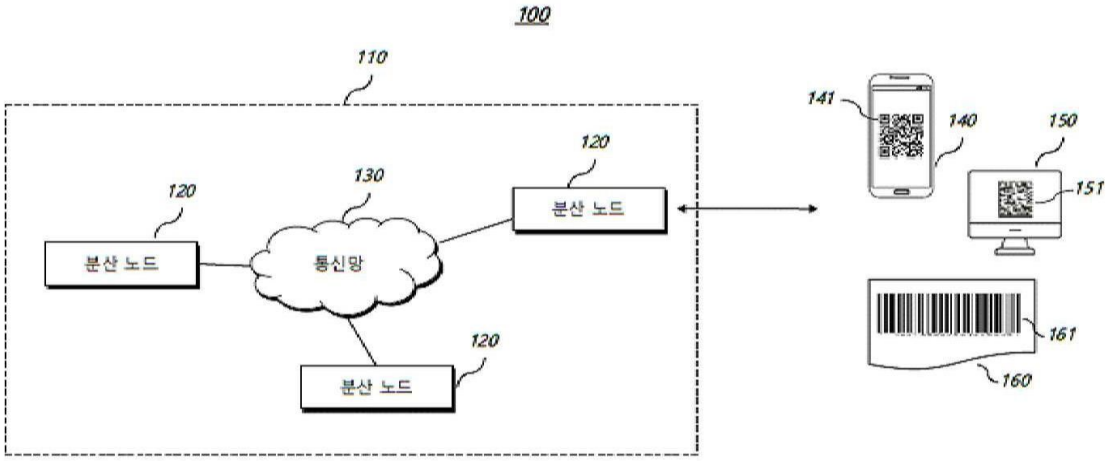
(54) 발명의 명칭 **블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법 및 장치**

(57) 요 약

블록체인에 기반하여 규격화된 패턴을 머클 트리(merkle tree) 구조로 인증하는 방법에 있어서, 규격화된 패턴을 입력 받는 단계; 상기 입력된 패턴을 복수의 단위 블록으로 분할하는 단계; 상기 복수의 단위 블록 중 n개의 검증 블록을 결정하는 단계; 상기 n개의 검증 블록으로부터 상기 입력된 패턴에 대한 n개의 머클 루트(merkle

(뒷면에 계속)

대 표 도



root) 값을 계산하는 단계; 및 상기 n개의 머클 루트 값 중 m개 이상이 블록체인 네트워크의 분산원장에 등록된 머클 루트 값과 동일하면, 상기 입력된 패턴을 인증하는 단계 - 상기 분산원장에 등록된 머클 루트는 상기 규격화된 패턴과 관련하여 기인증된 패턴으로부터 획득됨 - 를 포함하고, 상기 n개의 검증 블록 중 제1 검증 블록의 상기 입력된 패턴에 대한 제1 머클 루트 값은, 상기 제1 검증 블록의 비트스트림 및 상기 블록체인 네트워크의 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값(hash value)을 이용하여 획득되는 - 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값은 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록 중 상기 제1 검증 블록에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값임 -, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법이 개시된다.

(52) CPC특허분류

H04L 9/0643 (2013.01)

H04L 9/0836 (2013.01)

H04L 2209/38 (2013.01)

명 세 서

청구범위

청구항 1

블록체인에 기반하여 규격화된 패턴을 머클 트리(merkle tree) 구조로 인증하는 방법에 있어서,

규격화된 패턴을 입력 받는 단계;

상기 입력된 패턴을 복수의 단위 블록으로 분할하는 단계;

상기 복수의 단위 블록 중 n개의 검증 블록을 결정하는 단계;

상기 n개의 검증 블록으로부터 상기 입력된 패턴에 대한 n개의 머클 루트(merkle root) 값을 계산하는 단계; 및

상기 n개의 머클 루트 값 중 m개 이상이 블록체인 네트워크의 분산원장에 등록된 머클 루트 값과 동일하면, 상기 입력된 패턴을 인증하는 단계 - 상기 분산원장에 등록된 머클 루트는 상기 규격화된 패턴과 관련하여 기인증된 패턴으로부터 획득됨 -

를 포함하고,

상기 n개의 검증 블록 중 제1 검증 블록의 상기 입력된 패턴에 대한 제1 머클 루트 값은, 상기 제1 검증 블록의 비트스트림 및 상기 블록체인 네트워크의 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값(hash value)을 이용하여 획득되는 - 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값은 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록 중 상기 제1 검증 블록에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값임 -,

블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법.

청구항 2

제1항에 있어서, 상기 방법은,

상기 규격화된 패턴을 입력 받기 전에, 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록에 기초하여 상기 기인증된 패턴의 머클 경로 상의 적어도 하나의 토너먼트 해시 값 및 상기 기인증된 패턴의 머클 루트 값을 상기 블록체인 네트워크의 상기 분산원장에 등록하는 단계를 더 포함하는, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법.

청구항 3

제1항에 있어서, 상기 방법은,

상기 입력된 패턴을 복수의 블록으로 분할하기 전에, 상기 입력된 패턴의 방향 및 크기 중 적어도 하나를 상기 기인증된 패턴에 맞추어 정규화하는 단계를 더 포함하는, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법.

청구항 4

제1항에 있어서, 상기 제1 검증 블록의 비트스트림은,

미리 설정된 규칙에 따라 상기 제1 검증 블록을 이진화하여 획득되는, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법.

청구항 5

제1항에 있어서,

상기 규격화된 패턴은 가변 폭을 갖는 복수의 흑백 평형 막대의 조합 및 소정의 규칙에 따라 매트릭스(matrix) 형태로 배열된 정사각형 셀(cell)들의 조합 중 적어도 하나를 포함하는, 블록체인에 기반하여 규격화된 패턴을

머클 트리 구조로 인증하는 방법.

청구항 6

제1항에 있어서,

상기 규격화된 패턴은 QR(Quick Response) 코드를 포함하고,

상기 제1 검증 블록은 상기 QR 코드의 데이터 영역에 포함되는, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법.

청구항 7

제1항에 있어서,

상기 규격화된 패턴은 복수의 셀로 구성된 QR(Quick Response) 코드를 포함하고,

상기 복수의 단위 블록 중 일부는, 상기 QR 코드의 콰이어트 영역(Quiet Zone)의 셀을 포함하는, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법.

청구항 8

블록체인에 기반하여 규격화된 패턴을 머클 트리(merkle tree) 구조로 인증하는 분산 노드로서,

규격화된 패턴을 입력 받는 입력 모듈; 및

상기 입력된 패턴을 복수의 단위 블록으로 분할하고, 상기 복수의 단위 블록 중 n개의 검증 블록을 결정하고, 상기 n개의 검증 블록으로부터 상기 입력된 패턴에 대한 n개의 머클 루트(merkle root) 값을 계산하고, 상기 n개의 머클 루트 값 중 m개 이상이 블록체인 네트워크의 분산원장에 등록된 머클 루트 값과 동일하면, 상기 입력된 패턴을 인증하는 패턴 인증 모듈 - 상기 분산원장에 등록된 머클 루트는 상기 규격화된 패턴과 관련하여 기인증된 패턴으로부터 획득됨 -

을 포함하고,

상기 n개의 검증 블록 중 제1 검증 블록의 상기 입력된 패턴에 대한 제1 머클 루트 값은, 상기 제1 검증 블록의 비트스트림 및 상기 블록체인 네트워크의 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값(hash value)을 이용하여 획득되는 - 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값은 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록 중 상기 제1 검증 블록에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값임 -,

블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 분산 노드.

발명의 설명

기 술 분 야

[0001] 본 발명은 규격화된 패턴을 인증하는 방법 및 장치에 관한 것으로, 구체적으로는 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 2009년 나카모토 사토시가 암호화폐 비트코인을 통해 블록체인 기술을 세상에 선보인 이래 다양한 형태의 암호화폐들과 이들을 뒷받침하는 블록체인 기술에 관한 관심이 점점 더 뜨거워지고 있다. 블록체인 기술은, 탈 중앙화된 분산형 공유 원장 방식에 기초한 거래를 가능하게 하여, 높은 개방성, 신뢰성, 투명성, 및 상호작용성 등을 제공한다는 점에서, 다양한 분야에서 그 응용 가능성이 검토되고 있다.

