(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0077598
(43) 공개일자 2022년06월09일

(51) 국제특허분류(Int. Cl.)
G06F 21/10 (2013.01) *G06F 21/31* (2013.01)
G06F 21/46 (2013.01) *G06Q 30/06* (2012.01)
H04L 9/06 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
G06F 21/10 (2013.01)
G06F 21/31 (2013.01)
(21) 출원번호 10-2020-0166693
(22) 출원일자 2020년12월02일
심사청구일자 2020년12월02일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
도인실
인천광역시 연수구 센트럴로 194, 201동 1703호 (더샵센트럴파크2단지아파트)
채기준
서울특별시 강남구 강남대로136길 34, 402호 (논현동,월드노블레스빌)
허가빈
경상남도 창원시 의창구 하남천서길21번길 8-14, 1동 1107호 (도계동, 강남훼미리아파트)
(74) 대리인
윤귀상

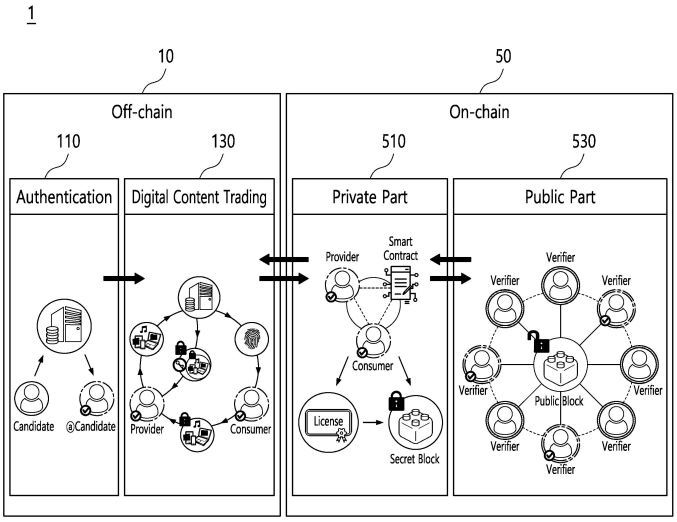
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **블록체인을 활용한 디지털 콘텐츠 거래 방법, 이를 수행하기 위한 기록 매체 및 시스템**

(57) 요 약

블록체인을 활용한 디지털 콘텐츠 거래 방법은, ID, PW 및 공개키를 서버에 저장하는 오프 체인(off-chain) 영역에서, 사용자 인증을 수행하는 단계; DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래하는 단계; 온 체인(On-chain) 영역에서, 스마트 컨트랙트를 생성하여 DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하는 단계; 디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 단계; 가중치를 적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증하는 단계; 및 검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 연결하는 단계;를 포함한다. 이에 따라, 안전하고 신뢰성 높은 디지털 콘텐츠 거래 환경을 제시한다.

대 표 도 - 도1



(52) CPC특허분류
G06F 21/46 (2013.01)
G06Q 30/0619 (2013.01)
H04L 9/0643 (2013.01)
H04L 9/0825 (2013.01)
H04L 9/0869 (2013.01)
H04L 9/50 (2022.05)
H04L 2209/603 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711114604
과제번호 2020R1A2C1006497
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 UAV를 활용한 모바일 IoT 환경에서 효율적이고 안전한 노드 및 데이터 프라이버시 보장 기법
기 여 율 1/2
과제수행기관명 이화여자대학교
연구기간 2020.03.01 ~ 2021.02.28
이 발명을 지원한 국가연구개발사업
과제고유번호 1711114922
과제번호 2019R1F1A1063194
부처명 과학기술정보통신부
과제관리(전문)기관명 한국연구재단
연구사업명 개인기초연구(과기정통부)(R&D)
연구과제명 블록체인과 통합 학습 기반의 안전하고 효율적인 FANET 구조 연구
기 여 율 1/2
과제수행기관명 이화여자대학교
연구기간 2020.03.01 ~ 2021.02.28

명 세 서

청구범위

청구항 1

ID, PW 및 공개키를 서버에 저장하는 오프 체인(off-chain) 영역에서, 사용자 인증을 수행하는 단계;

DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래하는 단계;

온 체인(On-chain) 영역에서, 스마트 컨트랙트를 생성하여 DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하는 단계;

디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 단계;

가중치를 적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증하는 단계; 및

검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 연결하는 단계;를 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 방법.

청구항 2

제1항에 있어서, 상기 사용자 인증을 수행하는 단계는,

사용자에 의해 설정된 ID, PW 및 비대칭 키를 기초로, ID의 해시값을 솔트(Salt) 값으로 사용하여 PW와 함께 해시함수를 통해 해시값을 생성하는 사용자 등록 단계;를 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 방법.

청구항 3

제2항에 있어서, 상기 사용자 인증을 수행하는 단계는,

사용자 등록 과정을 거친 사용자들이 거래를 원할 때 인증 요청을 보내는 경우 난수를 생성하는 단계;

생성된 난수의 값을 등록된 사용자의 공개키로 암호화하여 전송하는 단계;

PW 해시값과 인증 요청시간을 연결한 값을 랜덤 시드(SEED)로 사용하여 랜덤값을 생성하는 단계;

PW 해시값에 해당 랜덤값을 사용하여 x값을 선택하는 단계; 및

생성한 난수의 값 n에 x승을 계산하고 사용자가 전송한 값과 같을 경우 정상적인 사용자로 판단하여 사용자 인증을 완료하는 단계;를 더 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 방법.

청구항 4

제1항에 있어서, 상기 암호화된 콘텐츠를 거래하는 단계는,

인증받은 콘텐츠 제공자가 콘텐츠를 서버에 전송하고, 콘텐츠를 사용하고자 하는 소비자가 인증과정을 거친 후 디지털 콘텐츠 거래를 위해 거래를 요청하는 경우, DRM을 적용하기 위해 비대칭키를 생성하는 단계;

콘텐츠에 대한 비트를 랜덤한 크기로 세분화하고, 세분된 비트 중 랜덤한 장소에, 랜덤한 개수로 핑거프린트를 삽입하는 단계;

핑거프린트가 삽입된 콘텐츠를 DRM을 위해 생성된 공개키를 통해 암호화하는 단계; 및

암호화된 콘텐츠와 해당 콘텐츠를 복호화할 수 있는 비밀키, 소비자의 공개키를 콘텐츠 제공자의 공개키로 암호화하여 콘텐츠 제공자에게 전송하는 단계;를 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 방법.

청구항 5

제1항에 있어서, 상기 시크릿 블록으로 생성하는 단계는,

콘텐츠 제공자가 암호화된 디지털 콘텐츠를 복호화할 수 있는 비밀키를 소비자의 공개키로 암호화하여 스마트 컨트랙트로 전송하는 단계; 및

소비자가 라이센스를 성공적으로 전달받은 후 확인(Confirm) 메시지를 보내는 경우 거래내용을 시크릿 블록으로 생성하는 단계;를 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 방법.

청구항 6

제1항에 있어서, 상기 블록체인 사용자들의 거래를 검증하는 단계는,

인증받은 사용자의 가중치를 인증받지 않은 사용자의 가중치 보다 높게 부여하는 단계; 및

합의를 위한 검증자를 랜덤하게 선출하는 단계;를 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 방법.

청구항 7

제1항 내지 제6항 중 어느 하나의 항에 따른 상기 블록체인을 활용한 디지털 콘텐츠 거래 방법을 수행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 저장 매체.

청구항 8

ID, PW 및 공개키를 서버에 저장하여 사용자 인증을 수행하는 사용자 인증부;

DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래하도록 하는 디지털 콘텐츠 거래부;

스마트 컨트랙트를 생성하여 DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하고, 디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 프라이빗 영역부; 및

가중치를 적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증하고, 검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 연결하는 퍼블릭 영역부;를 포함하는, 블록체인을 활용한 디지털 콘텐츠 거래 시스템.

청구항 9

제8항에 있어서, 상기 사용자 인증부는,

사용자에 의해 설정된 ID, PW 및 비대칭 키를 기초로, ID의 해시값을 솔트(Salt) 값으로 사용하여 PW와 함께 해시함수를 통해 해시값을 생성하여 사용자 등록 과정을 수행하는, 블록체인을 활용한 디지털 콘텐츠 거래 시스템.

청구항 10

제9항에 있어서, 상기 사용자 인증부는,

사용자 등록 과정을 거친 사용자들이 거래를 원할 때 서버로 인증 요청을 보내면, 난수를 생성하여 등록된 사용자의 공개키로 암호화하여 전송하고, PW 해시값과 인증 요청시간을 연결한 값을 랜덤 시드(SEED)로 사용하여 랜덤값을 생성하고, PW 해시값에 상기 랜덤값을 사용하여 x값을 선택하고, 생성한 난수 n에 x승을 계산하여 사용

자 인증 과정을 수행하는, 블록체인을 활용한 디지털 콘텐츠 거래 시스템.

청구항 11

제8항에 있어서, 상기 디지털 콘텐츠 거래부는,

인증받은 콘텐츠 제공자가 콘텐츠를 서버에 전송하고, 콘텐츠를 사용하고자 하는 소비자가 인증과정을 거친 후 디지털 콘텐츠 거래를 위해 거래를 요청하는 경우, DRM을 적용하기 위해 비대칭키를 생성하고, 콘텐츠에 대한 비트를 랜덤한 크기로 세분화하고, 세분된 비트 중 랜덤한 장소에, 랜덤한 개수로 핑거프린트를 삽입하고, 핑거프린트가 삽입된 콘텐츠를 DRM을 위해 생성된 공개키를 통해 암호화하고, 암호화된 콘텐츠와 해당 콘텐츠를 복호화할 수 있는 비밀키, 소비자의 공개키를 콘텐츠 제공자의 공개키로 암호화하여 콘텐츠 제공자에게 전송하는, 블록체인을 활용한 디지털 콘텐츠 거래 시스템.

청구항 12

제8항에 있어서, 상기 프라이빗 영역부는,

콘텐츠 제공자가 암호화된 디지털 콘텐츠를 복호화할 수 있는 비밀키를 소비자의 공개키로 암호화하여 스마트 컨트랙트로 전송하고, 소비자가 라이센스를 성공적으로 전달받은 후 확인(Confirm) 메시지를 보내는 경우 거래 내용을 시크릿 블록으로 생성하는, 블록체인을 활용한 디지털 콘텐츠 거래 시스템.

청구항 13

제8항에 있어서, 상기 퍼블릭 영역부는,

인증받은 사용자의 가중치를 인증받지 않은 사용자의 가중치 보다 높게 부여하고, 합의를 위한 검증자를 랜덤하게 선출하여 합의를 진행하는, 블록체인을 활용한 디지털 콘텐츠 거래 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인을 활용한 디지털 콘텐츠 거래 방법, 이를 수행하기 위한 기록 매체 및 시스템에 관한 것으로서, 더욱 상세하게는 다양한 참여자가 존재하는 퍼블릭 블록체인을 기본 구조로 적용하여 프라이빗 블록체인에서 발생하는 권한 악용 및 거래 위조와 같은 문제점을 방지하는 기술에 관한 것이다.

배 경 기 술

[0003] 최근 사물에 네트워크를 연결하여 사물끼리 정보를 공유하는 환경인 IoT(Internet of Things) 시대를 지나, 사람과 사물을 포함하여 프로세스와 데이터까지 네트워크로 연결하여 모든 정보를 공유하는 환경인 IoE(Internet of Everything) 시대로 발전하면서 정보화시대의 모든 정보는 중요한 자원이 되었다.

[0004] 특히 정보화 시대가 도래하면서, 영화나 음악뿐만 아니라 가상현실(VR, Virtual Reality), 증강현실(AR, Augmented Reality), 혼합현실(MR, Mixed Reality)과 같은 다양한 형태의 디지털 콘텐츠가 등장하였다. 이를 통해 가상과 현실의 상호작용이 가능하고, 사용자들은 디지털 콘텐츠를 통해 새로운 경험을 창출할 수 있다.

[0005] 또한, '개인 콘텐츠 크리에이터'라는 새로운 직업이 생기면서 유튜브, 페이스북 등 영상 유통 플랫폼의 디지털 콘텐츠 양이 급속도로 증가하게 되었으며, 스마트기기 보급확대 및 세계적 기업들의 플랫폼 서비스 활성화 등으로 디지털 콘텐츠 시장의 규모 및 전망 또한 점점 증가할 것으로 예측된다.

[0006] 하지만, 기존 디지털 콘텐츠 거래환경에는 불법복제 및 유출, 수익분배, 위/변조 등의 문제점이 있으며, 이러한 문제점들로 인해 현재 디지털 콘텐츠 시장의 성장률은 낮아지고 있는 실정이다. 따라서, 4차 산업혁명의 핵심기

술로 주목받은 블록체인을 디지털 콘텐츠 거래환경에 적용하는 연구가 지속적으로 이루어지고 있다.

[0007] P2P(Peer to Peer) 기반의 분산공개 장부인 블록체인(Blockchain)은 모든 참여자가 거래 정보가 담긴 장부를 소유함으로써 투명성과 데이터 무결성 및 높은 보안성을 보장한다. 또한, 제3 기관 없이 거래하기 때문에 거래에 대한 신뢰성이 확보된다. 이러한 특징을 가진 블록체인을 디지털 콘텐츠 환경에 접목한다면 기존의 디지털 콘텐츠 거래환경의 문제점을 해결할 수 있다.

[0008] 하지만, 블록체인에 업로드 할 수 있는 용량이 적기 때문에 음원이나 동영상 같은 디지털 콘텐츠를 블록 체인에 업로드하기 위한 기술적인 문제가 존재하며, 모든 참여자가 거래장부를 가지고 있어 누구나 거래 정보를 확인할 수 있으므로 개인정보가 유출되는 문제가 여전히 존재한다.

[0009] 특히, 최근 유럽연합의 개인정보보호법인 GDPR(General Data Protection Regulation)이 제정됨에 따라 IT 시스템에서 개인정보보호 개념을 준수하는 것은 개인정보 취급 시 중요한 요구사항 중 하나로 대두되고 있으므로 블록체인에서 개인정보보호를 위한 방안을 심각하게 고려해야 한다.

[0010] 현재 기존의 디지털 콘텐츠 거래환경에서 무분별하게 나타나는 불법유출과 수익분배 문제에 블록체인 기술을 접목시켜, 분산 원장 및 P2P(Peer to Peer) 통신의 특징을 통해 해결할 수 있다. 하지만, 블록체인에서 발생하는 문제점은 고려하지 않았기 때문에, 디지털 콘텐츠 거래환경에서 기존의 블록체인을 접목하기에 적합하지 않다.