[0003] 블록체인에는 해시 함수(hash function) 및 머클 트리(merkel tree) 등의 기술이 핵심적으로 사용되고 있다. 해시 함수 및 머클 트리 모두 데이터를 효율적이고 안전하게 압축할 수 있다는 특징을 갖고 있다. 구체적으로, 해시 함수는 어떤 형태의 데이터든 입력 데이터의 길이와 상관없이 고정된 길이의 비트스트림을 출력할 수 있는 함수이며, 출력 값으로부터 입력 값을 추론 또는 복원하기가 사실상 불가능하다는 특징이 있어, 데이터 압축 및 보안에 적합한 기술이다. 머클 트리는 해시 함수를 계층적으로 적용하여 블록체인의 트랜잭션들을 압축할 수 있

는 데이터 구조 기술로, 머클 트리 구조를 이용하면 트랜잭션의 위변조를 효율적으로 검증할 수 있다.

[0004] 한편, 많은 정보를 효율적으로 처리하기 위하여, 다양한 형태의 규격화된 패턴들이 개발되어 왔다. 예를 들어, DENSO WAVE INCORPORATED에 의해 개발된 QR 코드는, 종래의 바코드(barcode)에 비하여 수십배 내지 수백배의 정보량을 취급할 수 있는 2차원 이미지이다. 시장의 요구에 따라 Micro QR 코드와 같이 아주 작은 공간에도 부착할 수 있는 형태의 QR 코드가 개발되기도 하였지만, 반대로 최대 가로 422셀(cell) 세로 422셀로 구성되어, 4만 자리의 숫자까지 취급 가능한 iQR 코드가 개발되기도 하였다. 이외에도, 의약품 표준코드 및 의료기기 표준코드와 같이, GS1 체계에 따라 상품 및 거래처의 식별과 유통 및 거래정보의 교환을 위한 국제표준 식별코드, 국제표준 바코드 등이 개발되었다.

[0005] 많은 정보량을 용이하게 취급할 수 있는 규격화된 패턴들이 널리 활용되면서, 이를 활용하여 일반 소비자에게 악성 어플리케이션을 유포하는 방법과 같이, 새로운 방식의 금융 사기가 탄생하였다. 이에 따라, 규격화된 패턴의 위변조를 차단하고, 취급할 수 있는 정보량을 증가시킬 수 있는 기술에 대한 수요가 늘어나고 있다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) 일본등록특허 JP2938338

비특허문헌

[0007] (비특허문헌 0001) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2009.

발명의 내용

해결하려는 과제

[0008] 본 발명은, 대용량의 규격화된 패턴을 효율적으로 압축하면서도, 규격화된 패턴의 위변조를 검증할 수 있는 기술을 제공하여, 전술한 바와 같은 신종 금융 사기를 방지하고자 한다.

과제의 해결 수단

[0009] 본 발명의 일 실시예에 따르면, 블록체인에 기반하여 규격화된 패턴을 머클 트리(merkle tree) 구조로 인증하는 방법에 있어서, 규격화된 패턴을 입력 받는 단계; 상기 입력된 패턴을 복수의 단위 블록으로 분할하는 단계; 상기 복수의 단위 블록 중 n개의 검증 블록을 결정하는 단계; 상기 n개의 검증 블록으로부터 상기 입력된 패턴에 대한 n개의 머클 루트(merkle root) 값을 계산하는 단계; 및 상기 n개의 머클 루트 값 중 m개 이상이 블록체인 네트워크의 분산원장에 등록된 머클 루트 값과 동일하면, 상기 입력된 패턴을 인증하는 단계 - 상기 분산원장에 등록된 머클 루트는 상기 규격화된 패턴과 관련하여 기인증된 패턴으로부터 획득됨 - 를 포함하고, 상기 n개의 검증 블록 중 제1 검증 블록의 상기 입력된 패턴에 대한 제1 머클 루트 값은, 상기 제1 검증 블록의 비트스트림 및 상기 블록체인 네트워크의 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값(hash value)을 이용하여 획득되는 - 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값은 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록 중 상기 제1 검증 블록에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값임 -, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법이 개시된다.

[0010] 상술한 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법은 상기 규격화된 패턴을 입력 받기 전에, 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록에 기초하여 상기 기인증된 패턴의 머클 경로 상의 적어도 하나의 토너먼트 해시 값 및 상기 기인증된 패턴의 머클 루트 값을 상기 블록체인 네트워크의 상기 분산원장에 등록하는 단계를 더 포함할 수 있다.

[0011] 상술한 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법은, 상기 입력된 패턴을 복수의 블록으로 분할하기 전에, 상기 입력된 패턴의 방향 및 크기 중 적어도 하나를 상기 기인증된 패턴에 맞추어 정규화하는 단계를 더 포함할 수 있다.

[0012] 상술한 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법에 있어서, 상기 제1 검증 블록의 비트스트림은 미리 설정된 규칙에 따라 상기 제1 검증 블록을 이진화하여 획득될 수 있다.

[0013] 상술한 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법은, 상기 규격화된 패턴은 가변 폭을 갖는 복수의 흑백 평형 막대의 조합 및 소정의 규칙에 따라 매트릭스(matrix) 형태로 배열된 정사각형 셀(cell)들의 조합 중 적어도 하나를 포함할 수 있다.

[0014] 상술한 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법에 있어서, 상기 규격화된 패턴은 QR(Quick Response) 코드를 포함하고, 상기 제1 검증 블록은 상기 QR 코드의 데이터 영역에 포함될 수 있다.

[0015] 상술한 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법에 있어서, 상기 규격화된 패턴은 복수의 셀로 구성된 QR(Quick Response) 코드를 포함하고, 상기 복수의 단위 블록 중 일부는, 상기 QR 코드의 콰이어트 영역(Quiet Zone)의 셀을 포함할 수 있다.

[0016] 본 발명의 일 실시에에 따르면, 블록체인에 기반하여 규격화된 패턴을 머클 트리(merkle tree) 구조로 인증하는 분산 노드로서, 규격화된 패턴을 입력 받는 입력 모듈; 및 상기 입력된 패턴을 복수의 단위 블록으로 분할하고, 상기 복수의 단위 블록 중 n개의 검증 블록을 결정하고, 상기 n개의 검증 블록으로부터 상기 입력된 패턴에 대한 n개의 머클 루트(merkle root) 값을 계산하고, 상기 n개의 머클 루트 값 중 m개 이상이 블록체인 네트워크의 분산원장에 등록된 머클 루트 값과 동일하면, 상기 입력된 패턴을 인증하는 패턴 인증 모듈 - 상기 분산원장에 등록된 머클 루트는 상기 규격화된 패턴과 관련하여 기인증된 패턴으로부터 획득됨 - 을 포함하고, 상기 n개의 검증 블록 중 제1 검증 블록의 상기 입력된 패턴에 대한 제1 머클 루트 값은, 상기 제1 검증 블록의 비트스트림 및 상기 블록체인 네트워크의 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값(hash value)을 이용하여 획득되는 - 상기 분산원장에 등록된 적어도 하나의 토너먼트 해시 값은 상기 기인증된 패턴으로부터 분할된 복수의 단위 블록 중 상기 제1 검증 블록에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값임 -, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 분산 노드가 개시된다.

발명의 효과

[0017] 본 발명에 의하면, 규격화된 패턴의 위변조 여부를 빠르게 검증할 수 있으며, 대용량의 규격화된 패턴을 효율적으로 압축할 수 있다. 따라서, 본 발명에 의하면, 일반 사용자들이 QR 코드와 같은 규격화된 패턴을 안전하게 사용할 수 있는 환경을 제공할 수 있다.

[0018] 또한, 본 발명에 의하면, 규격화된 패턴을 블록체인 네트워크의 분산 노드에서 직접 인증할 수 있어, 인증을 위한 중앙 집중형 서버가 필요하지 않다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 시스템의 구성을 개략적으로 도시한다.

도 2는 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 분산 노드의 개략적인 블록도이다.

도 3은 본 발명의 일실시예에 따른, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 분사 노드에 저장될 수 있는, 블록체인 및 그에 포함된 각 블록의 구성을 개념적으로 도시한 도면이다.

도 4는 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법을 개략적으로 설명하기 개념도이다.

도 5는 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법의 흐름도이다.

도 6은 본 발명의 일 실시예에 따라 블록체인에 기반하여 QR 코드를 머클 트리 구조로 인증하기 위하여, QR 코드를 단위 블록으로 분할하는 동작을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하, 첨부 도면을 참조하여 본 개시의 실시예에 관하여 상세히 설명한다. 이하에서는, 본 개시의 요지를 불필요하게 흐릴 우려가 있다고 판단되는 경우, 이미 공지된 기능 및 구성에 관한 구체적인 설명을 생략한다. 또한,

이하에서 설명하는 내용은 어디까지나 본 개시의 일 실시예에 관한 것일 뿐 본 개시가 이로써 제한되는 것은 아님을 알아야 한다.

[0021] 본 개시에서 사용되는 용어는 단지 특정한 실시예를 설명하기 위해 사용되는 것으로 본 개시를 한정하려는 의도에서 사용된 것이 아니다. 예를 들면, 단수로 표현된 구성요소는 문맥상 명백하게 단수만을 의미하지 않는다면 복수의 구성요소를 포함하는 개념으로 이해되어야 한다. 본 개시에서 사용되는 "및/또는"이라는 용어는, 열거되는 항목들 중 하나 이상의 항목에 의한 임의의 가능한 모든 조합들을 포괄하는 것임이 이해되어야 한다. 본 개시에서 사용되는 '포함하다' 또는 '가지다' 등의 용어는 본 개시 상에 기재된 특징, 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것이 존재함을 지정하려는 것일 뿐이고, 이러한 용어의 사용에 의해 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성 요소, 부분품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 배제하려는 것은 아니다.

[0022] 본 개시의 실시예에 있어서 '모듈' 또는 '부'는 적어도 하나의 기능이나 동작을 수행하는 기능적 부분을 의미하며, 하드웨어 또는 소프트웨어로 구현되거나 하드웨어와 소프트웨어의 결합으로 구현될 수 있다. 또한, 복수의 '모듈' 또는 '부'는, 특정한 하드웨어로 구현될 필요가 있는 '모듈' 또는 '부'를 제외하고는, 적어도 하나의 소프트웨어 모듈로 일체화되어 적어도 하나의 프로세서에 의해 구현될 수 있다.

[0023] 덧붙여, 달리 정의되지 않는 한 기술적 또는 과학적인 용어를 포함하여, 본 개시에서 사용되는 모든 용어들은 본 개시가 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가진다. 일반적으로 사용되는 사전에 정의된 용어들은, 관련 기술의 문맥상 의미와 일치하는 의미를 갖는 것으로 해석되어야 하며, 본 개시에서 명백하게 달리 정의하지 않는 한 과도하게 제한 또는 확장하여 해석되지 않는다는 점을 알아야 한다.

[0024] 이하, 첨부된 도면을 참조하여, 본 개시의 실시예에 대해 구체적으로 설명하기로 한다.

[0025] 도 1은 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 시스템의 구성을 개략적으로 도시한다.

[0026] 도시된 바에 의하면, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 시스템(100)은, 블록체인 네트워크(110) 및 규격화된 패턴을 제공하는 외부 기기(140, 150) 또는 규격화된 패턴의 인쇄물(160) 등을 포함하고, 블록체인 네트워크(110)는 복수의 분산 노드(120) 및 통신망(130)을 포함한다.

[0027] 본 개시의 일 실시예에 의하면, 블록체인 네트워크(110)는 통신망(130)을 통하여 서로 연결된 복수의 분산 노드(120)를 포함하는 임의의 유선 또는 무선 통신망일 수 있다. 본 개시의 일 실시예에 의하면, 블록체인 네트워크(110)는, 예컨대 TCP/IP 통신망 상에 구현된 P2P 분산 네트워크를 포함할 수 있다. 본 개시의 일 실시예에 의하면, 블록체인 네트워크(110)는, 예컨대 Wi-Fi망, LAN망, WAN망, 인터넷망 등에 구현된 P2P 네트워크일 수 있으며, 다만 본 개시가 이로써 제한되는 것은 아니다. 본 개시의 일 실시예에 의하면, 블록체인 네트워크(110)는, 퍼블릭 블록체인 네트워크, 즉 제한 없이 모든 사용자가 참여할 수 있는 블록체인 네트워크(예컨대, 이더리움 네트워크 등)일 수 있으며, 다만 본 개시가 이로써 제한되는 것은 아니다.

[0028] 본 개시의 일 실시예에 의하면, 블록체인 네트워크(110)의 각 분산 노드(120)는 통신망(130)을 통하여 다른 분산 노드로부터 배포된 각 블록체인 트랜잭션을 수신 및 처리할 수 있다. 본 개시의 일 실시예에 의하면, 각각의 분산 노드(120)는, 수신된 트랜잭션 상의 프로그램 코드(예컨대, 소정의 스마트 계약에 관한 프로그램 코드)를 실행할 수 있다.

[0029] 본 개시의 일 실시예에 의하면, 복수의 분산 노드(120) 각각은, 소정의 알고리즘에 따라, 블록체인 네트워크(110) 상의 각 블록체인 트랜잭션의 기록을 위한 블록을 생성(또는 채굴) 및/또는 검증할 수 있다. 본 개시의 일 실시예에 의하면, 소정의 시간 간격 동안에 각 분산 노드(120)를 통하여 블록체인 네트워크(110) 상에 배포된 블록체인 트랜잭션들은, 새로이 생성된 블록에 함께 저장될 수 있다. 본 개시의 일 실시예에 의하면, 분산 노드(120) 각각은, 소정의 알고리즘에 따라, 블록체인 네트워크(110)를 위한 블록체인(즉, 블록체인 분산 원장)의 적어도 일부를 저장할 수 있다.

[0030] 본 개시의 일 실시예에 의하면, 복수의 분산 노드(120) 각각은, 블록체인의 분산원장에 등록된 트랜잭션 정보를 이용하여, 규격화된 패턴을 인증할 수 있다. 예를 들어, 분산 노드(120)는 결제 및 송금과 같이 금융 거래를 진행하기 위하여, 외부 기기(140)에 제공된 QR 코드(141), GS1 Datamatrix 체계에 따라 외부 기기(150)에 제공된 의약품 표준코드(151), GS1-128 체계에 따라 인쇄물(160)에 제공된 의료기기 바코드(161) 등과 같은 규격화된 패턴을 분산원장 상에 압축 저장된 기인증 패턴 정보와 비교하여, 외부 기기(140, 150) 또는 인쇄물(160)에 제

공된 규격화된 패턴의 위변조 여부를 판단할 수 있다. 분산 노드(120)가 규격화된 패턴을 인증하는 방법에 대해서는, 이하 도 4 내지 도 6을 참조하여 상세히 설명한다.

[0031] 도 2는 본 발명의 일 실시예에 따른 블록체인 네트워크의 분산 노드의 개략적인 블록도이다. 분산 노드는 컴퓨팅 동작을 수행할 수 있는 장치로서, PC, 노트북, 스마트폰, 태블릿 등으로 구현될 수 있으나 이에 한정되지 않는다.

[0032] 도시된 바에 의하면, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 분산 노드(120)는, 트랜잭션 처리 모듈(202), 통신 모듈(204), 블록 생성/검증 모듈(206), 및 블록체인 분산원장 저장 모듈(208)을 포함한다.

[0033] 본 개시의 일 실시예에 의하면, 트랜잭션 처리 모듈(202)은 블록체인 네트워크(110) 상의 다른 분산 노드들(120)에 의해 배포된 각 트랜잭션을 수신할 수 있다. 본 개시의 일 실시예에 의하면, 트랜잭션 처리 모듈(202)은, 수신된 각 트랜잭션을 처리(예컨대, 트랜잭션에 포함된 각 스마트 계약의 실행 등을 포함하며, 다만 본 개시가 이로써 제한되는 것은 아님)할 수 있다. 본 개시의 일 실시예에 의하면, 트랜잭션 처리 모듈(202)에 의해 수신 및 처리되는 블록체인 트랜잭션은, 예컨대 외부 기기(140, 150) 또는 인쇄물(160)로부터 유래한 규격화된 패턴과 연관된 트랜잭션을 포함할 수 있다. 구체적으로, 블록체인 트랜잭션은, 도 4 내지 도 6을 통해 후술할 바와 같이, 기인증된 패턴과 관련하여 기인증된 패턴으로부터 획득된 머클 루트 및 머클 경로 상의 토너먼트 해시 값 등을 포함할 수 있다. 본 개시의 일 실시예에 의하면, 트랜잭션 처리 모듈(202)에 의해 수신 및 처리되는 트랜잭션은, 임의의 분산 노드(120)에 의해서 블록체인 네트워크(110) 상의 각 분산 노드들에 배포된, 블록체인 네트워크(110)를 통하여 처리될 기타 다양한 트랜잭션(예컨대, 해당 블록체인 네트워크(110) 상에서 지원되는 디지털 화폐의 거래 정보 또는 기타 스마트 계약 정보를 포함한 트랜잭션 등을 포함하며, 본 개시가 이로써 제한되지 않음)을 포함할 수 있다.