선행기술문헌

특허문헌

[0012] (특허문헌 0001) KR 10-2020-0104590 A

(특허문헌 0002) KR 10-2020-0022202 A

(특허문헌 0003) US 2020/0042990 A1

발명의 내용

해결하려는 과제

[0013] 이에, 본 발명의 기술적 과제는 이러한 점에서 착안된 것으로 본 발명의 목적은 블록체인을 활용한 디지털 콘텐츠 거래 방법을 제공하는 것이다.

[0014] 본 발명의 다른 목적은 상기 블록체인을 활용한 디지털 콘텐츠 거래 방법을 수행하기 위한 컴퓨터 프로그램이 기록된 기록 매체를 제공하는 것이다.

[0015] 본 발명의 또 다른 목적은 상기 블록체인을 활용한 디지털 콘텐츠 거래 방법을 수행하기 위한 시스템을 제공하는 것이다.

과제의 해결 수단

[0017] 상기한 본 발명의 목적을 실현하기 위한 일 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 방법은, ID, PW 및 공개키를 서버에 저장하는 오프 체인(off-chain) 영역에서, 사용자 인증을 수행하는 단계; DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래하는 단계; 온 체인(On-chain) 영역에서, 스마트 컨트랙트를 생성하여 DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하는 단계; 디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 단계; 가중치를 적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증하는 단계; 및 검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 연결하는 단계;를 포함한다.

[0018] 본 발명의 실시예에서, 상기 사용자 인증을 수행하는 단계는, 사용자에 의해 설정된 ID, PW 및 비대칭 키를 기초로, ID의 해시값을 솔트(Salt) 값으로 사용하여 PW와 함께 해시함수를 통해 해시값을 생성하는 사용자 등록

단계;를 포함할 수 있다.

[0019] 본 발명의 실시예에서, 상기 사용자 인증을 수행하는 단계는, 사용자 등록 과정을 거친 사용자들이 거래를 원할 때 인증 요청을 보내는 경우 난수를 생성하는 단계; 생성된 난수의 값을 등록된 사용자의 공개키로 암호화하여 전송하는 단계; PW 해시값과 인증 요청시간을 연결한 값을 랜덤 시드(SEED)로 사용하여 랜덤값을 생성하는 단계; PW 해시값에 해당 랜덤값을 사용하여 x값을 선택하는 단계; 및 생성한 난수의 값 n에 x승을 계산하고 사용자가 전송한 값과 같을 경우 정상적인 사용자로 판단하여 사용자 인증을 완료하는 단계;를 더 포함할 수 있다.

[0020] 본 발명의 실시예에서, 상기 암호화된 콘텐츠를 거래하는 단계는, 인증받은 콘텐츠 제공자가 콘텐츠를 서버에 전송하고, 콘텐츠를 사용하고자 하는 소비자가 인증과정을 거친 후 디지털 콘텐츠 거래를 위해 거래를 요청하는 경우, DRM을 적용하기 위해 비대칭키를 생성하는 단계; 콘텐츠에 대한 비트를 랜덤한 크기로 세분화하고, 세분된 비트 중 랜덤한 장소에, 랜덤한 개수로 핑거프린트를 삽입하는 단계; 핑거프린트가 삽입된 콘텐츠를 DRM을 위해 생성된 공개키를 통해 암호화하는 단계; 및 암호화된 콘텐츠와 해당 콘텐츠를 복호화할 수 있는 비밀키, 소비자의 공개키를 콘텐츠 제공자의 공개키로 암호화하여 콘텐츠 제공자에게 전송하는 단계;를 포함할 수 있다.

[0021] 본 발명의 실시예에서, 상기 시크릿 블록으로 생성하는 단계는, 콘텐츠 제공자가 암호화된 디지털 콘텐츠를 복호화할 수 있는 비밀키를 소비자의 공개키로 암호화하여 스마트 컨트랙트로 전송하는 단계; 및 소비자가 라이센스를 성공적으로 전달받은 후 확인(Confirm) 메시지를 보내는 경우 거래내용을 시크릿 블록으로 생성하는 단계;를 포함할 수 있다.

[0022] 본 발명의 실시예에서, 상기 블록체인 사용자들의 거래를 검증하는 단계는, 인증받은 사용자의 가중치를 인증받지 않은 사용자의 가중치 보다 높게 부여하는 단계; 및 합의를 위한 검증자를 랜덤하게 선출하는 단계;를 포함할 수 있다.

[0023] 상기한 본 발명의 다른 목적을 실현하기 위한 일 실시예에 따른 컴퓨터로 판독 가능한 저장 매체에는, 상기 블록체인을 활용한 디지털 콘텐츠 거래 방법을 수행하기 위한 컴퓨터 프로그램이 기록되어 있다.

[0024] 상기한 본 발명의 또 다른 목적을 실현하기 위한 일 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 시스템은, ID, PW 및 공개키를 서버에 저장하여 사용자 인증을 수행하는 사용자 인증부; DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래하도록 하는 디지털 콘텐츠 거래부; 스마트 컨트랙트를 생성하여 DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하고, 디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 프라이빗 영역부; 및 가중치를 적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증하고, 검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 연결하는 퍼블릭 영역부;를 포함한다.

[0025] 본 발명의 실시예에서, 상기 사용자 인증부는, 사용자에 의해 설정된 ID, PW 및 비대칭 키를 기초로, ID의 해시값을 솔트(Salt) 값으로 사용하여 PW와 함께 해시함수를 통해 해시값을 생성하여 사용자 등록 과정을 수행할 수 있다.

[0026] 본 발명의 실시예에서, 상기 사용자 인증부는, 사용자 등록 과정을 거친 사용자들이 거래를 원할 때 서버로 인증 요청을 보내면, 난수를 생성하여 등록된 사용자의 공개키로 암호화하여 전송하고, PW 해시값과 인증 요청시간을 연결한 값을 랜덤 시드(SEED)로 사용하여 랜덤값을 생성하고, PW 해시값에 상기 랜덤값을 사용하여 x값을 선택하고, 생성한 난수 n에 x승을 계산하여 사용자 인증 과정을 수행할 수 있다.

[0027] 본 발명의 실시예에서, 상기 디지털 콘텐츠 거래부는, 인증받은 콘텐츠 제공자가 콘텐츠를 서버에 전송하고, 콘텐츠를 사용하고자 하는 소비자가 인증과정을 거친 후 디지털 콘텐츠 거래를 위해 거래를 요청하는 경우, DRM을 적용하기 위해 비대칭키를 생성하고, 콘텐츠에 대한 비트를 랜덤한 크기로 세분화하고, 세분된 비트 중 랜덤한 장소에, 랜덤한 개수로 핑거프린트를 삽입하고, 핑거프린트가 삽입된 콘텐츠를 DRM을 위해 생성된 공개키를 통해 암호화하고, 암호화된 콘텐츠와 해당 콘텐츠를 복호화할 수 있는 비밀키, 소비자의 공개키를 콘텐츠 제공자의 공개키로 암호화하여 콘텐츠 제공자에게 전송할 수 있다.

[0028] 본 발명의 실시예에서, 상기 프라이빗 영역부는, 콘텐츠 제공자가 암호화된 디지털 콘텐츠를 복호화할 수 있는 비밀키를 소비자의 공개키로 암호화하여 스마트 컨트랙트로 전송하고, 소비자가 라이센스를 성공적으로 전달받은 후 확인(Confirm) 메시지를 보내는 경우 거래내용을 시크릿 블록으로 생성할 수 있다.

[0029] 본 발명의 실시예에서, 상기 퍼블릭 영역부는, 인증받은 사용자의 가중치를 인증받지 않은 사용자의 가중치 보

다 높게 부여하고, 합의를 위한 검증자를 랜덤하게 선출하여 합의를 진행할 수 있다.

발명의 효과

[0031] 이와 같은 블록체인을 활용한 디지털 콘텐츠 거래 방법에 따르면, 기존 디지털 콘텐츠 거래환경의 문제점과 블록체인의 문제점을 해결하기 위해 SBBC(Secret Block based BlockChain) 시스템을 제안한다. 시크릿 블록(Secret Block) 생성을 통해 기존 블록체인의 저장공간 한계 문제와 개인정보 유출 문제를 해결하였으며, 다수의 참여자가 합의에 참여하기 때문에 블록체인의 강점인 무결성과 투명성의 특징은 기존과 같이 보장한다.

[0032] 또한, 해당 환경의 특징을 고려하여 인증받은 사용자의 가중치를 높게 부과하여 합의하는 WBFT(Weighted authentication Byzantine Fault Tolerance) 알고리즘을 제안하여 합의의 신뢰성을 보장한다.

도면의 간단한 설명

[0034] 도 1은 본 발명의 일 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 시스템의 블록도이다.

도 2는 도 1의 블록체인 시스템인 SBBC(Secret Block based Block Chain)의 콘텐츠 거래 과정을 보여주는 타임도이다.

도 3은 도 1의 사용자 인증부에서 인증과정을 보여주는 타임도이다.

도 4는 본 발명에서 제안하는 디지털 핑거프린팅 적용 구조를 보여주는 도면이다.

도 5는 DRM이 적용된 콘텐츠를 사용할 수 있는 라이센스 구조와 시크릿 블록(Secret Block)의 구조를 보여주는 도면이다.

도 6은 검증자에게 공개하지 않고 정보를 소지하고 있다는 것을 증명하는 과정의 일례를 보여주는 도면이다.

도 7은 가중치에 따라 랜덤으로 검증자를 선출하는 것을 보여주는 도면이다.

도 8은 SBBC 시스템의 네트워크 구성을 보여주는 도면이다.

도 9는 SBBC의 블록구조와 연결 구조를 보여주는 도면이다.

도 10은 SBBC의 참여자 간의 원장 구조 차이를 보여주는 도면이다.

도 11은 본 발명의 일 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 방법의 흐름도이다.

도 12는 본 발명을 적용하여 가중치에 따른 노드 공정성 측정값을 보여주는 표이다.

도 13은 PBFT와 WBFT의 노드 수에 따른 합의 실행시간 비교 결과를 보여주는 표이다.

도 14는 SBBC 시스템에서 인증받은 사용자 비율에 따른 합의 실행 시간 비교를 보여주는 표이다.

발명을 실시하기 위한 구체적인 내용

[0035] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예에 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0036] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0037] 도 1은 본 발명의 일 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 시스템의 블록도이다. 도 2는 도 1

의 블록체인 시스템인 SBBC(Secret Block based Block Chain)의 콘텐츠 거래 과정을 보여주는 타임도이다.

[0038] 본 발명에 블록체인을 활용한 디지털 콘텐츠 거래 시스템(1, 이하 시스템)은 디지털 콘텐츠 거래환경에서 블록체인 시스템을 접목할 때 나타나는 문제점을 분석하여 새로운 블록체인 시스템인 SBBC(Secret Block based Block Chain)를 제안한다.

[0039] SBBC는 오프 체인(Off-chain) 영역(10)과 온 체인(On-chain) 영역(50)으로 분리하여 정의한다. 오프 체인 영역(10)은 인증단계를 거쳐 디지털 콘텐츠를 거래하는 부분이다. 거래되는 디지털 콘텐츠는 디지털 핑거프린트가 삽입되어 불법 유출이 발생했을 경우, 유출지를 추적할 수 있다. 또한, 콘텐츠는 암호화되어 거래되고 정당한 권리를 가진 사용자만이 디지털 콘텐츠를 이용할 수 있으므로 콘텐츠 저작자의 정당한 수입을 보장한다.

[0040] 다음으로 온 체인 영역(50)은 디지털 콘텐츠를 사용하는데 필요한 라이센스를 발급받고, 합의 알고리즘을 사용한 검증 과정이 이루어진다. 라이센스를 발급받은 사용자는 자신의 거래내용을 시크릿 블록(Secret Block)으로 생성하여 자신의 원장에만 기록한다. 비공개 환경에서 시크릿 블록 생성을 통해 개인정보보호를 보장하며, 블록체인에 디지털 콘텐츠를 업로드 했을 때 일어날 수 있는 네트워크 과부하를 해결하였다. 마지막으로 모든 블록체인 참여자들의 거래 검증 및 합의를 통해 퍼블릭 블록(Public Block)을 생성하여 모든 참여자의 원장에 기록하여 거래를 마무리한다.

[0041] 디지털 콘텐츠 거래환경에서 블록체인을 접목한 기존의 연구들은 디지털 콘텐츠 거래환경의 문제점에만 초점을 맞추었기 때문에 수익분배, 위/변조 문제점은 해결할 수 있다. 하지만, 블록체인 기술에 의해 발생하는 개인정보 유출 문제를 해결하지 못하였으며 블록체인의 저장공간의 한계 문제를 해결하지 못하였다는 한계점이 존재한다.

[0042] 따라서, 본 발명에서는 시크릿 블록을 생성하여 개인정보 유출 문제와 용량 한정의 문제를 해결하였으며, 결론적으로 디지털 콘텐츠 거래환경의 새로운 해결책으로 떠오른 블록체인의 기존 문제점을 해결한 SBBC를 제안하고 이를 접목함으로써 안전한 디지털 콘텐츠 거래를 가능하도록 하였다.

[0043] 도 1을 참조하면, 본 발명에 따른 시스템(1)은 디지털 콘텐츠 거래환경에 알맞은 블록체인 시스템 접목을 위해 오프 체인(Off-chain) 영역(10)과 온 체인(On-chain) 영역(50)으로 정의된다. 기본 구조는 퍼블릭 블록체인을 기반으로 구성되며 해당 환경을 통해 투명성 및 무결성 특징을 보장한다. 또한, 시크릿 블록을 통해 블록체인의 문제점을 해결하고, 결론적으로 안전하고 신뢰성 높은 디지털 콘텐츠 거래환경을 위한 시스템을 제시한다.

[0044] 상기 오프 체인(Off-chain) 영역(10)에서는 디지털 콘텐츠를 거래하기 전 인증과정이 이루어지며, 인증받은 사용자들은 디지털 콘텐츠 거래를 진행하게 되는데 콘텐츠 제공자 및 콘텐츠 소비자 모두 인증을 받아야 거래를 진행할 수 있다.

[0045] 이를 위해, 상기 오프 체인(Off-chain) 영역(10)은 ID, PW 및 공개키를 서버에 저장하여 사용자 인증을 수행하는 사용자 인증부(110) 및 DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래하도록 하는 디지털 콘텐츠 거래부(130)를 포함한다.

[0046] 상기 온 체인(On-chain) 영역(50)에서는 DRM이 적용된 콘텐츠를 사용하기 위해 라이센스를 발급받는 과정이 이루어진다.

[0047] 이를 위해, 상기 온 체인(On-chain) 영역(50)은 스마트 컨트랙트를 생성하여 DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하고, 디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 프라이빗 영역부(510) 및 가중치를 적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증하고, 검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 연결하는 퍼블릭 영역부(530)를 포함한다.