[0034] 본 개시의 일 실시예에 의하면, 통신 모듈(204)은, 분산 노드(120)가 블록체인 네트워크(110) 상에서 소정의 프로토콜에 따라 다른 분산 노드들(120)과 통신할 수 있도록 동작할 수 있다. 본 개시의 일 실시예에 의하면, 통신 모듈(204)은, 블록체인 트랜잭션이 소정의 프로토콜에 따라 통신망(134)을 통해 블록체인 네트워크(110) 상에 배포되도록 할 수 있고, 아울러 통신망(134)을 통하여 다른 노드들(120)로부터 블록체인 네트워크(110) 상의 각종 정보를 수신하도록 할 수 있다.

[0035] 본 개시의 일 실시예에 의하면, 블록 생성/검증 모듈(206)은, 블록체인 네트워크(110)를 위한 블록을 생성하고, 소정의 시간 간격 동안 블록체인 네트워크(110) 상에서 발생한 트랜잭션들을 모아서 적절한 헤더 정보와 함께 그 생성된 블록에 기록할 수 있다. 본 개시의 일 실시예에 의하면, 블록 생성/검증 모듈(206)은, 생성된 블록을 통신 모듈(204)을 통하여 블록체인 네트워크(110) 상에 공지할 수 있다. 본 개시의 일 실시예에 의하면, 블록 생성/검증 모듈(206)은, 블록체인 네트워크(110) 상에 공지된, 다른 분산 노드(120)에 의하여 생성된 블록에 대한 검증을 수행할 수 있다.

[0036] 본 개시의 일 실시예에 의하면, 블록체인 분산원장 저장 모듈(208)은, 소정의 알고리즘에 따라, 블록체인 네트워크(110)를 위한 블록체인 데이터베이스(즉, 트랜잭션들의 이력을 모두 포함하는 분산 원장)의 적어도 일부를 저장할 수 있다. 본 개시의 일 실시예에 의하면, 블록체인 분산원장 저장 모듈(208)은, 또한, 소정의 알고리즘에 따라, 블록체인 네트워크(110) 상의 블록체인에 의해 유지 및 관리되는 스마트 계약에 관한 정보의 적어도 일부를 저장할 수 있으며, 다만 본 개시가 이로써 제한되는 것은 아니다.

[0037] 본 개시의 일 실시예에 의하면, 입력 모듈(210)은, 외부로부터 규격화된 패턴을 입력 받을 수 있다. 예를 들어, 입력 모듈(210)은 카메라 및 적외선 센서 중 적어도 하나를 포함하여, 외부 기기(140, 150)의 디스플레이 또는 앤쇄물(160)에 제공된 규격화된 패턴을 촬영하거나 인식할 수 있다.

[0038] 본 개시의 일 실시예에 의하면, 통신 모듈(204)이 외부 기기(140, 150)와 통신하여 규격화된 패턴을 직접 입력받을 수 있으며, 이 경우, 분산 노드(120)에는 별도의 입력 모듈(210)이 존재하지 않을 수 있다.

[0039] 본 개시의 일 실시예에 의하면, 패턴 인증 모듈(212)은, 입력 모듈(210) 또는 통신 모듈(204)을 통해 입력된 QR 코드를 복수의 단위 블록으로 분할하고, 분할된 단위 블록 중 일부를 검증 블록으로 결정할 수 있다. 예를 들어, 패턴 인증 모듈(212)은 n개의 단위 블록을 검증 블록으로 결정할 수 있고, n 개의 검증 블록 각각으로부터 입력된 패턴에 대한 머클 루트 값을 계산하여, 계산된 n개의 머클 루트 값 중 m개 이상이 블록체인 분산 원장 저장 모듈(208)에 저장된 기인증된 패턴에 대한 머클 루트 값과 동일하면, 입력된 패턴을 인증할 수 있다. 반면, 계산된 n개의 머클 루트 값 중 블록체인 분산 원장 저장 모듈(208)에 저장된 기인증된 패턴에 대한 머클

루트 값과 동일한 값이 m개 미만인 경우, 패턴 인증 모듈(212)은 입력된 패턴이 위변조된 것으로 판단할 수 있다.

[0040] 도 2에 개시된 모든 구성요소가 분산 노드(120)의 필수적인 구성이 아닐 수 있으며, 분산 노드(120)는 도 2에 개시되지 않은 구성요소도 포함할 수 있다. 예를 들어, 트랜잭션 처리 모듈(202), 블록 생성/검증 모듈(206), 블록체인 분산 원장 저장 모듈(208), 패턴 인증 모듈(212)은 단일 프로세서 혹은 복수의 프로세서로 구현될 수 있으며, 전술한 바와 같이 분산 노드(120)는 별도의 입력 모듈(210)을 포함하지 않을 수 있다. 또한, 분산 노드(120)는 트랜잭션 처리 정보를 표시하기 위한 디스플레이를 더 포함할 수 있다.

[0041] 도 3은 본 발명의 일실시예에 따른, 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 분산 노드에 저장될 수 있는, 블록체인 및 그에 포함된 각 블록의 구성을 개념적으로 도시한 도면이다.

[0042] 도시된 바에 의하면, 블록체인은 복수의 블록을 포함하며, 각 블록(300)은 블록 헤더(302)와 복수의 트랜잭션 정보(304a-304n)를 포함할 수 있다.

[0043] 본 개시의 일 실시예에 의하면, 블록 헤더(302)는, 이전 블록 헤더의 해시(hash) 값, 넌스(nonce) 값, 해당 블록(300)에 포함될 트랜잭션 정보들(304a-304n)의 머클루트, 블록(300)이 생성된 시간을 나타내는 타임스탬프, 해당 블록(300)의 채굴 난이도 등의 값을 포함할 수 있다. 본 개시의 일 실시예에 의하면, 블록(300)에 포함된 복수의 트랜잭션 정보(304a-304n)는, 소정의 시간 간격 동안, 도 1의 분산 노드들(132)로부터 블록체인 네트워크(130) 상에 배포된 복수의 트랜잭션 기록들일 수 있다. 본 개시의 일 실시예에 의하면, 블록(300)의 트랜잭션 정보(304a-304n)는, 블록체인 네트워크(130) 상에서 발생한 각 거래 기록(예컨대, 기인증된 패턴에 대한 머클 경로 상의 토너먼트 해시 값 및 머클 루트 값, 소정의 디지털 암호 화폐의 거래에 관한 기록 등)에 관한 트랜잭션 정보를 포함할 수 있다.

[0044] 도 4는 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법을 개략적으로 설명하기 개념도이다.

[0045] 분산 노드(120)는 외부 기기(140)에 제공된 QR 코드(400)를 촬영할 수 있다. 도시된 바와 같이, 분산 노드(120)는 촬영된 QR 코드(400)의 크기(즉, 촬영된 QR 코드에 포함된 셀의 개수)에 따라 단위 블록의 크기를 결정하고, QR 코드(400)를 결정된 크기의 단위 블록들로 분할할 수 있다.

[0046] 분산 노드(120)는 QR 코드(400)로부터 분할된 단위 블록들을 머클 트리 구조에 적용하였을 때 계산된 머클 루트 값(Merkel Root C1)을 기인증된 패턴에 기초하여 분산원장 상에 등록된 머클 루트 값(Merkel Root R1)과 비교하여, 촬영된 QR 코드(400)를 인증할 수 있다.

[0047] 구체적으로, 분산 노드(120)는 촬영된 QR 코드(400)로부터 분할된 단위 블록들(410) 중, 일부의 단위 블록을 검증 블록(420)으로 결정하고, 검증 블록(420)을 이진화하여, 검증 블록(420)의 비트스트림(0110110…)을 생성하고, 검증 블록(420)의 비트스트림(0110110…)에 해시 함수를 적용하여, 검증 블록(420)의 비트스트림(0110110…)에 대한 해시 값(hash C1)을 획득할 수 있다. 해시 함수로는, SHA-256과 같이 공지된 알고리즘을 이용할 수 있다.

[0048] 분산 노드(120)는 촬영된 QR 코드(400)와 관련하여 기인증된 QR 코드로부터 획득한 머클 루트 값(Merkel Root R1)을 분산원장 상에 트랜잭션으로 저장하고 있을 수 있다. 또한, 분산 노드(120)는 촬영된 QR 코드(400)와 관련하여 기인증된 QR 코드로부터 분할된 단위 블록 중, 검증 블록(420)에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값(hash R1, hash R2, hash R3)을 분산원장 상에 트랜잭션으로 저장하고 있을 수 있다.

[0049] 분산 노드(120)는 검증 블록(420)의 해시 값(hash C1)을 머클 트리 구조에 있어서 최하위 계층인 리프(leaf) 해쉬 값으로 설정하고, 분산원장 상에 등록된 단계별 토너먼트 해시 값(hash R1, hash R2, hash R3)에 기초하여, 검증 블록(420)의 해시 값(hash C1)으로부터 촬영된 QR 코드(400)에 대한 머클 트리 구조에 있어서 최상위 계층인 머클 루트 값(Merkel Root C1)을 계산할 수 있다.

[0050] 도시된 바와 같이, '머클 경로'란 머클 트리 구조의 최하위 해시 값(예를 들어, 검증 블록(420)의 해시 값(hash C1))으로부터 머클 트리 구조의 최상위 해시 값인 머클 루트 값(예를 들어, 촬영된 QR 코드(400)의 머클 루트 값(Merkel Root C1))을 획득하기 위한 계산 과정을 의미할 수 있다. 또한, '토너먼트 해시 값'이란, 머클 루트 상에서 각 단계마다 필요한 계층적 해시 함수의 상대 인자를 의미할 수 있다. 예를 들어, 분산 노드(120)는 검증 블록(420)의 해시 값(hash C1)과 인접한 블록(430)의 해시 값(hash R1)을 결합한 값에 해시 함수를 적용하여 다음 단계의 해시 값(hash C2)을 획득할 수 있다.

[0051] 이와 같이, 임의의 리프 해시 값으로부터, 머클 경로 상의 토너먼트 해시 값만을 이용하여 머클 루트 값(Merkel Root C1)을 계산하면, 머클 트리 구조의 다른 리프 해시 값이나 머클 경로 상에 포함되지 않은 계층적 해시 값들을 참조하지 않아도 되므로 계산 속도를 더욱 향상시킬 수 있다. 따라서, 분산 노드(120)는 규격화된 패턴을 빠르게 인증할 수 있으며, 위변조가 불가능한 분산원장 상의 트랜잭션 정보를 이용하므로, 정확한 인증을 할 수 있다.

[0052] 또한, 규격화된 패턴을 블록체인 네트워크(110)에 포함된 분산 노드(120)에서 직접 인증할 수 있으므로, 종래와 같이 인증을 위한 중앙 집중형 서버가 필요하지 않고, 인증을 위해 중앙 집중형 서버와의 통신 또한 필요하지 않으므로, 인증 속도를 향상시킬 수 있다.

[0053] 촬영된 QR 코드가 기인증된 QR 코드와 일치함이 인증되면, 분산 노드(120)는 촬영된 QR 코드와 관련된 상품이 정품이라고 판단하거나, 분산 노드(120)는 촬영된 QR 코드에 포함된 정보에 기초하여 블록체인 네트워크(110)의 트랜잭션에 포함된 스마트 계약을 실행할 수 있다.

[0054] 도 5는 본 발명의 일 실시예에 따른 블록체인에 기반하여 규격화된 패턴을 머클 트리 구조로 인증하는 방법의 흐름도이다.

[0055] S510 단계에서, 분산 노드(120)는 규격화된 패턴을 입력 받을 수 있다.

[0056] 여기서, 규격화된 패턴은 가변 폭을 갖는 복수의 흑백 평형 막대의 조합을 포함할 수 있다. 예를 들어, 규격화된 패턴은 GS1 체계에 따라 상품 및 거래처의 식별과 유통 및 거래정보의 교환을 위한 국제표준 바코드를 포함할 수 있다. 또한, 규격화된 패턴은 소정의 규칙에 따라 매트릭스(matrix) 형태로 배열된 정사각형 셀(cell)들을 포함할 수 있다. 예를 들어, 규격화된 패턴은 QR 코드 모델 1 및 모델 2, Micro QR 코드, iQR 코드, SQRC, Frame QR 코드를 포함할 수 있으며, 이외에도, 의약품 표준코드 및 의료기기 표준코드와 같이, GS1 체계에 따라 상품 및 거래처의 식별과 유통 및 거래정보의 교환을 위한 국제표준 식별코드를 포함할 수 있다.

[0057] 분산 노드(120)는 규격화된 패턴을 입력 받기 위하여, 카메라로 규격화된 패턴을 촬영하거나, 적외선 센서를 이용하여 규격화된 패턴을 검출하거나, 규격화된 외부 기기(140, 150) 혹은 블록체인 네트워크(110) 내 다른 분산 노드(120)로부터 규격화된 패턴의 데이터를 유무선 통신을 통하여 수신할 수 있다.

[0058] 분산 노드(120)는 규격화된 패턴을 입력 받기 전에, 규격화된 패턴과 관련하여 기인증된 패턴의 머클 루트 값 및 머클 경로 상의 토너먼트 해시 값을 기인증된 패턴의 크기에 따라 기인증된 패턴으로부터 분할된 복수의 단위 블록에 기초하여 블록체인 네트워크(110)의 분산원장에 등록할 수 있다. 구체적으로, 패턴의 머클 루트 값 및 머클 경로 상의 토너먼트 해시 값은 기인증된 패턴으로부터 분할된 복수의 단위 블록 각각의 비트스트림을 머클 트리 구조에 따른 리프 노드에 적용하여 기인증된 획득될 수 있다.

[0059] 기인증된 패턴의 머클 루트 값 및 머클 경로 상의 토너먼트 해시 값은 분산원장의 트랜잭션에 포함될 수 있으며, 분산 노드(120)에 의해 블록체인 네트워크(110) 상에 직접 배포되거나, 블록체인 네트워크(110)의 다른 분산 노드(120)에 의해 배포될 수 있다.

[0060] S520 단계에서, 분산 노드(120)는 입력된 패턴을 복수의 단위 블록으로 분할할 수 있다.

[0061] 예를 들어, 분산 노드(120)는 입력된 패턴의 크기에 따라 단위 블록의 크기를 결정하고, 입력된 패턴을 결정된 크기의 단위 블록들로 분할할 수 있다. 이와 같은 방식에 의하면, 입력된 패턴의 크기가 커짐에 따라 단위 블록의 크기 또한 커질 수 있다. 또 다른 예로, 분산 노드(120)는 입력된 패턴의 크기에 무관하게, 입력된 패턴을 고정된 크기의 단위 블록들로 분할할 수 있다. 이와 같은 방식에 의하면, 입력된 패턴의 크기가 커지더라도 단위 블록의 크기는 변하지 않으며, 입력된 패턴으로부터 분할된 단위 블록의 개수가 증가할 수 있다.

[0062] 머클 트리 구조에 따른 데이터 압축 효과를 달성하기 위하여, 단위 블록의 비트스트림의 길이가 머클 트리 구조에 따른 머클 루트 값의 길이보다 길고, 머클 트리 구조에 적용되는 해시 함수의 입력값의 최대 길이보다 짧도록, 단위 블록의 크기가 제한될 수 있다.