[0048] 디지털 콘텐츠를 구매하는 사용자는 자신의 거래기록을 시크릿 블록으로 생성하게 되고, 퍼블릭 블록체인에서 다수의 검증자에 의해 합의가 이루어진다. SBBC는 도 2와 같은 과정으로 진행된다. 본 발명에서 제안하는 SBBC는 디지털 콘텐츠 거래환경의 문제점을 개선할 뿐만 아니라 블록체인을 접목 했을 때 나타나는 프라이버시, 한정된 용량 문제점 또한 개선한다.

[0049] 기존 퍼블릭 블록체인은 인증과정 없이 누구나 거래와 검증에 참여할 수 있는 환경이다. 거래 참여에 제한이 없으므로 투명성이 높고 다수의 사용자가 거래기록을 가지고 있으므로 무결성도 보장된다. 하지만, 익명성의 특징을 통해 악의적인 행위 또한 증가하고 있는데, 그 중 하나가 거짓 거래이다. 퍼블릭 블록체인에서는 모든 거래를 검증하기 때문에 거짓 거래가 늘어날수록 실제 거래에 대한 검증 대기 시간이 길어지고, 결론적으로 이는 시

스템 네트워크 부하로 이어진다.

[0050] 이러한 문제점을 개선하고자 본 발명의 시스템(1)의 사용자 인증부(110)에서는 거래 전 사용자 인증 과정이 이루어진다. 검증은 누구나 가능하지만, 거래를 위해서는 인증 과정을 거쳐 거짓 거래 발생을 방지하고자 한다.

[0051] SBBC의 참여자 중 디지털 콘텐츠를 판매하고자 하거나, 사용하고자 한다면 해당 인증과정을 거쳐야 한다. 인증과정은 도 3을 참고하여 다음과 같은 순서로 이루어진다.

[0052] 도 3을 참조하면, 먼저 시스템에 등록되어 있지 않은 사용자는 사용자 등록 과정을 거치게 된다. 사용자는 ID, PW를 설정하고 비대칭 키를 생성한다. 생성한 ID의 해시값을 솔트(Salt) 값으로 사용하여 PW와 함께 해시함수를 통해 해시값을 생성한다. 이후 사용자는 ID, PW 해시값과 공개키를 서버에 저장한다.

[0053] 사용자 등록 과정을 거친 사용자들은 거래를 원할 때 인증과정을 거치게 된다. 사용자가 서버로 인증 요청을 보내면 서버는 난수를 생성한 후 이 값을 등록된 사용자의 공개키로 암호화를 진행하여 전송한다. 사용자는 암호문을 자신의 비밀키로 복호화하여 난수를 확인한다. 서버와 사용자는 PW 해시값과 인증 요청시간을 연결한 값을 랜덤 시드(SEED)로 사용하여 랜덤값을 생성한다. PW 해시값에 해당 랜덤값을 사용하여 x값을 선택한다.

[0054] 이후 서버에서 생성한 난수 n에 x승을 계산하여 서버로 전송한다. 서버는 해당 값이 같을 경우 정상적인 사용자로 판단하고, 인증을 완료한다. 이처럼 생성된 난수를 사용자의 공개키로 암호화하여 전송하므로, 개인키가 없는 사용자는 인증에 필요한 난수 값을 알 수 없다. 또한, 인증 요청시간을 랜덤 값을 찾는 시드에 포함시키기 때문에 랜덤값의 중복을 방지한다. 랜덤값을 알지 못하면 x의 값을 계산할 수 없으므로 안전한 인증을 진행할 수 있다.

[0055] 디지털 콘텐츠 거래(Digital Content Trading)에서는 모든 정보가 0, 1의 비트 형태로 표시되는 디지털 콘텐츠는 아날로그 콘텐츠보다 다양한 형태의 프로세싱에 친화적이며 콘텐츠 사이의 상호 융합이 훨씬 쉽다. 또한, 완벽하고 무한히 복제될 수 있으며 압축을 통해 내용 손실 없이 전달 가능 하다. 하지만, 이러한 특징을 통해 불법적인 복제와 유출의 문제점이 생겨나기 시작했고, 해당 문제는 최근까지 해결되지 못하고 매년 문제점으로 대두되고 있다.

[0056] 이러한 문제점을 개선하고자 본 발명의 오프 체인(Off-chain) 영역(10)의 디지털 콘텐츠 거래 영역에서는 디지털 콘텐츠에 정당한 권리를 가진 사용자만이 디지털 콘텐츠를 사용할 수 있는 DRM을 사용하기 위해 암호화를 진행한다. 하지만, 사용자가 콘텐츠를 사용하기 위해서는 원본 상태로 복호화하는 과정이 필요하므로 '안전하지 않은 구간'이 생기게 되고, 콘텐츠가 원본 상태로 존재하는 '암호화되지 않은 상태'가 생기게 된다.

[0057] 이러한 상황에서 콘텐츠의 불법 유출이 발생할 수 있으므로 불법 유출이 발생했을 경우, 유출지를 추적할 수 있도록 디지털 핑거프린팅 삽입을 진행할 수 있다. 도 4는 본 발명에서 제안하는 디지털 핑거프린팅 적용 구조도를 보여준다.

[0058] 먼저 인증받은 콘텐츠 제공자는 자신의 콘텐츠를 서버에 전송한다. 콘텐츠를 사용하고자 하는 소비자는 인증과정을 거친 후, 디지털 콘텐츠 거래를 위해 서버로 거래를 요청한다. 이후 서버는 DRM을 적용하기 위해 비대칭키를 생성하고, 저장된 사용자의 정보를 이용하여 핑거프린팅 작업을 진행한다. 이때, 서버는 콘텐츠에 대한 비트를 랜덤한 크기로 세분화하고, 세분된 비트 중 랜덤한 장소에, 랜덤한 개수로 핑거프린트를 삽입한다.

[0059] 이는 사용자가 어떠한 위치에 핑거프린트가 삽입되었는지 알 수 없도록 하기 위함이다. 핑거프린트가 삽입된 콘텐츠는 DRM을 위해 생성된 공개키를 통해 암호화된다. 서버는 암호화된 콘텐츠와 해당 콘텐츠를 복호화할 수 있는 비밀키, 소비자의 공개키를 콘텐츠 제공자의 공개키로 암호화하여 콘텐츠 제공자에게 전송한다. 콘텐츠 제공자는 해당 소비자의 거래요청을 받아 들일 때, 소비자에게 암호화된 콘텐츠를 전송한다.

[0060] 이와 같은 순서로 진행되는 디지털 콘텐츠 거래를 통해 불법복제와 유출의 가능성을 예방한다. 또한, 핑거프린팅을 랜덤한 장소 및 개수로 삽입함으로써 악의적인 의도를 가진 사용자가 콘텐츠 내용을 변형함으로써 사용자 정보에 대한 부분을 훼손하여 유출하는 문제점을 해결할 수 있다. 따라서, 오프 체인(Off-chain) 영역(10)의 디지털 콘텐츠 거래 영역에서 안전하게 거래를 진행한 후, 온 체인(On-chain) 영역(50)을 진행한다.

[0061] 한편, 유럽연합의 개인정보보호법인 GDPR(General Data Protection Regulation)에 따르면, 사용자 모두는 자신의 개인정보 처리에 대한 동의 및 삭제 요구, 개인정보 사용 내용 등을 알 권리가 있다. 특히, IT 시스템에서 개인정보보호 개념을 준수하는 것은 개인정보 취급 시 중요한 요구사항 중 하나로 대두되고 있다. 하지만, 일부 IT 기술은 개인정보보호가 미흡한 실정이며 그 중 대표적으로 언급되는 기술이 블록체인이다. 일반적으로, 블록

체인은 모든 거래정보가 다수의 사용자에게 분산 저장되어 있으므로 삭제권을 보장하기 어렵다.

[0062] 따라서, 본 발명에서는 온 체인(On-chain) 영역(50)의 프라이빗 영역부(510)에서는 개인정보를 보호하고, 블록체인의 한정된 용량 문제를 해결한다.

[0063] 상기 프라이빗 영역부(510)는 소비자가 DRM이 적용된 콘텐츠를 사용하기 위해서 라이센스를 발급받고, 해당 거래 정보를 시크릿 블록(Secret Block)으로 생성하는 영역이다. 소비자는 라이센스를 발급받기 위해 스마트 컨트랙트를 생성한다. 이후, 콘텐츠 제공자는 암호화된 디지털 콘텐츠를 복호화할 수 있는 비밀키를 소비자의 공개키로 암호화하여 스마트 컨트랙트로 전송한다.

[0064] 스마트 컨트랙트를 통해 해당 규칙들이 포함된 라이센스가 패키징되고, 해당 라이센스는 소비자에게 전송된다. 소비자는 라이센스를 성공적으로 전달받았다면, 확인(Confirm) 메시지를 보내고, 거래내용을 시크릿 블록으로 생성한다.

[0065] 도 5는 DRM이 적용된 콘텐츠를 사용할 수 있는 라이센스 구조와 시크릿 블록(Secret Block)의 구조를 보여준다. 라이센스에는 소비자의 공개키로 암호화된 디지털 콘텐츠 복호화키와 디지털 콘텐츠의 사용시간 및 종료시각, 기간 등이 포함된 관련 규칙이 포함되어 있다. 또한, 라이센스 데이터의 무결성을 위해 해당 라이센스의 해시값이 포함된다.

[0066] 시크릿 블록에는 이전블록 해시값과 생성시간, 소비자의 사용자 인증정보와 콘텐츠 제공자의 정보가 헤더로 구성된다. 블록 바디에는 암호화된 콘텐츠와 라이센스의 정보가 저장되어 있다. 해당 블록은 소비자만이 소지하고 있으므로, 블록체인의 저장공간의 한계 문제점을 해결하며 개인 프라이버시 문제 또한 해결할 수 있다.

[0067] 기존 프라이빗 블록체인에서는 운영주체에 의해 운영되므로 운영주체를 장악하거나 권한을 도용하는 것만으로도 블록체인을 점유하여 악의적인 행동이 가능하다. 이를 방지하고자 본 발명에서 제안하는 시스템(1)의 기본 환경은 퍼블릭 블록체인으로 사용한다. 이러한 환경은 다수의 사람에게 합의를 받기 때문에 탈중앙성 및 투명성을 높일 수 있다.

[0068] 상기 온 체인 영역(50)의 퍼블릭 영역부(530)는 거래 검증 과정과 검증된 거래가 모여 블록으로 생성되는 합의 과정으로 구성된다. SBBC에서는 개인정보보호를 위해 거래정보가 저장된 시크릿 블록을 소비자만 소지한다. 따라서, 거래를 위한 검증 또한 거래정보가 없이 이루어져야 한다.

[0069] 이러한 이유로 본 발명에서는 영지식증명(Zero-knowledge Proof)를 사용한다. 영지식증명이란, 상대방에게 어떠한 정보도 제공하지 않고, 자신이 해당 정보를 가지고 있다는 사실을 증명하는 것을 말한다. 영지식증명을 활용한 대표적인 프로토콜은 슈노르 프로토콜(Schnorr Protocol)이 있다. 암호학에서 슈노르 프로토콜은 증명자가 자신의 개인 키를 공개하지 않고 이를 가지고 있다는 것을 증명하는 방법이다. 해당 프로토콜은 실제 블록체인에 많이 적용되고 있다.

[0070] 소비자는 s(라이센스 해시값)를 블록체인 네트워크의 검증자에게 공개하지 않고 자신이 s를 소지하고 있다는 것을 증명해야 한다. 증명과정은 도 6과 같다.

[0071] 도 6을 참조하면, ① 소비자는 랜덤 넘버 r을 생성하고 X를 계산한다. ② 이후, 보내고자 하는 메시지 M(Secret Block 해시값)과 계산한 X값을 연결한 후, 해싱하여 서명 e를 생성한다. ③ 또한, e와 r을 사용하여 또 다른 서명 y를 도출한다. ④ 소비자는 M과 생성된 서명 e, y를 검증자에게 전송한다. ⑤ 검증자는 M과 e, y를 통해 X'를 도출하고, 이를 통해 e'를 도출한다. ⑥ 소비자가 전송한 서명 e와 검증자가 도출한 e'가 같을 경우, 검증에 성공한다.

[0072] 본 발명의 일 실시에에서, 영지식증명의 일종인 슈노르 프로토콜을 사용하여 프라이버시를 보장한 신뢰성 있는 블록체인 네트워크 구성이 가능하다.

[0073] 거래 검증을 완료한 트랜잭션들은 일정 사이즈 및 시간만큼 모인 이후, 블록으로 생성된다. 생성된 블록은 유효성 검사를 거쳐야만 블록에 포함된 모든 거래에 대한 유효성이 승인되며, 해당 블록은 체인으로 연결될 수 있다. 이때 블록의 유효성을 검사하기 위해 합의 알고리즘을 사용하는데, 합의를 성공적으로 완료해야만 해당 블록의 모든 트랜잭션을 신뢰할 수 있다고 판정한다.

[0074] 퍼블릭 블록체인의 기본 합의 알고리즘인 PoW와 PoS는 각각 에너지 낭비, 부익부 빈익빈과 같은 문제점이 존재하며, 결제 불확실성 및 블록 생성 시간이 상대적으로 오래 걸린다는 문제점 또한 존재한다. 이러한 성능 문제를 해결한 합의 알고리즘으로 PBFT가 있다. 하지만, PBFT는 모든 합의 참여자의 의사를 고려하기 때문에 노드가

많아질수록 속도 저하 문제가 존재하기 때문에 퍼블릭 블록체인 환경에서 사용하기 알맞지 않다.

[0075] 이에, 본 발명에서 제안하는 SBBC는 인증받은 사용자와 인증받지 않은 사용자 모두가 존재하는 하는 시스템이므로 해당 환경을 고려하고, PBFT의 문제점을 해결한 새로운 합의 알고리즘인 WBFT(Weighted authentication Byzantine Fault Tolerance)를 제안한다.

[0076] WBFT는 인증받은 사용자의 가중치를 높게 부여하고, 합의를 위한 검증자를 랜덤하게 선출하여 합의를 진행한다. 예를 들어, WBFT를 진행하기 위해 인증받은 사용자의 가중치는 1.5로 설정하고, 인증받지 않은 사용자의 가중치는 1.0으로 설정할 수 있다. 가중치는 검증자를 선출할 때와 합의 결과에 대한 가중치를 의미하며, 인증받은 사용자가 검증자로 선출될 가능성이 높기 때문에 합의의 신뢰도 또한 보장한다.

[0077] 도 7과 같이 각 참여자는 인증 여부에 따라 가중치가 다르게 설정되며, 해당 가중치를 통해 랜덤으로 검증자를 선출한다. 해당 가중치는 시뮬레이션의 결과로 결정될 수 있다. WBFT는 검증자들이 무작위로 선출되기 때문에 객관적이며, 가중치를 통해 적은 수의 검증자들이 합의를 진행하기 때문에 노드가 많은 퍼블릭 블록체인 환경에서도 사용하기 적합하다.

[0078] 기존 디지털 콘텐츠 거래환경의 문제점을 개선할 뿐만 아니라, 블록체인에서 발생하는 문제점을 해결한 SBBC는 퍼블릭 블록체인을 기본 환경으로 구성되지만, 스마트 컨트랙트를 사용하여 거래를 진행하고자 하는 사용자는 반드시 인증과정을 거쳐야 한다. 이는 기존 퍼블릭 블록체인에서 빈번히 발생하고 있는 거짓 거래 발생과 거짓 거래의 유효성 검사로 인한 네트워크 부하를 방지하고자 함이다.

[0079] 도 8은 SBBC 시스템의 네트워크 구성도를 보여준다. WBFT를 사용하는 SBBC는 인증받은 사용자와 인증받지 않은 사용자 모두 거래 검증 및 블록의 유효성을 검사하는 합의에 참여하므로 원장(Ledger)에 접근 할 수 있지만, 스마트 컨트랙트에는 인증받은 사용자만이 접근하여 거래 계약서를 작성할 수 있다.

[0080] SBBC의 시크릿 블록에는 이전블록해시, 현재블록해시가 블록 헤더로 포함되어 있다. 블록 바디에는 거래내용인 암호화된 콘텐츠와 해당 콘텐츠를 실행할 수 있는 라이센스 정보가 저장되어 있다.

[0081] 도 9는 SBBC의 블록구조와 연결 구조를 보여준다.

[0082] 도 9에서 시크릿 블록 #1은 퍼블릭 블록 #3이 생성되고 난 이후 생성된 블록으로 가정한다. 시크릿 블록 #1이 생성될 시기에는 퍼블릭 블록 #3 이 원장에 기록된 마지막 블록이므로 3번 블록의 해시값이 시크릿 블록 #1의 구성요소인 '이전블록해시'로 저장된다. 이를 통해, 시크릿 블록 #1이 퍼블릭 블록 #3과 연결될 수 있다.

[0083] 시크릿 블록 #1이 생성된 이후, 해당 블록의 해시 값은 다음 블록인 퍼블릭 블록 #4의 트랜잭션으로 저장된다. 이를 통해, 시크릿 블록 #1과 퍼블릭 블록 #4를 연결할 수 있다. 퍼블릭 블록 #4와 시크릿 블록 #1에 저장된 '이전블록해시'는 모두 퍼블릭 블록 #3의 해시값을 의미한다. 따라서, 이전블록 해시값이 같은 퍼블릭 블록에 서브 블록으로 시크릿 블록을 연결할 수 있다.

[0084] SBBC는 시크릿 블록을 생성하여 거래 당사자만이 소지하고 있으므로 참여자 들은 각각 원장이 다르게 구성된다. 도 10은 SBBC의 참여자 간의 원장 구조 차이를 보여준다.

[0085] 도 10을 참조하면, 참여자 A는 자신의 거래내용이 존재하는 블록 SA_block #1과 SA_block #2를 가지고 있으며 해당 블록들은 각각 퍼블릭 블록인 Pub_block #3 과 Pub_block #5의 서브 블록으로 연결된다. 참여자 B는 SB_block #1을 소지하고 있으며 해당 블록은 Pub_block #4의 서브 블록으로 연결되어 저장된다.

[0086] 결론적으로, 퍼블릭 블록은 사용자 모두가 공통으로 가지고 있으며, 자신의 거래 횟수에 따라 시크릿 블록이 추가되는 구조라고 말할 수 있다. 디지털 콘텐츠가 저장된 시크릿 블록을 자신만이 소지하고 있으므로 블록체인의 저장용량 한계 문제를 해결하며, 사용자의 프라이버시 또한 보장된다.

[0088] 도 11은 본 발명의 일 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 방법의 흐름도이다.

[0089] 본 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 방법은, 도 1의 장치(10)와 실질적으로 동일한 구성에서 진행될 수 있다. 따라서, 도 1의 장치(10)와 동일한 구성요소는 동일한 도면부호를 부여하고, 반복되는 설명은 생략한다.

[0090] 또한, 본 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 방법은 블록체인을 활용한 디지털 콘텐츠 거래를 수행하기 위한 소프트웨어(애플리케이션)에 의해 실행될 수 있다.

[0091] 본 발명에 블록체인을 활용한 디지털 콘텐츠 거래 방법은 디지털 콘텐츠 거래환경에서 블록체인 시스템을 접목할 때 나타나는 문제점을 분석하여 새로운 블록체인 시스템인 SBBC(Secret Block based Block Chain)에서 수행된다.

[0092] SBBC는 오프 체인(Off-chain) 영역과 온 체인(On-chain) 영역으로 분리하여 정의한다. 오프 체인 영역은 인증단계를 거쳐 디지털 콘텐츠를 거래하는 부분이다. 거래되는 디지털 콘텐츠는 디지털 핑거프린트가 삽입되어 불법 유출이 발생했을 경우, 유출지를 추적할 수 있다. 또한, 콘텐츠는 암호화되어 거래되고 정당한 권리를 가진 사용자만이 디지털 콘텐츠를 이용할 수 있으므로 콘텐츠 저작자의 정당한 수입을 보장한다.

[0093] 다음으로 온 체인 영역은 디지털 콘텐츠를 사용하는데 필요한 라이센스를 발급받고, 합의 알고리즘을 사용한 검증 과정이 이루어진다. 라이센스를 발급받은 사용자는 자신의 거래내용을 시크릿 블록(Secret Block)으로 생성하여 자신의 원장에만 기록한다.

[0094] 비공개 환경에서 시크릿 블록 생성을 통해 개인정보보호를 보장하며, 블록체인에 디지털 콘텐츠를 업로드 했을 때 일어날 수 있는 네트워크 과부하를 해결하였다. 마지막으로 모든 블록체인 참여자들의 거래 검증 및 합의를 통해 퍼블릭 블록(Public Block)을 생성하여 모든 참여자의 원장에 기록하여 거래를 마무리한다.

[0095] 디지털 콘텐츠 거래환경에서 블록체인을 접목한 기존의 연구들은 디지털 콘텐츠 거래환경의 문제점에만 초점을 맞추었기 때문에 수익분배, 위/변조 문제점은 해결할 수 있다. 하지만, 블록체인 기술에 의해 발생하는 개인정보 유출 문제를 해결하지 못하였으며 블록체인의 저장공간의 한계 문제를 해결하지 못하였다는 한계점이 존재한다.

[0096] 따라서, 본 발명에서는 시크릿 블록을 생성하여 개인정보 유출 문제와 용량 한정의 문제를 해결하였으며, 결론적으로 디지털 콘텐츠 거래환경의 새로운 해결책으로 떠오른 블록체인의 기존 문제점을 해결한 SBBC를 제안하고 이를 접목함으로써 안전한 디지털 콘텐츠 거래를 가능하도록 하였다.

[0097] 도 11을 참조하면, 본 실시예에 따른 블록체인을 활용한 디지털 콘텐츠 거래 방법은, ID, PW 및 공개키를 서버에 저장하도록 마련되는 오프 체인(off-chain) 영역에서, 사용자 인증을 수행한다(단계 S10).

[0098] 사용자 인증을 수행하는 단계(단계 S10)는, 사용자에 의해 설정된 ID, PW 및 비대칭 키를 기초로 ID의 해시값을 솔트(Salt) 값으로 사용하여 PW와 함께 해시함수를 통해 해시값을 생성하는 사용자 등록할 수 있다.

[0099] 상기 사용자 인증을 수행하는 단계는, 사용자를 인증하는 단계를 더 포함할 수 있다. 사용자 인증 단계는, 사용자 등록 과정을 거친 사용자들은 거래를 원할 때 인증 요청을 보내면 난수를 생성하고, 생성된 난수의 값을 등록된 사용자의 공개키로 암호화하여 전송한다. PW 해시값과 인증 요청시간을 연결한 값을 랜덤 시드(SEED)로 사용하여 랜덤값을 생성하고, PW 해시값에 해당 랜덤값을 사용하여 x값을 선택한다. 생성한 난수의 값 n에 x승을 계산하고 사용자가 전송한 값과 같을 경우 정상적인 사용자로 판단하여 사용자 인증을 완료한다.

[0100] 사용자 거래 요청이 있는 경우(단계 S20), DRM(Digital Rights Management)을 적용하기 위해 핑거프린트가 삽입되어 암호화된 콘텐츠를 거래한다(단계 S30).

[0101] 상기 암호화된 콘텐츠를 거래하는 단계(단계 S30)는, 인증받은 콘텐츠 제공자가 콘텐츠를 서버에 전송하고, 콘텐츠를 사용하고자 하는 소비자가 인증과정을 거친 후 디지털 콘텐츠 거래를 위해 거래를 요청하는 경우, DRM을 적용하기 위해 비대칭키를 생성한다. 콘텐츠에 대한 비트를 랜덤한 크기로 세분화하고, 세분된 비트 중 랜덤한 장소에, 랜덤한 개수로 핑거프린트를 삽입한다.

[0102] 핑거프린트가 삽입된 콘텐츠를 DRM을 위해 생성된 공개키를 통해 암호화하고, 암호화된 콘텐츠와 해당 콘텐츠를 복호화할 수 있는 비밀키, 소비자의 공개키를 콘텐츠 제공자의 공개키로 암호화하여 콘텐츠 제공자에게 전송한다.

[0103] 온 체인(On-chain) 영역에서, 스마트 컨트랙트를 생성하여(단계 S40) DRM이 적용된 콘텐츠를 사용 가능하도록 라이센스를 발급하고, 디지털 콘텐츠를 거래하는 거래 정보를 시크릿 블록(Secret Block)으로 생성한다(단계 S50).

[0104] 상기 시크릿 블록으로 생성하는 단계(단계 S50)는, 콘텐츠 제공자가 암호화된 디지털 콘텐츠를 복호화할 수 있는 비밀키를 소비자의 공개키로 암호화하여 스마트 컨트랙트로 전송하고, 소비자가 라이센스를 성공적으로 전달받은 후 확인(Confirm) 메시지를 보내는 경우 거래내용을 시크릿 블록으로 생성할 수 있다.

[0105] 거래 검증을 위한 정보와 시크릿 블록의 해시값을 블록체인 참여자에게 브로드캐스팅하고(단계 S60), 가중치를

적용한 합의 알고리즘을 이용하여 블록체인 사용자들의 거래를 검증한다(단계 S70).

[0106] 이 경우, WBFT는 인증받은 사용자의 가중치를 높게 부여하고, 합의를 위한 검증자를 랜덤하게 선출하여 합의를 진행하는 WBFT(Weighted authentication Byzantine Fault Tolerance)를 사용할 수 있다(단계 S80).

[0107] 검증이 완료되면 퍼블릭 블록을 소비자를 포함하여 모든 참여자에게 브로드캐스트하고(단계 S90), 소비자는 검증이 완료된 시크릿 블록을 퍼블릭 블록(Public Block)에 참조로 연결한다(단계 S100).

[0108] 이하에서는, 본 발명의 효과를 검증하기 위한 시뮬레이션 결과를 설명한다. 블록체인 기술을 비교 분석하기 위해 각각의 환경을 구성하여 테스트를 진행하였다. PoW와 PoS 합의 알고리즘은 Window 10 Pro 환경에서 시뮬레이션이 진행되었으며, PBFT와 WBFT 합의 알고리즘은 Linux 5.0 환경에서 시뮬레이션이 진행되었다.

[0109] 먼저, PoW 합의 알고리즘을 테스트하기 위해 Python 코드로 개발된 Github의 오픈소스를 참고하여 난이도에 따른 블록 생성 시간을 확인하였다. 또한, PoS 합의 알고리즘을 테스트하기 위해 Go언어로 작성된 Github의 오픈소스를 참고하여 네트워크 통신을 위한 Netcat을 통해 검증자의 지분(Stake)에 따른 거래 검증 횟수를 확인하였다.

[0110] PBFT 합의 알고리즘은 IBM에서 제공하는 Hyperledger Sawtooth 1.1 버전의 오픈소스를 사용하였으며 Docker를 사용하여 가상환경을 구축하고 테스트를 진행하였다. Visual Studio Code를 사용하여 노드 수를 변환하며 테스트를 진행하여, PBFT 합의 알고리즘에서 노드 수에 따른 합의 실행 시간을 확인하였다.

[0111] 본 발명에서 제안하는 WBFT 합의 알고리즘 또한, IBM에서 제공하는 Hyperledger Sawtooth 1.1 버전의 오픈소스를 참고하여 합의 알고리즘 실행 시간을 확인하였고, 기존의 PBFT 알고리즘과 비교 분석을 진행하였다.

[0112] 본 시뮬레이션을 바탕으로, 디지털 콘텐츠 거래환경에 알맞은 새로운 블록체인인 SBBC에서 합의 알고리즘을 통한 안전하고 신뢰성 있는 시스템 구축을 위한 결과를 도출하고 분석하였다.

[0113] 본 발명에서 제안한 SBBC에서 사용하는 WBFT의 알고리즘의 결과를 비교 분석하고자 한다. 디지털 콘텐츠 거래환경의 문제점을 해결하기 위해 제안된 SBBC는 기존의 블록체인 알고리즘을 분석한 결과를 토대로, PoW와 PoS 합의 알고리즘의 문제점을 개선한 PBFT알고리즘을 발전시켜 적용하였다.

[0114] SBBC에서 사용하는 WBFT는 인증 여부에 따라 가중치를 다르게 적용하여 합의하는 방식이다. WBFT에서 인증받은 사용자의 인증 가중치는 인증받지 않은 사용자의 가중치보다 상대적으로 높게 설정한다. 이때, 가중치를 너무 높게 설정한 다면 인증받은 사용자만이 합의에 계속 참여할 수 있고, 이를 통한 담합 행위 및 독점 행위 등의 악의적인 행동이 가능하다.

[0115] 따라서, 인증받은 사용자의 높은 참여를 통해 신뢰성을 높이지만, 악의적인 행동을 방지하도록 적절한 가중치 설정이 중요하다. 공정성 평가는 아래의 수학식 1과 같이 계산될 수 있다.

[0116] [수학식 1]

[0117] $$f_a = \frac{\sum_{i=1}^{n}(k \cdot f(i) + b)}{n}$$

[0119] 여기서, f_a는 평균 공정성, k는 공정성 감소계수(w-1.0), f(i)는 인증 받은 노드의 합의 참여 횟수, b는 공정성 수준(b=1.0), n은 전체 합의 횟수로 정의된다.

[0120] 해당 알고리즘에서 공정성의 수준(b)은 모든 노드가 공정한 상태의 가중치인 1.0으로 설정할 수 있다. 또한, 공정성 감소 계수(k)는 공정한 상태인 1.0과의 차이 값으로 설정하고, 인증받은 노드의 합의 참여 횟수(())를 계산하여 알고리즘에 대입한다. 이를 기반으로 가중치에 따른 노드 공정성을 확인하였다.