[0063] 분산 노드(120)는 입력된 패턴을 복수의 블록으로 분할하기 전에, 입력된 패턴의 방향 및 크기 중 적어도 하나를 기인증된 패턴에 맞추어 정규화할 수 있다. 구체적으로, 규격화된 패턴은 실질적인 정보를 포함하고 있는 데이터 부호화 영역(data encoding region)과 규격화된 패턴의 존재, 위치, 및 방향을 나타내기 위한 기능성 패턴 영역(function pattern region)으로 구분될 수 있다. 예를 들어, 분산 노드(120)가 규격화된 패턴을 촬영하는 경우, 분산 노드(120)는 기능성 패턴 영역에 포함된 정보를 이용하여 기인증된 패턴에 맞추어 촬영된 패턴의 방향을 정렬하고, 촬영된 패턴의 크기를 조절할 수 있다. 분산 노드(120)가 입력된 패턴을 정규화하는 방법에 대

해서는 이하 도 6에서 QR 코드의 예시로 더욱 상세히 설명한다.

[0064] S530 단계에서, 분산 노드(120)는 입력된 패턴으로부터 분할된 복수의 단위 블록 중 n개의 검증 블록을 결정할 수 있다.

[0065] 검증 블록은 규격화된 패턴에서 실질적인 정보를 포함하고 있는 데이터 부호화 영역에 위치하는 단위 블록일 수 있다. 검증 블록의 개수가 많아질수록, 인증의 신뢰도가 높아지지만 인증 속도는 떨어질 수 있다. 따라서, 검증 블록의 개수는 규격화된 패턴의 크기에 따라 증감할 수 있다.

[0066] S540 단계에서, 분산 노드(120)는 n개의 검증 블록으로부터 입력된 패턴에 대한 n개의 머클 루트 값을 계산할 수 있다.

[0067] 먼저, 분산 노드(120)는 제1 검증 블록을 미리 설정된 규칙에 따라 이진화하여 검증 블록의 비트스트림을 획득할 수 있다. 예를 들어, 규격화된 패턴이 흑백 평형 막대의 조합인 경우, 분산 노드(120)는 제1 검증 블록 내 흑색 평형 막대와 백색 평형 막대에 서로 다른 비트값(즉, 0 또는 1)을 순차적으로 부여하여 비트스트림을 생성할 수 있다. 또 다른 예로, 규격화된 패턴이 흑백 정사각형 셀들의 조합인 경우, 분산 노드(120)는 제1 검증 블록 내 좌상단 셀로부터 제1 검증 블록 내 우하단 셀까지 횡방향 또는 종방향으로 순차적으로 스캔하면서, 흑색 셀과 백색 셀에 서로 다른 값을 부여하여 비트스트림을 생성할 수 있다.

[0068] 이후, 분산 노드(120)는 제1 검증 블록의 비트스트림 및 블록체인 네트워크(110)의 분산원장에 등록된 기인증된 패턴에 대한 토너먼트 해시 값을 이용하여, 제1 검증 블록의 입력된 패턴에 대한 제1 머클 루트 값을 획득할 수 있다. 구체적으로, 분산 노드(120)는 제1 검증 블록의 비트스트림에 해시 함수를 적용하여 머클 트리 구조에 대한 리프 해시 값을 획득할 수 있다. 분산 노드(120)는, 제1 검증 블록의 리프 해시 값과, 기인증된 패턴으로부터 분할된 복수의 단위 블록 중 입력된 패턴의 제1 검증 블록에 대응하는 블록에 대한 머클 경로 상의 토너먼트 해시 값을 이용하여, 제1 머클 루트 값을 계산할 수 있다.

[0069] 이와 같이 제1 검증 블록으로부터 제1 머클 루트 값을 계산하는 방식으로, 분산 노드(120)는 n개의 검증 블록(제1 검증 블록, 제2 검증 블록, …, 제n 검증 블록)으로부터 n개의 머클 루트 값(제1 머클 루트 값, 제2 머클 루트 값, …, 제n 머클 루트 값)을 계산할 수 있다.

[0070] S550 단계에서, 분산 노드(120)는 n개의 검증 블록으로부터 획득된 입력된 패턴에 대한 n개의 머클 루트 값 중 m개 이상이 블록체인 네트워크(110)의 분산원장에 등록된 기인증된 패턴에 대한 머클 루트 값과 동일한지 여부를 판단할 수 있다.

[0071] 입력된 패턴에 대한 n개의 머클 루트 값 중 m개 이상이 기인증된 패턴에 대한 머클 루트 값과 동일하면, S560 단계 및 S570 단계에서, 분산 노드(120)는 입력된 패턴을 인증하고, 입력된 패턴과 관련된 분산원장 상의 스마트 계약을 실행할 수 있다. 또한, 분산 노드(120)는 입력된 패턴이 인증되면, 입력된 패턴과 관련된 상품 및 서비스가 정품이라고 판단할 수 있다.

[0072] 반면, S560 단계 및 S580 단계에서, 입력된 패턴에 대한 n개의 머클 루트 값 중 기인증된 패턴에 대한 머클 루트 값과 동일한 값이 m개 이상이 아니면, 분산 노드(120)는 입력된 패턴의 위변조를 검출할 수 있다. 또한, 분산 노드(120)는 입력된 패턴이 인증되면, 입력된 패턴과 관련된 상품 및 서비스가 정품이라고 아니라고 판단할 수 있다.

[0073] 이와 같이, 분산 노드(120)는 머클 트리 구조에 따른 입력된 패턴과 기인증된 패턴 사이의 유사도(m/n)를 이용함으로써, 입력된 패턴과 기인증된 패턴을 셀별로 일대일 비교하는 종래의 방식에 비하여 인증 속도를 향상시킬 수 있으며, 위변조가 불가능한 분산원장의 특징을 이용함으로써, 인증의 신뢰성을 보장할 수 있다.

[0074] 더불어, 규격화된 패턴을 블록체인 네트워크(110)에 포함된 분산 노드(120)에서 직접 인증할 수 있으므로, 인증을 위한 중앙 집중형 서버가 필요하지 않다.

[0075] 도 6은 본 발명의 일 실시예에 따라 블록체인에 기반하여 QR 코드를 머클 트리 구조로 인증하기 위하여, QR 코드를 단위 블록으로 분할하는 동작을 설명하기 위한 도면이다.

[0076] 분산 노드(120)가 QR 코드를 촬영하는 경우, QR 코드를 단위 블록으로 분할하기 전에, 분산 노드(120)는 QR 코드의 적어도 하나의 모서리에 존재하는 위치 찾기 심볼(610a, 610b, 610c)을 이용하여, QR 코드의 존재, 위치, 및 방향을 식별하고, 촬영된 QR 코드의 방향을 기인증된 패턴에 맞추어 정규화 할 수 있다.

[0077] 분산 노드(120)는 정규화된 QR 코드의 크기(즉, 촬영된 QR 코드에 포함된 셀의 개수)에 따라 단위 블록의 크기

를 결정하고, QR 코드(400)를 결정된 크기의 단위 블록들로 분할할 수 있다. 또 다른 예로, 분산 노드(120)는 촬영된 QR 코드(400)의 크기와 무관하게, QR 코드(400)를 고정된 크기의 단위 블록들(410)로 분할할 수 있다.

[0078] 일반적으로, QR 코드에 포함된 셀의 개수는 홀수 개이다 (셀의 개수 = N^2, N = 4*V+17, V = 양의 정수). 반면, 머클 트리 구조에는 짝수 개의 단위 블록이 필요하다. 따라서, 분산 노드(120)는 촬영된 QR 코드 주변의 밝은 마진(margin) 해당하는 콰이어트 영역(630)의 셀들을 일부 단위 블록에 포함시킬 수 있다. 예를 들어, 촬영된 QR 코드로부터 분할된 복수의 단위 블록 중, 마지막 열에 위치하는 단위 블록들(640a, 640b, 640c, 640d)이 콰이어트 영역(630)의 셀들을 포함할 수 있다. 또한, 콰이어트트 영역(630)의 셀들은 QR 코드의 밝은 영역의 이진화 값(0 또는 1)으로 패딩(padding)될 수 있다.