[0121] 도 12는 해당 알고리즘을 적용하여 가중치에 따른 노드 공정성 측정값을 보여준다. SBBC는 인증받은 사용자와 인증받지 않은 사용자 모두가 공존하는 시스템이다. 따라서, 인증받은 사용자의 비율을 높여가며 시뮬레이션을 진행하였다. 또한, 블록체인 네트워크에서 50% 이상을 점유할 때 블록 내용의 조작이 가능하므로 공정성에 따른

가중치 설정에서 50%를 임계 값으로 설정하였다.

[0122] 시뮬레이션 결과에 따르면, SBBC에서 인증받은 사용자가 전체의 90% 존재할 때, 공정성이 급격하게 감소하는 것을 확인할 수 있으며, 가중치 1.6 이상이 된다면 공정성이 50% 이하로 떨어지는 것을 확인할 수 있다. 따라서, 인증받은 사용자가 많은 상황인 Worst Case를 고려하여 SBBC에서 인증받은 사용자의 합의 가중치는 1.5 로 설정한다.

[0123] 본 시뮬레이션은 블록체인 네트워크에서 합의에 참여하는 노드를 5개씩 증가시키면서 진행하였다. 도 13은 PBFT와 WBFT의 노드 수에 따른 합의 실행시간 비교 결과를 보여준다. 노드 수가 많아질수록 실행 시간이 증가하지만, WBFT 합의 알고리즘은 PBFT 합의 알고리즘보다 평균적으로 적은 시간이 소요되는 것을 확인할 수 있다. 이는 인증받은 사용자의 합의 가중치를 통해 PBFT보다 더 적은 수의 노드가 선별되어 합의를 진행하기 때문이다.

[0124] 도 14는 SBBC 시스템에서 인증받은 사용자 비율에 따른 합의 실행 시간 비교를 보여준다. 전체 사용자 중 인증받은 사용자의 비율이 높아질수록, 합의를 위해 선출되는 노드 수가 적기 때문에 합의 실행시간이 감소 것을 확인할 수 있다. 특히, 인증받은 사용자의 비율이 70%만 되어도 기존의 PBFT 합의 알고리즘보다 약 40% 합의 실행시간이 개선된 것을 확인할 수 있다.

[0125] 결론적으로, 본 발명에서 제안한 WBFT 합의 알고리즘에서 다수의 사용자가 합의에 참여할 때, 인증된 사용자의 수가 많을수록 전체적인 속도 감소와 높은 처리량을 확인할 수 있다. 인증된 사용자의 가중치 설정과 높은 참여를 통해 안전하고 신뢰성 있는 합의를 보장한다. 따라서, 노드 수가 많은 퍼블릭 블록체인 환경에서도 BFT 합의 알고리즘을 사용할 수 있음을 확인하였다.

[0126] 한편, IT 보안을 위해 정보 시스템은 무단 변경으로부터 보호되어야 하는 무결성과 허가된 사용자는 서비스를 원하는 시간에 받아야 하는 가용성, 마지막으로 허가된 자에 의해서만 접근할 수 있게 하는 기밀성을 보장해야 한다. 또한, 유럽의 개인정보보호법인 GDPR(General Data Protection Regulation)을 준수하여 개인정보에 대한 보호 개념을 준수하는 것도 중요한 보안요소로 고려되고 있다. 블록체인은 모든 거래내용이 블록으로 생성되어 체인 형태로 저장되고, 분산되어 기록되기 때문에 위조나 변조를 할 수 없으므로 무결성이 보장된다.

[0127] 따라서, 본 발명에서 제안한 SBBC는 퍼블릭 블록체인을 기본 구조로 구성되기 때문에 블록체인의 강점인 투명성과 데이터 무결성의 특징이 보장된다. 이때, 퍼블릭 블록체인을 사용할 경우 누구나 거래를 생성하고 검증할 수 있기 때문에 거짓 거래가 발생한다. 거짓 거래의 유효성 검사를 위해 실제 거래의 유효성 검사 대기 시간이 증가하고, 이를 통한 네트워크 부하가 나타나 가용성 저하 문제가 발생한다. 따라서, 본 발명에서는 인증된 사용자만이 거래를 진행할 수 있도록 구성하여 가용성 감소 문제를 해결했다.

[0128] 또한, SBBC는 시크릿 블록을 통해 거래내용은 거래 당사자만이 확인할 수 있으므로 기밀성을 보장함과 동시에 시크릿 블록은 당사자만 소지하고 있으므로 개인정보 유출에 대한 문제점도 해결할 수 있다. 이러한 특징을 가진 SBBC는 인증받은 사용자와 인증받지 않은 사용자 모두가 존재하는 하는 시스템이므로 해당 환경을 고려한 합의 알고리즘 WBFT를 제안한다.

[0129] WBFT는 인증받은 사용자가 상대적으로 높은 가중치를 적용되어 합의에 참여하므로 합의에 신뢰도를 높였으며, 기존 퍼블릭 블록체인의 대표적 합의 알고리즘의 문제점인 합의 속도 문제 또한 개선하였다. 안전한 디지털 콘텐츠 거래환경을 구축하기 위해 제안된 SBBC는 큰 용량의 디지털 콘텐츠를 거래할 때 발생하는 블록체인의 저장 공간 한계 문제를 해결한다. 또한, 블록체인 뿐만 아니라 DRM, 디지털 핑거프린팅 기술을 사용하여 기존의 디지털 콘텐츠 거래환경의 문제점인 불법복제 및 유출 문제 또한 해결하였다.

[0130] 정보화 시대가 도래하면서 가상현실, 증강현실, 혼합현실과 같은 다양한 형태의 디지털 콘텐츠가 등장하였다. 이를 통해 디지털 콘텐츠의 시장 규모와 소비량이 증가하게 되었고, 디지털 콘텐츠에 대한 중요성도 높아지고 있다. 하지만, 디지털 콘텐츠는 네트워크망을 통해 유통되므로 불법복제 및 유출이 쉬우며, 수익 분배, 위변조 등의 문제점이 계속해서 지적되고 있다. 이러한 문제점을 해결할 수 있는 새로운 해결책으로 블록체인이 대두되고 있다. 블록체인은 지속 가능한 개발을 위한 첨단 기술 중 하나로 소개되고 있으며, 현재 AI, 바이오(Bio), 재생 에너지 산업 등 여러 분야에서 접목 연구가 활발하게 이루어지고 있다.

[0131] 하지만 블록체인 또한 한계점이 존재한다. 특히 디지털 콘텐츠와 같은 대용량의 데이터를 저장할 수 없는 문제점을 가지고 있으며, 거래내용이 모두 블록에 저장되어 분산되기 때문에 개인정보보호가 미흡한 문제가 발생한다. 이를 해결하기 위해 본 발명에서는 오프 체인(Off-chain) 영역과 온 체인(On-chain) 영역으로 나누어 정의된 SBBC(Secret Block based BlockChain) 시스템을 제안하여 안전하고 신뢰성 있는 디지털 콘텐츠 거래환경을

구축하고자 하였다.

[0132] 먼저 오프 체인 영역에서는 데이터 가용성과 디지털 콘텐츠의 불법복제 및 유출 문제를 방지하기 위해 사용자 인증과 디지털 핑거프린팅이 삽입된 콘텐츠 거래를 통해 안전성을 제공한다. 다음 영역인 온 체인 에서는 데이터의 기밀성 및 무결성, 개인정보보호를 보장하기 위해 블록체인 네트워크 내에서 거래가 이루어지며, 거래 당사자만 소지하는 시크릿 블록 생성과 다수의 사용자에게 합의가 이루어진다. 또한, 해당 환경을 고려한 인증 여부에 따른 합의 가중치를 설정하여 합의하는 WBFT(Weighted authentication Byzantine Fault Tolerance) 합의 알고리즘을 제안하여 신뢰성 향상을 보였다.

[0133] 따라서, 본 발명에서는 디지털 콘텐츠 거래환경의 새로운 해결책으로 주목받은 블록체인을 기존의 문제점을 해결하여 접목함으로써 안전성과 신뢰성을 보장할 수 있다.

[0134] 이와 같은, 블록체인을 활용한 디지털 콘텐츠 거래 방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.

[0135] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거니와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.

[0136] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.

[0137] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0138] 이상에서는 실시예들을 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.

산업상 이용가능성

[0140] 콘텐츠의 디지털화 및 네트워크화로 인하여 미디어 콘텐츠 산업은 급격하게 변화하였고, 디지털 콘텐츠를 이용한 영상 스트리밍 플랫폼, 인터넷 방송 플랫폼 등 새로운 분야의 사업이 등장하고 있다. 디지털 콘텐츠는 기존의 아날로그 콘텐츠와 달리 네트워크망을 통해 빠르고 편리하게 유통 할 수 있다는 특징이 있으며, 압축 등의 기술을 통해 축소화하여 저장할 수 있으므로 보관이 쉬운 특성으로 언제, 어디에서나 사용할 수 있다는 장점이 있다.

[0141] 또한, 생산자와 소비자로 크게 구분되는 것이 아니라 정보 이용자가 정보 제공자가 되는 상호작용이 가능하다. 이를 통한 개인화, 지식화는 더 많은 부가가치를 창출하는 바탕이 된다. 특히, 4차 산업 혁명의 초연결, 실감화 환경은 전통적 콘텐츠의 디지털화를 넘어 혁신적인 ICT(Information & Communication Technology) 기술과 융합을 통해 새로운 시장과 산업을 창출할 것으로 예상된다.

[0142] 또한, 콘텐츠 산업은 방송/통신 인프라 개선 및 모바일 기기 보급 증가로 인하여 지속적인 성장을 유지하며 차세대 핵심 산업으로 거듭나고 있다. 콘텐츠 시장의 증가에 따른 디지털 콘텐츠의 비중 또한 높아지고 있으며, 디지털 콘텐츠의 시장규모는 시간이 갈수록 점점 증가할 것으로 예상된다.

[0143] 본 발명에서 제안하는 SBBC는 디지털 콘텐츠 거래환경뿐만 아니라 개인정보보호가 중요한 의료 시스템, 다수가 참여해야 하지만 거래 처리 속도가 중요한 물류 시스템 등에서 적용할 수 있을 것으로 예상된다.