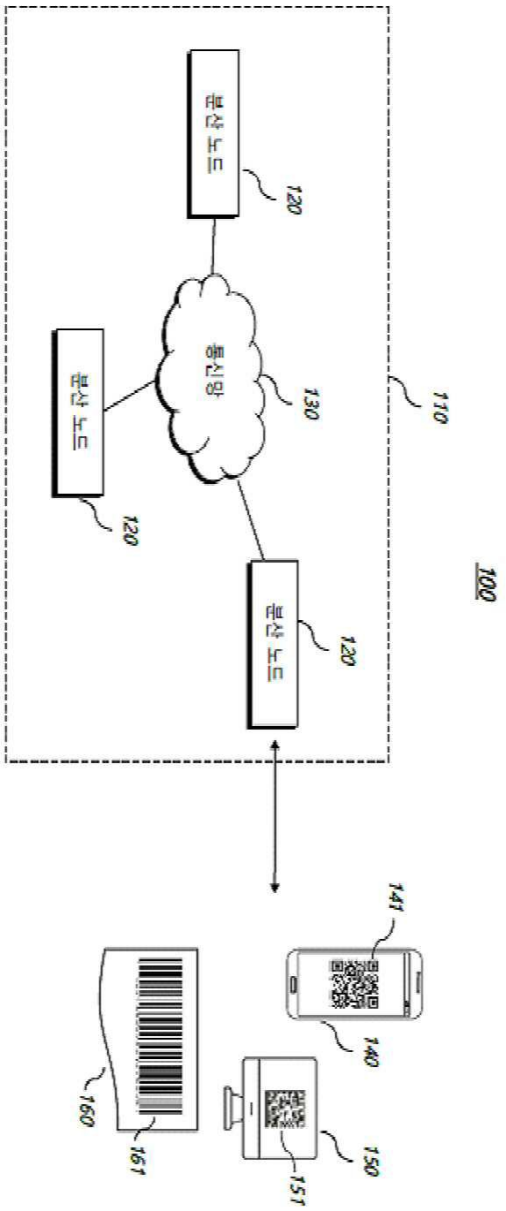
[0079] 분산 노드(120)는 촬영된 QR 코드의 데이터 부호화 영역에 포함된 단위 블록을 검증 블록(650)으로 결정할 수 있다. 또한, 분산 노드(120)는 검증 블록(650)의 좌상단 셀로부터 우하단 셀까지 횡방향으로 순차적으로 스캔하여, 검증 블록(650)의 비트스트림(1110000…)을 생성하고, 검증 블록(650)의 비트스트림(1110000…)을 도 4 내지 도 5를 통해 전술한 머클 트리 구조의 리프 노드로 설정할 수 있다. 비트스트림을 생성할 때, 흑색 셀과 백색 셀은 서로 다른 비트값(즉, 0 또는 1)로 이진화 될 수 있다.

[0080] 당업자라면 알 수 있듯이, 본 개시가 본 명세서에 기술된 예시에 한정되는 것이 아니라 본 개시의 범주를 벗어나지 않는 범위 내에서 다양하게 변형, 재구성 및 대체될 수 있다. 본 명세서에 기술된 다양한 기술들은 하드웨어 또는 소프트웨어, 또는 하드웨어와 소프트웨어의 조합에 의해 구현될 수 있음을 알아야 한다.

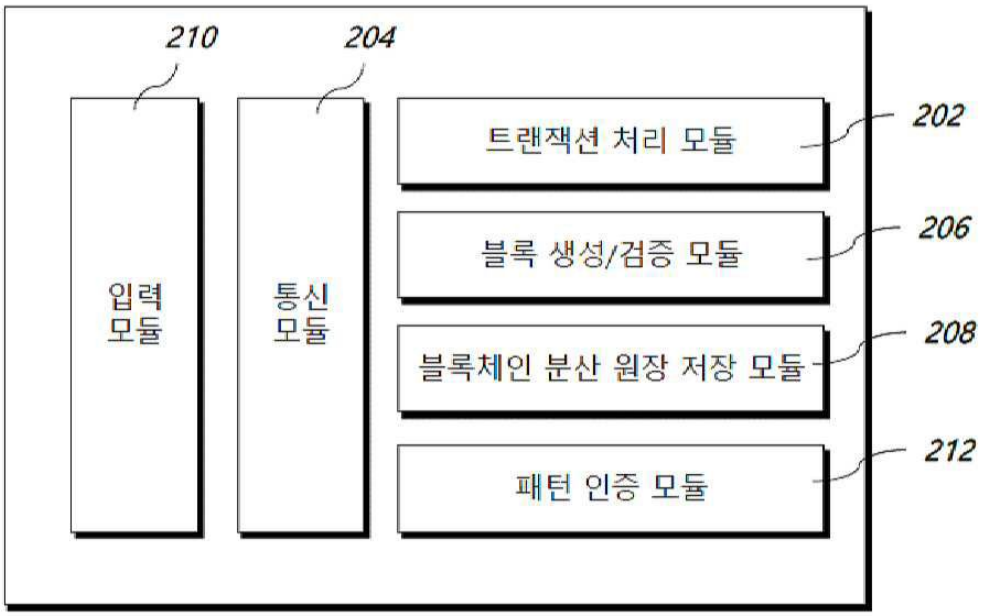
[0081] 본 개시의 일 실시예에 따른 컴퓨터 프로그램은, 컴퓨터 프로세서 등에 의해 판독 가능한 저장 매체, 예컨대 EPROM, EEPROM, 플래시 메모리장치와 같은 비휘발성 메모리, 내장형 하드 디스크와 착탈식 디스크 같은 자기 디스크, 광자기 디스크, 및 CDROM 디스크 등을 포함한 다양한 유형의 저장 매체에 저장된 형태로 구현될 수 있다. 또한, 프로그램 코드(들)는 어셈블리어나 기계어로 구현될 수 있다. 본 개시의 진정한 사상 및 범주에 속하는 모든 변형 및 변경을 이하의 특허청구범위에 의해 모두 포괄하고자 한다.