부호의 설명

[0145] 1: 블록체인을 활용한 디지털 콘텐츠 거래 시스템

10: 오프 체인(Off-chain) 영역

50: 온 체인(On-chain) 영역

110: 사용자 인증부

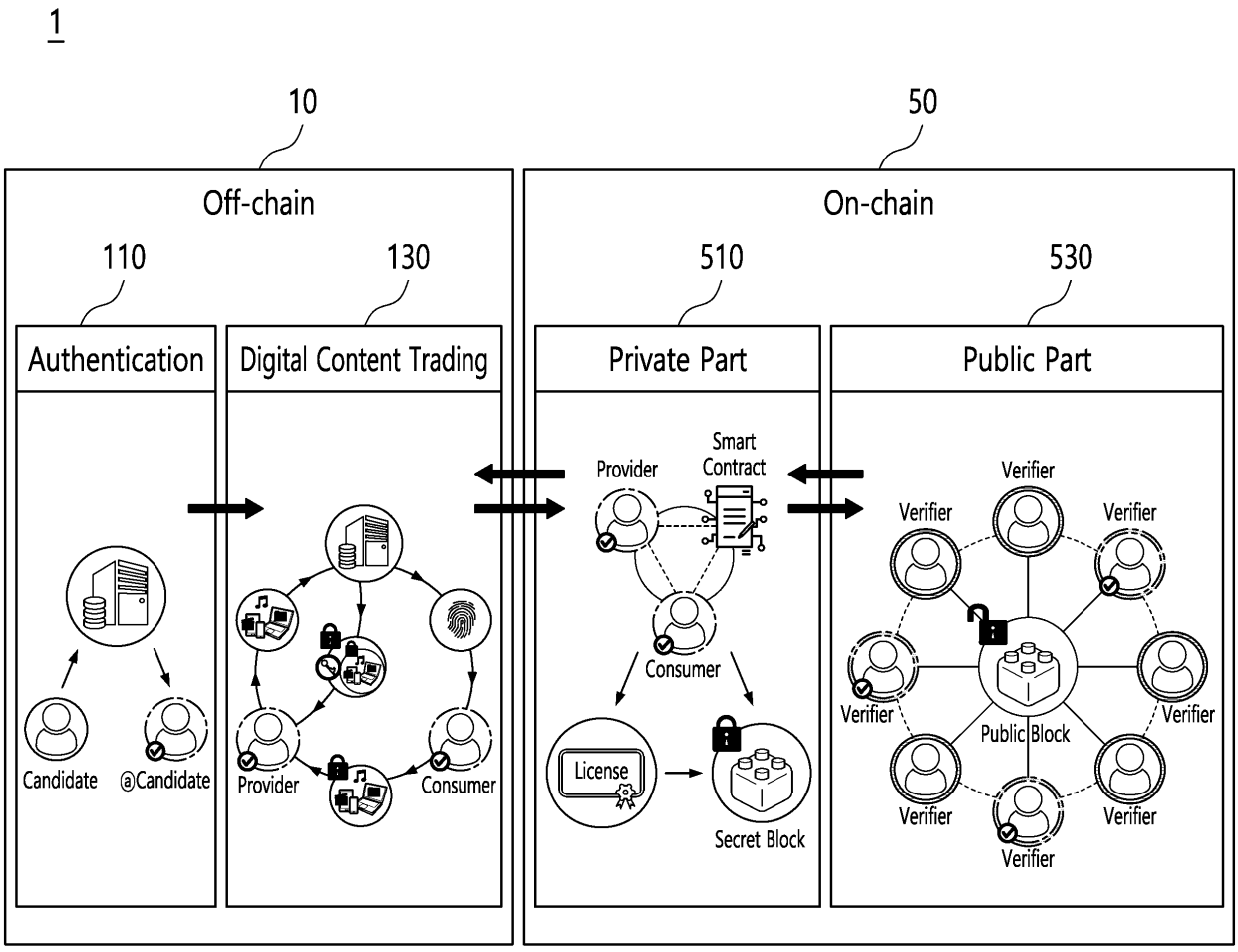
130: 디지털 콘텐츠 거래부

510: 프라이빗 영역부

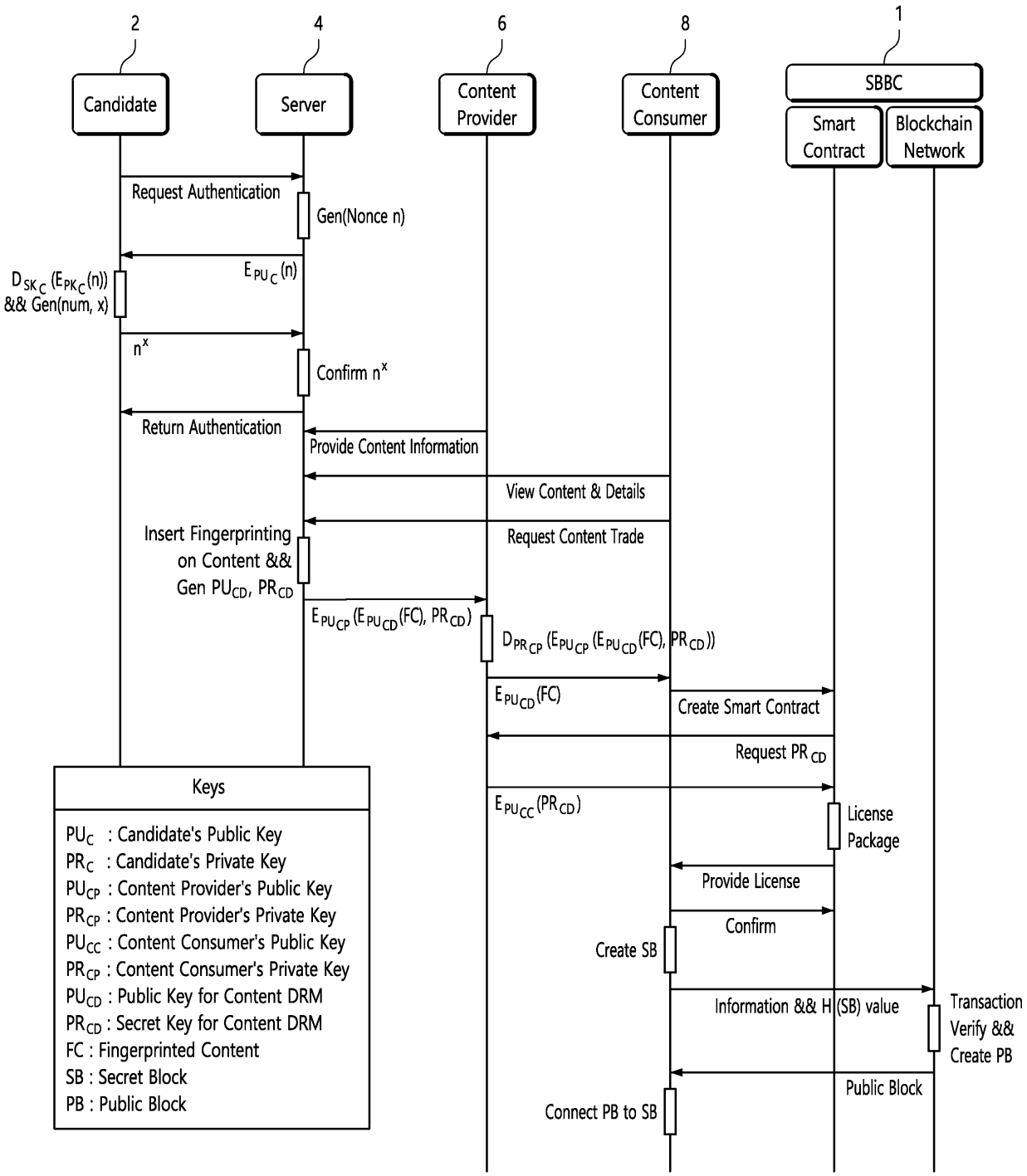
530: 퍼블릭 영역부

도면

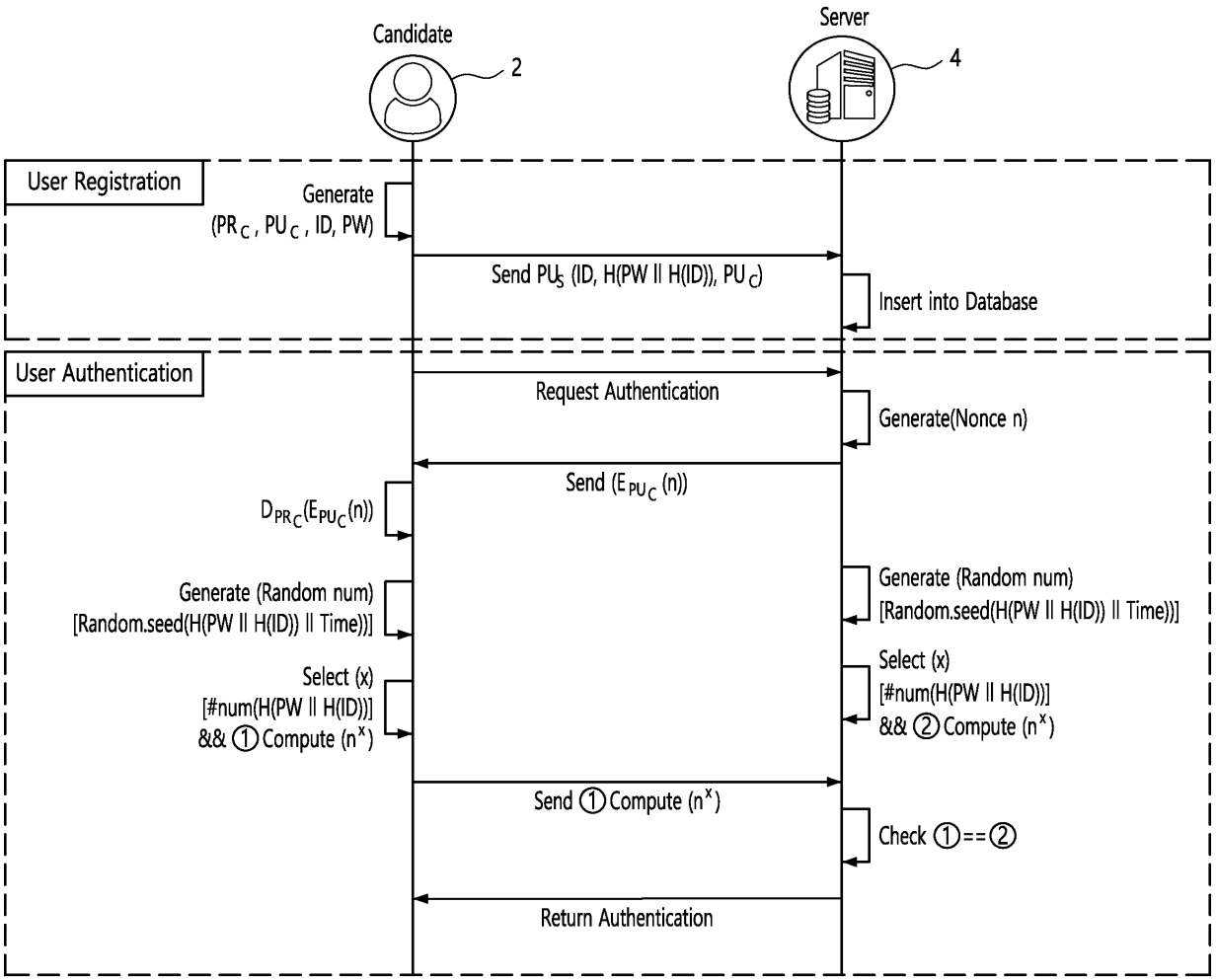
도면1



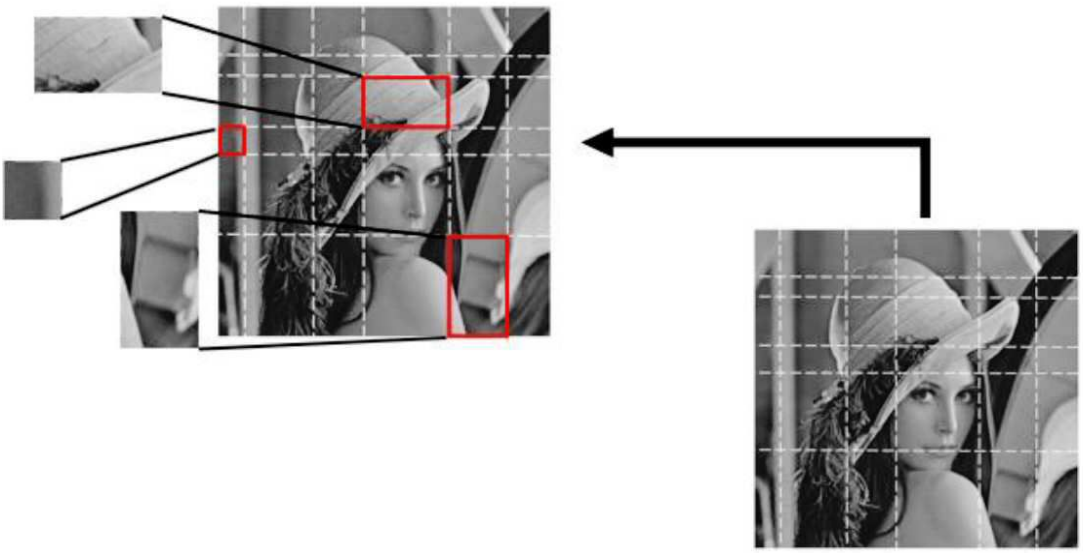
도면2


2
4
6
8
1
Candidate
Server
Content Provider
Content Consumer
SBBC
Smart Contract
Blockchain Network
Request Authentication
Gen(Nonce n)
$E_{PU_C}(n)$
$D_{SK_C}(E_{PK_C}(n))$ && Gen(num, x)
n^x
Confirm n^x
Return Authentication
Provide Content Information
View Content & Details
Request Content Trade
Insert Fingerprinting on Content && Gen PU_{CD}, PR_{CD}
$E_{PU_{CP}}(E_{PU_{CD}}(FC), PR_{CD})$
$D_{PR_{CP}}(E_{PU_{CP}}(E_{PU_{CD}}(FC), PR_{CD}))$
$E_{PU_{CD}}(FC)$
Create Smart Contract
Request PR_{CD}
$E_{PU_{CC}}(PR_{CD})$
License Package
Provide License
Confirm
Create SB
Information && H(SB) value
Transaction Verify && Create PB
Public Block
Connect PB to SB
Keys
PU_C : Candidate's Public Key
PR_C : Candidate's Private Key
PU_{CP} : Content Provider's Public Key
PR_{CP} : Content Provider's Private Key
PU_{CC} : Content Consumer's Public Key
PR_{CP} : Content Consumer's Private Key
PU_{CD} : Public Key for Content DRM
PR_{CD} : Secret Key for Content DRM
FC : Fingerprinted Content
SB : Secret Block
PB : Public Block

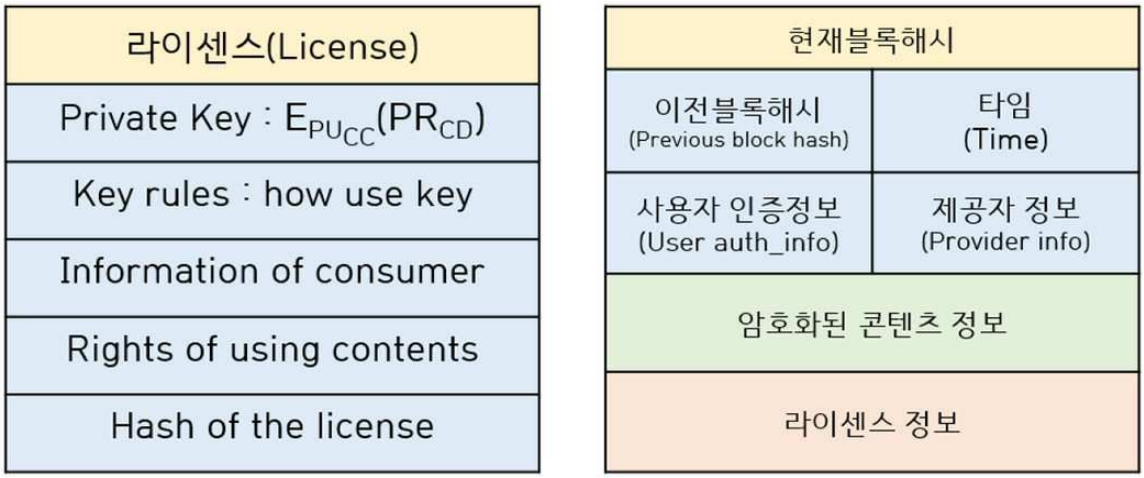
도면3


Candidate
2
Server
4
User Registration
Generate
(PR C , PU C , ID, PW)
Send PU S (ID, H(PW || H(ID)), PU C)
Insert into Database
User Authentication
Request Authentication
Generate(Nonce n)
Send (E PU C (n))
D PR C(E PU C(n))
Generate (Random num)
[Random.seed(H(PW || H(ID)) || Time))]
Generate (Random num)
[Random.seed(H(PW || H(ID)) || Time))]
Select (x)
[#num(H(PW || H(ID))]
&& ① Compute (n x)
Select (x)
[#num(H(PW || H(ID))]
&& ② Compute (n x)
Send ① Compute (n x)
Check ①==②
Return Authentication

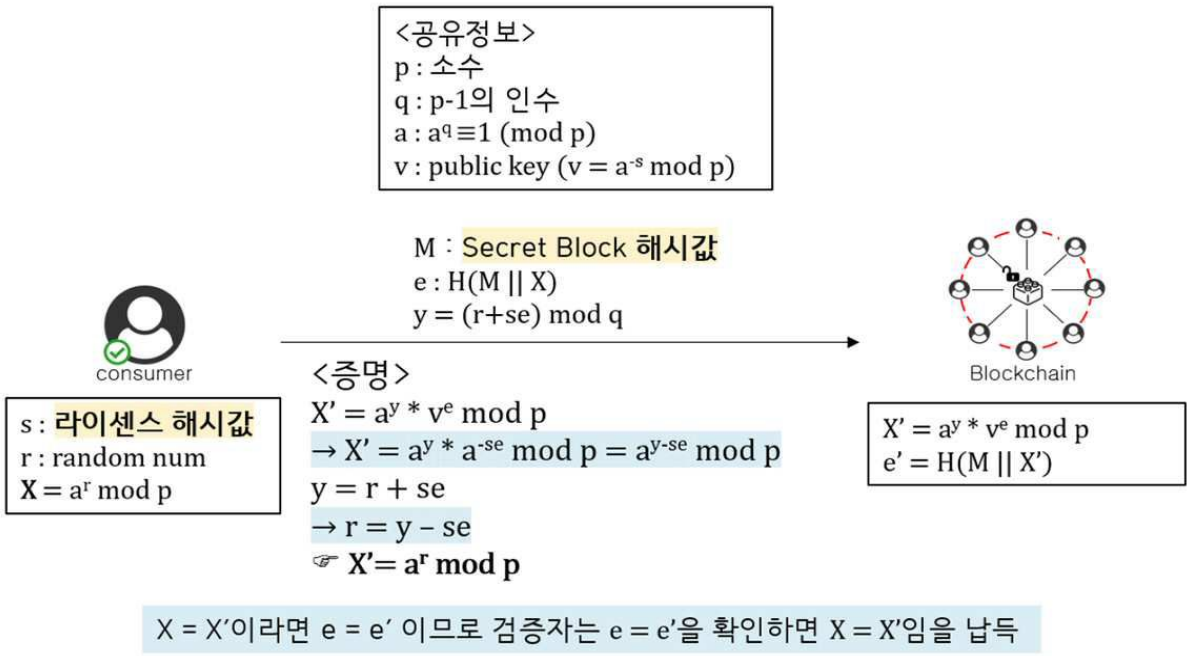
도면4



도면5

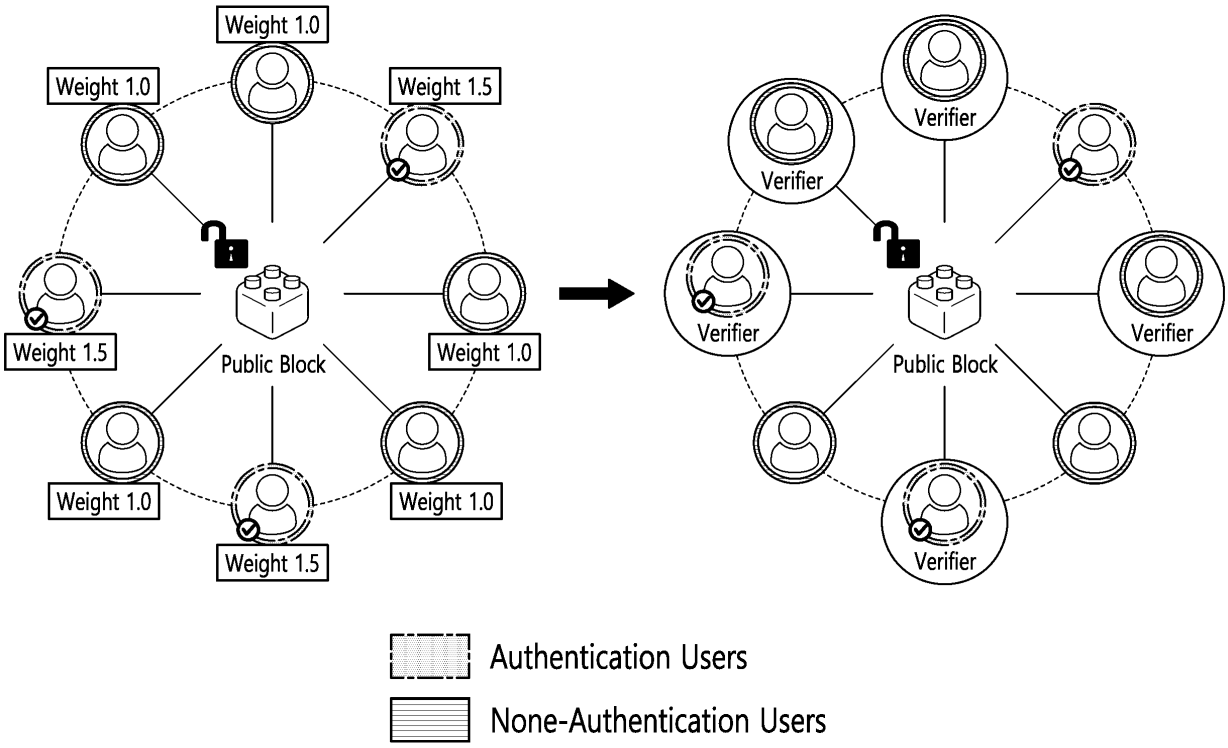


도면6

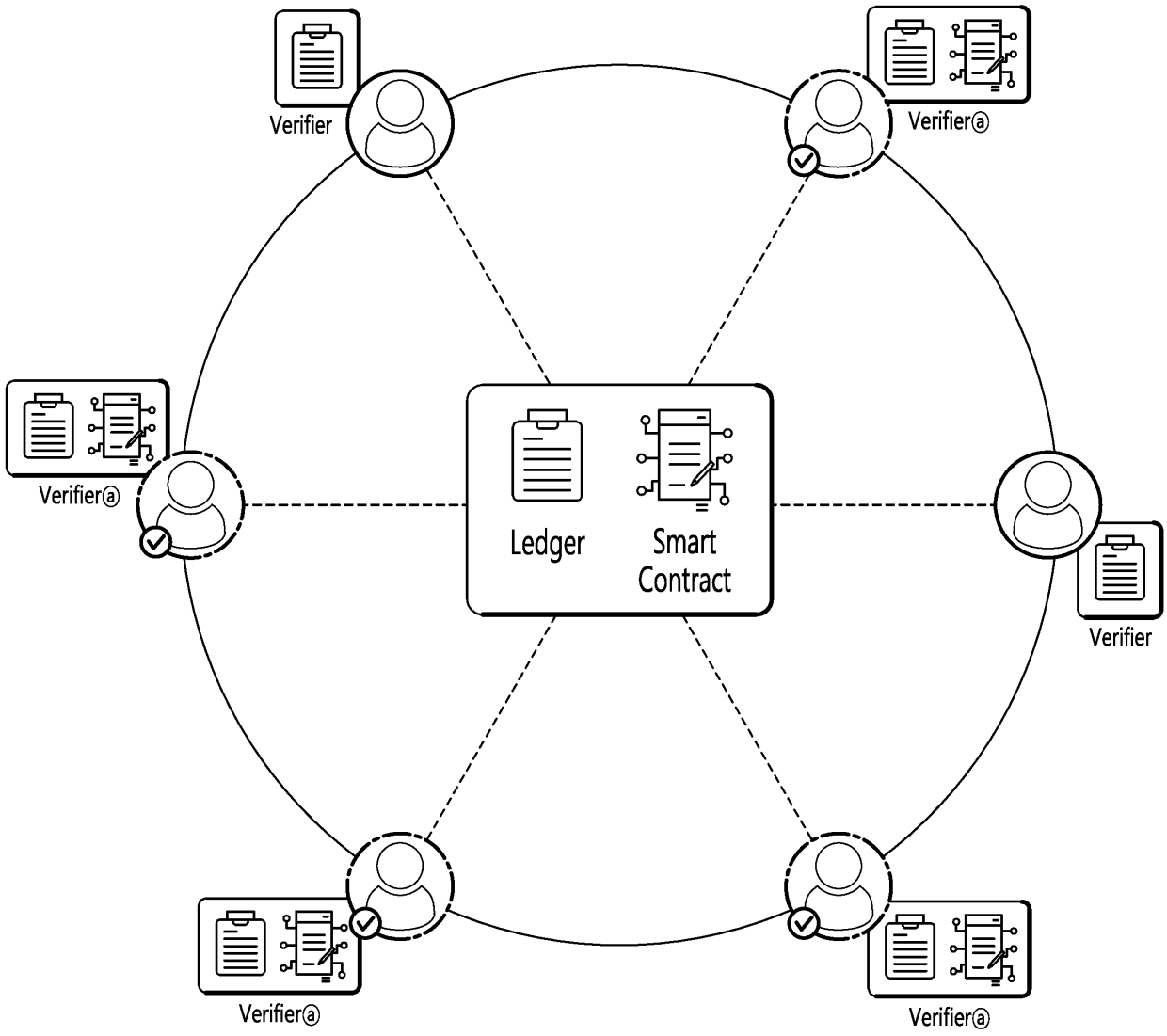


X = X'이라면 e = e' 이므로 검증자는 e = e'을 확인하면 X = X'임을 납득

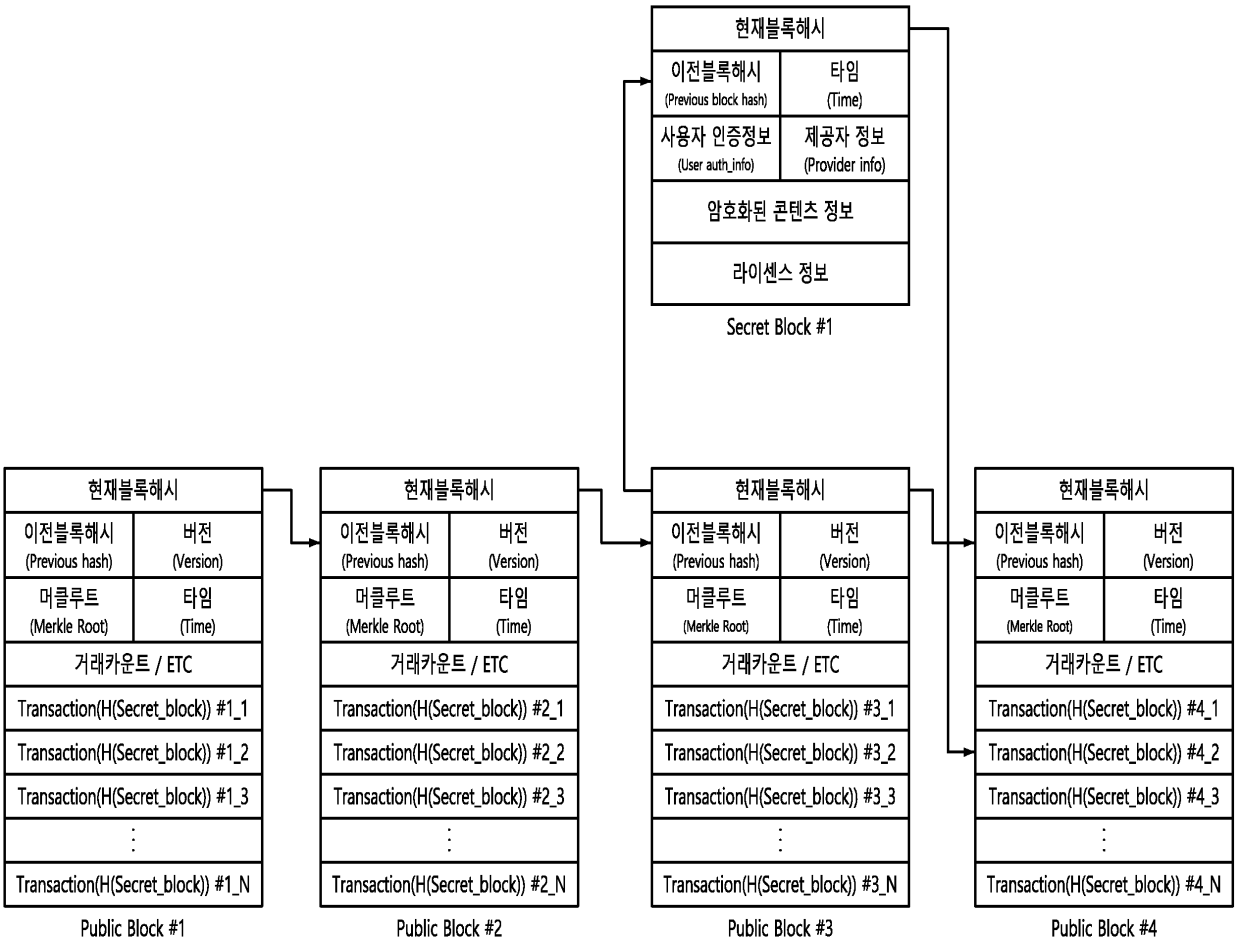
도면7


Weight 1.0
Weight 1.0
Weight 1.5
Weight 1.5
Public Block
Weight 1.0
Weight 1.0
Weight 1.0
Weight 1.5
Verifier
Verifier
Verifier
Verifier
Public Block
Verifier
Verifier
Authentication Users
None-Authentication Users