도면

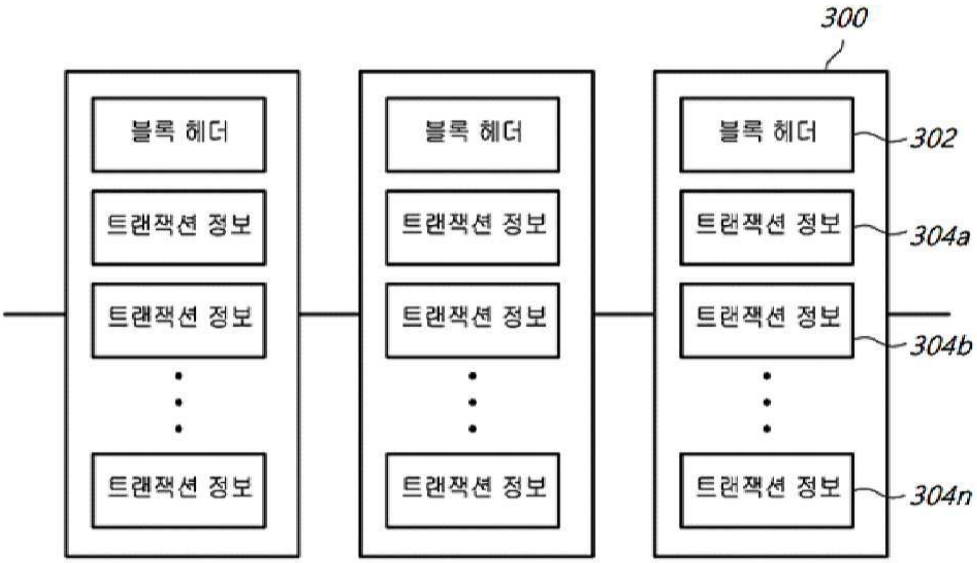
도면1


분산 노드
120
통신망
130
분산 노드
120
분산 노드
120
110
100
141
140
150
151
160
161

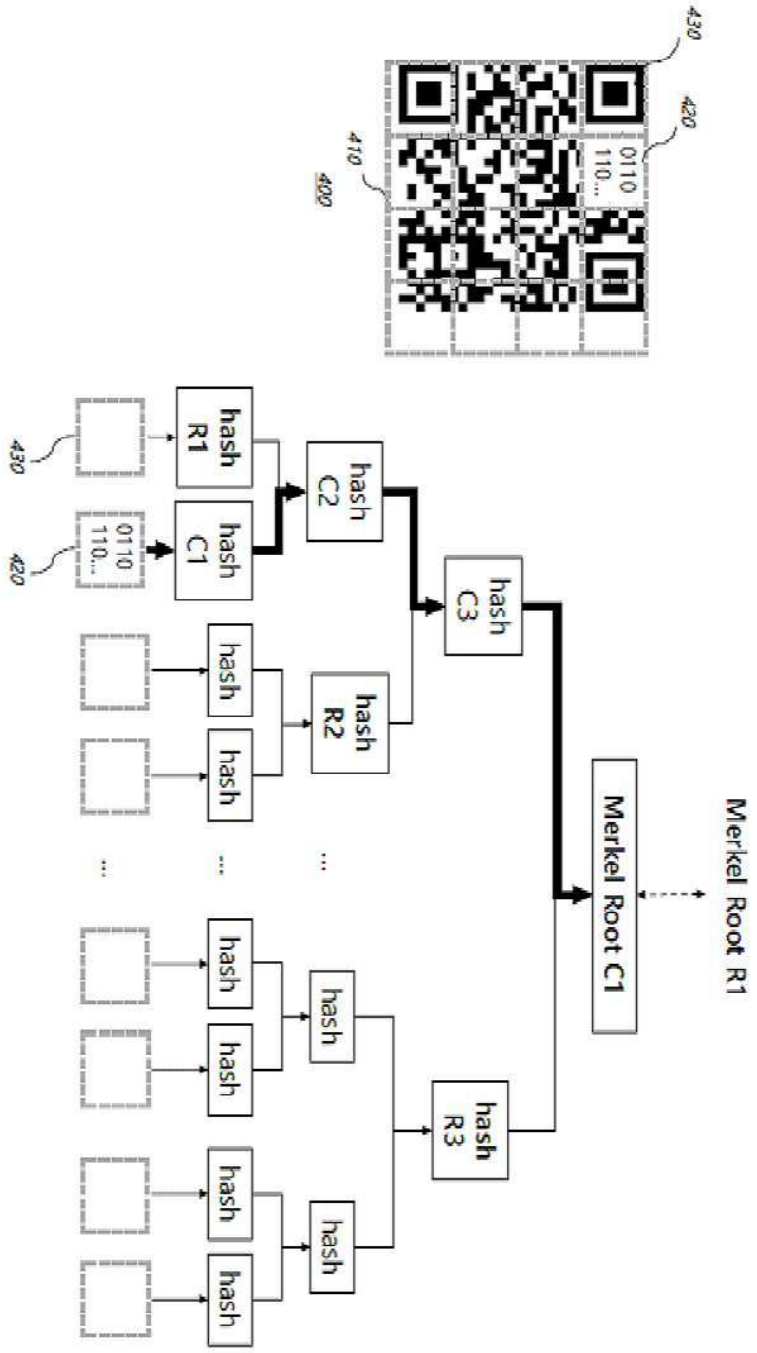
도면2


210
204
입력 모듈
통신 모듈
트랜잭션 처리 모듈
202
블록 생성/검증 모듈
206
블록체인 분산 원장 저장 모듈
208
패턴 인증 모듈
212

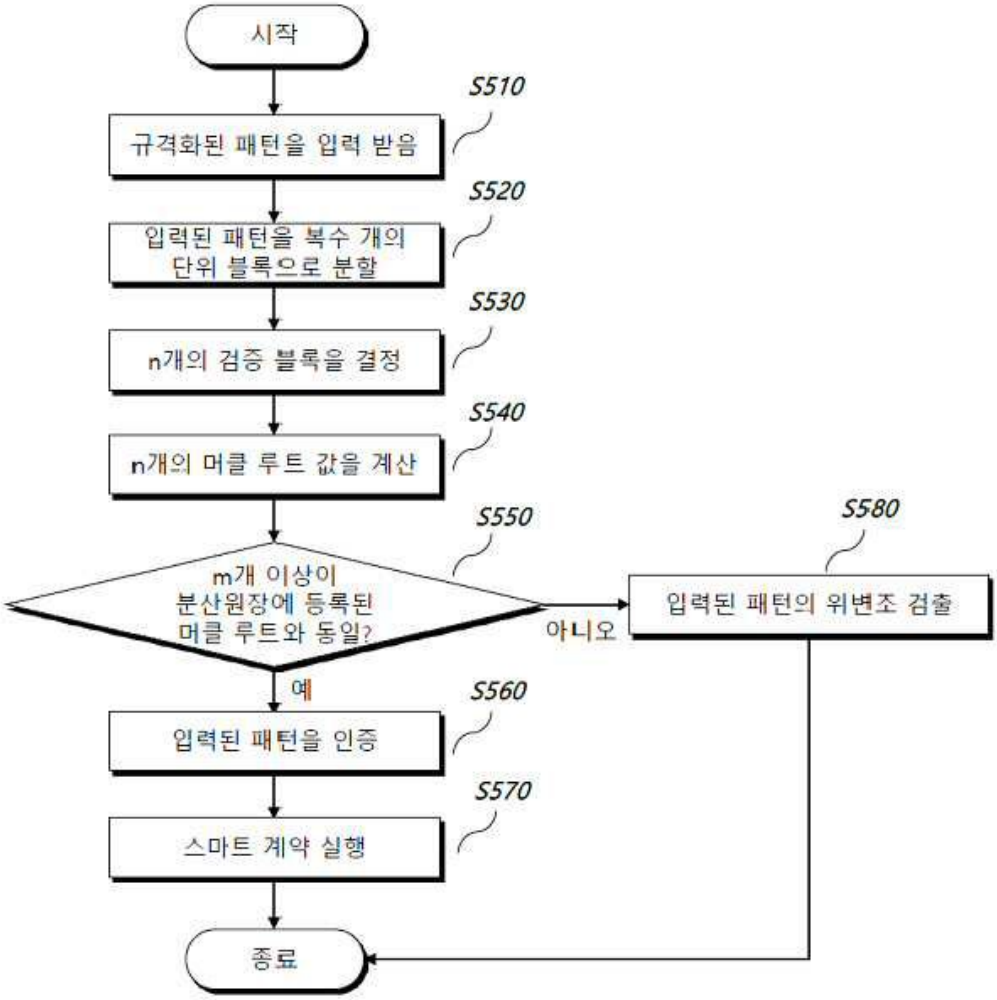
도면3


300
블록 헤더
트랜잭션 정보
트랜잭션 정보
트랜잭션 정보
302
304a
304b
304n

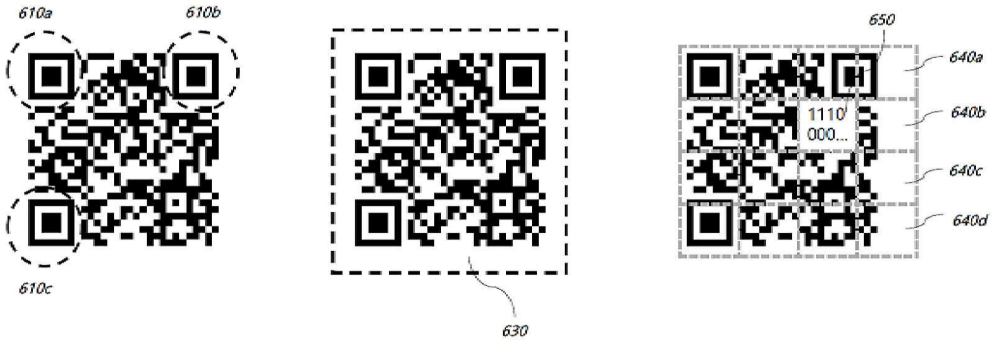
도면4


400
410
420
430
0110
110...
hash
R1
C1
C2
C3
R2
R3
Merkel Root C1
Merkel Root R1

도면5


시작
S510
규격화된 패턴을 입력 받음
S520
입력된 패턴을 복수 개의 단위 블록으로 분할
S530
n개의 검증 블록을 결정
S540
n개의 머클 루트 값을 계산
S550
m개 이상이 분산원장에 등록된 머클 루트와 동일?
아니오
S580
입력된 패턴의 위변조 검출
예
S560
입력된 패턴을 인증
S570
스마트 계약 실행
종료

도면6


610a
610b
610c
630
650
640a
640b
640c
640d
1110
000...