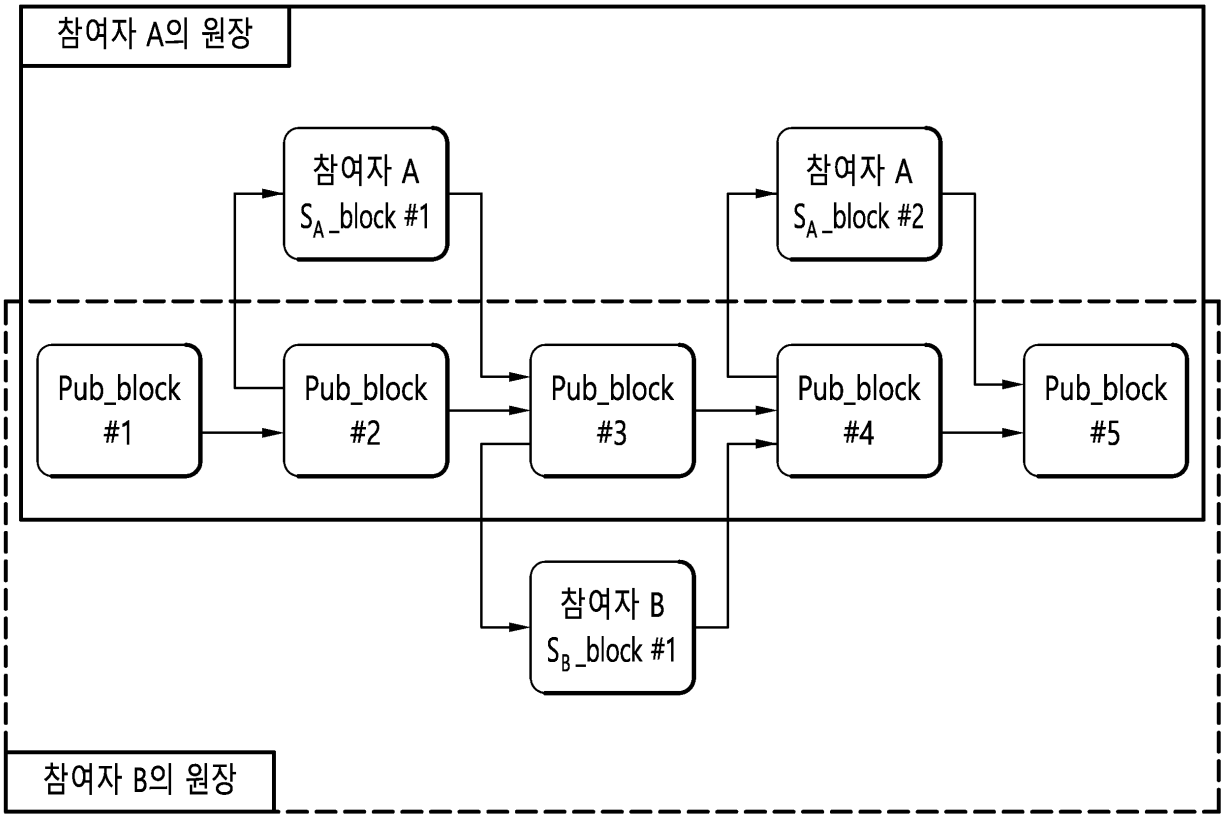
도면8


Verifier
Verifier@
Verifier@
Ledger
Smart Contract
Verifier
Verifier@
Verifier@

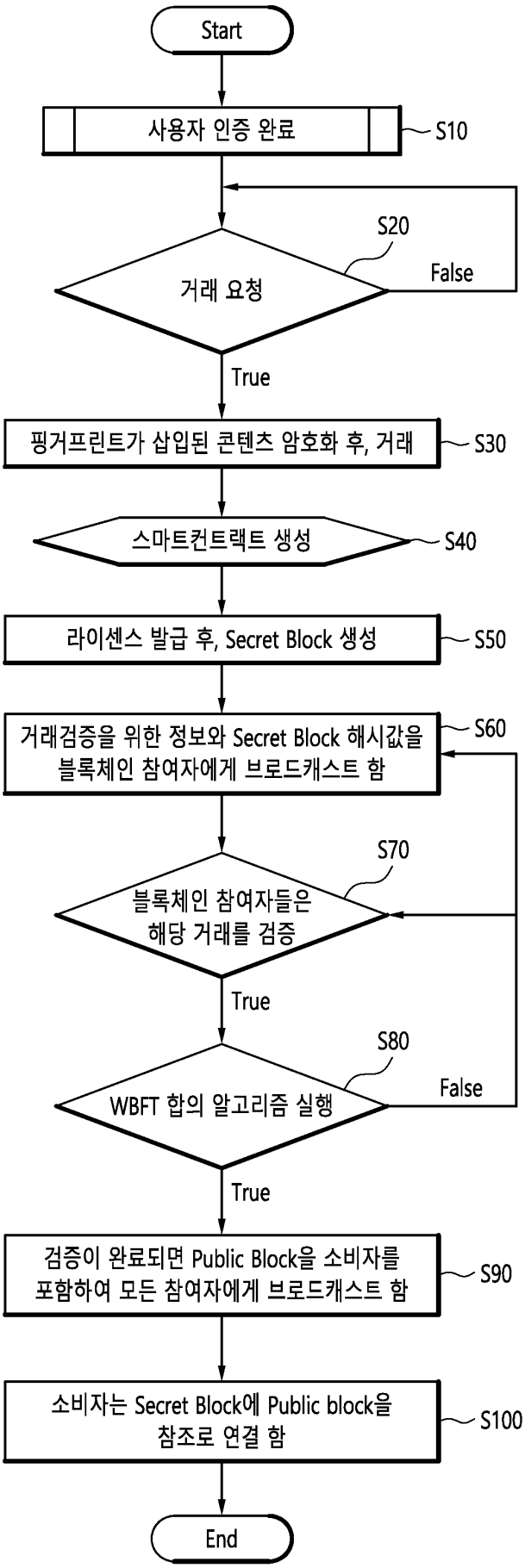
도면9


현재블록해시
이전블록해시 (Previous block hash)
타임 (Time)
사용자 인증정보 (User auth_info)
제공자 정보 (Provider info)
암호화된 콘텐츠 정보
라이센스 정보
Secret Block #1
현재블록해시
이전블록해시 (Previous hash)
버전 (Version)
머클루트 (Merkle Root)
타임 (Time)
거래카운트 / ETC
Transaction(H(Secret_block)) #1_1
Transaction(H(Secret_block)) #1_2
Transaction(H(Secret_block)) #1_3
Transaction(H(Secret_block)) #1_N
Public Block #1
Transaction(H(Secret_block)) #2_1
Transaction(H(Secret_block)) #2_2
Transaction(H(Secret_block)) #2_3
Transaction(H(Secret_block)) #2_N
Public Block #2
Transaction(H(Secret_block)) #3_1
Transaction(H(Secret_block)) #3_2
Transaction(H(Secret_block)) #3_3
Transaction(H(Secret_block)) #3_N
Public Block #3
Transaction(H(Secret_block)) #4_1
Transaction(H(Secret_block)) #4_2
Transaction(H(Secret_block)) #4_3
Transaction(H(Secret_block)) #4_N
Public Block #4

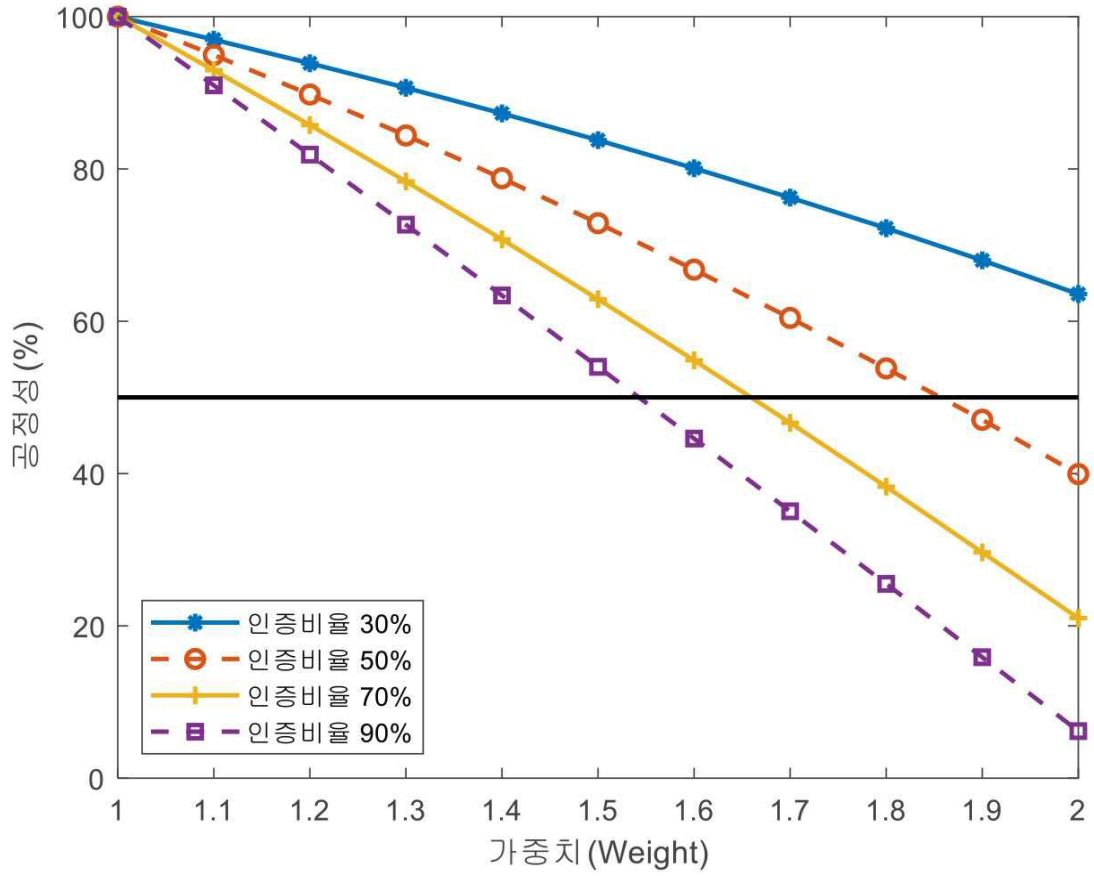
도면10


참여자 A의 원장
참여자 A
S_A_block #1
참여자 A
S_A_block #2
Pub_block
#1
Pub_block
#2
Pub_block
#3
Pub_block
#4
Pub_block
#5
참여자 B
S_B_block #1
참여자 B의 원장

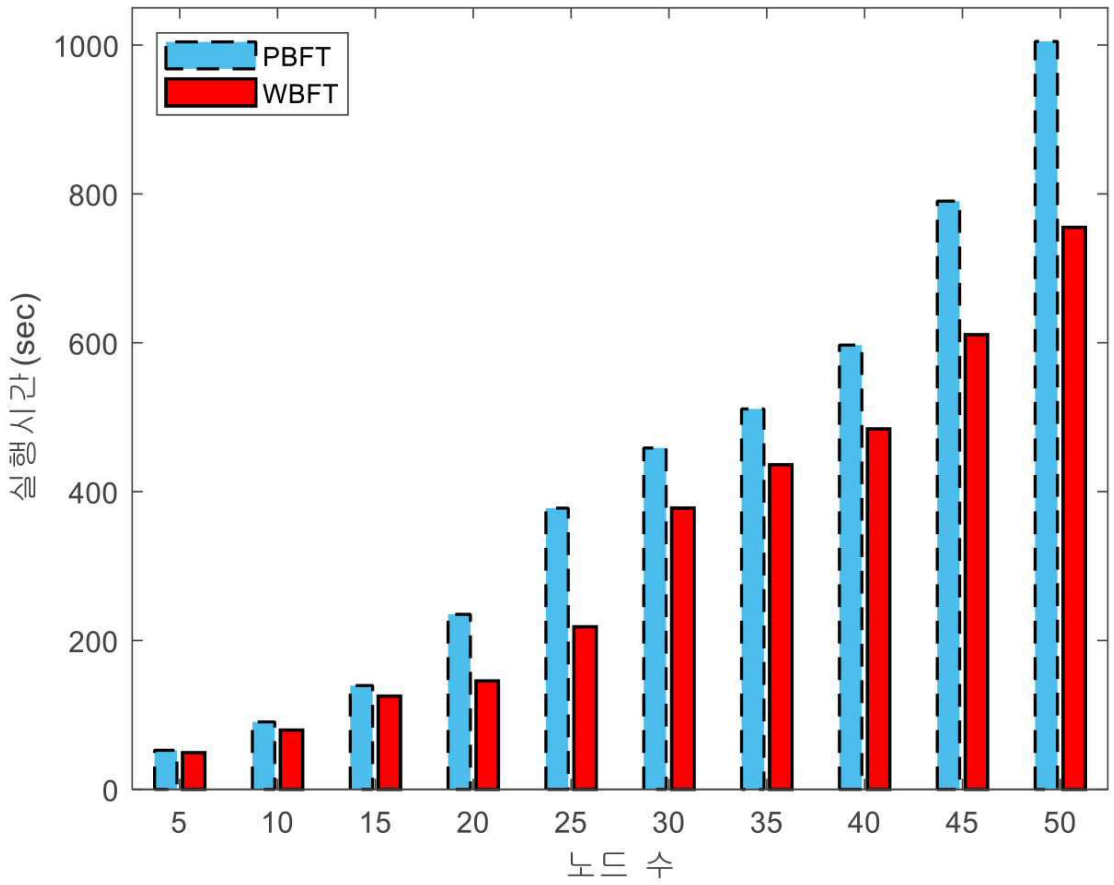
도면11


Start
사용자 인증 완료
S10
S20
거래 요청
False
True
핑거프린트가 삽입된 콘텐츠 암호화 후, 거래
S30
스마트컨트랙트 생성
S40
라이센스 발급 후, Secret Block 생성
S50
거래검증을 위한 정보와 Secret Block 해시값을
블록체인 참여자에게 브로드캐스트 함
S60
S70
블록체인 참여자들은
해당 거래를 검증
True
S80
WBFT 합의 알고리즘 실행
False
True
검증이 완료되면 Public Block을 소비자를
포함하여 모든 참여자에게 브로드캐스트 함
S90
소비자는 Secret Block에 Public block을
참조로 연결 함
S100
End

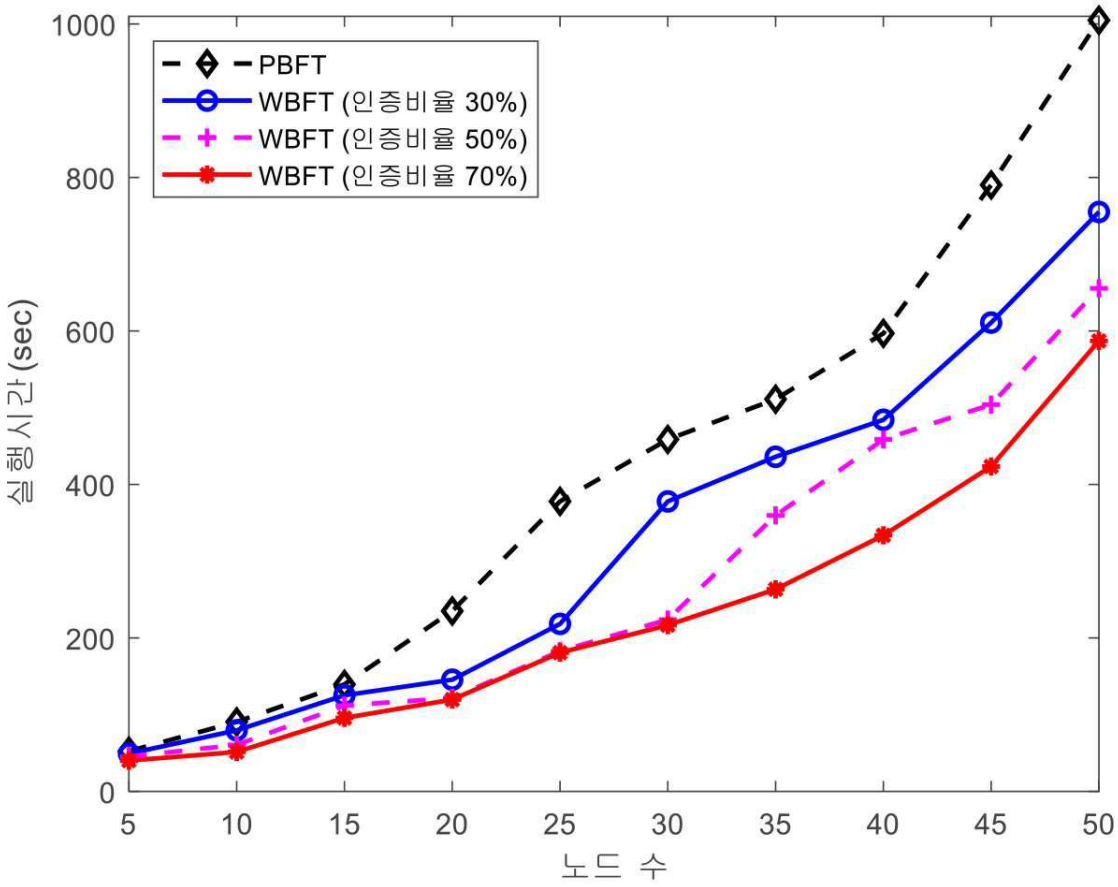
도면12


100
80
60
40
20
0
공정성 (%)
1
1.1
1.2
1.3
1.4
1.5
1.6
1.7
1.8
1.9
2
가중치 (Weight)
인증비율 30%
인증비율 50%
인증비율 70%
인증비율 90%

도면13


PBFT
WBFT
1000
800
600
400
200
0
실행시간(sec)
5
10
15
20
25
30
35
40
45
50
노드 수

도면14


PBFT
WBFT (인증비율 30%)
WBFT (인증비율 50%)
WBFT (인증비율 70%)
실행시간 (sec)
노드 수
0
200
400
600
800
1000
5
10
15
20
25
30
35
40
45
50