처음 배우는 블록체인

4장. 블록체인 2.0과 스마트 계약 플랫폼

4.1 블록체인 2.0과 알트코인

내용: 블록체인 2.0 사례, 알트코인, 알트체인

용어: 메인넷, 테스트넷, 코인, 토큰

- 메인넷: 독립적인 암호화폐로 인정하는 프로그램을 출시, 운용하는 네트워크
- 테스트넷: 블록체인 애플리케이션 개발할 때 사용하는 메인넷과 같은 구조의 네트워크
- 코인: 메인넷이 있는 블록체인(또는 다른 암호화폐) 시스템에서 발행한 암호화폐
- 토큰: 메인넷의 블록체인 시스템을 빌려 독자적인 암호화폐를 발행. 토큰 사용이 활발해지면 별도 메인넷을 만들어 코인으로 승격
- [그림4-1] 블록체인 2.0과 알트코인

4.1.1 블록체인 2.0

블록체인이 할 수 있는 것

- 디지털 데이터 소유자 정의
- 거래 증명
- P2P 네트워크에서 소유권을 양도
- 블록체인 특징 이용해 귀금속, 보석, 주식 등의 거래 내역을 디지털화하려는 움직임
- 비트코인 스크립트라는 프로그램 언어로 유연하게 사용 가능

컬러드 코인

- BTC를 특정 자산과 연결해 별도의 가치를 부여
- 비트코인과는 다른 ‘색', 예를 들어 ‘BTC’를 ‘한빛코인'으로 여기도록 프로토콜을 변경해 활용
- 컬러드코인을 바탕으로 구현한 프로토콜: EPOBC, Open Assets => 서로 호환하지 않음
- 비트코인 기반이므로 적지만 수수료 발생
- 10분에 1회라는 블록 간격을 준수해야 하는 제약

옴니

- 비트코인의 블록체인 안에서 자체 암호화폐를 만들어 특정 자산과 연결해 거래하려는 플랫폼 개발 프로젝트
- OMNI라는 암호화화폐를 발행
- 분산 거래 시스템을 이용해 다른 블록체인 플랫폼의 암호화폐와 교환 가능
- 옴니 플랫폼 기반으로 자체 암호화폐 만든 예: 메이드세이프 - 개인이 소유한 CPU, 메모리, 저장공간 등의 컴퓨팅 지원을 암호화폐에 담아 P2P네트워크에서 거래
- ICO (Initial Coin Offering) 진행해 운영 자금을 받았음

4.1.2 알트코인

- Alternative Coin의 준말로 비트코인을 대체할 수 있는 암호화폐를 뜻함

라이트코인

- 비트코인의 블록체인 기반으로 새롭게 만든 플랫폼, LTC라는 코인 있음
- 블록 간격을 약 2.5분에 1번으로 설정해 비트코인보다 간편하게 채굴할 수 있는 것이 목표
- 비트코인보다 4배가량 빠른 속도로 블록을 생성하므로 블록 생성 반감기도 4배인 84만 블록으로 설정되어 있음
- 4년에 한 번씩 보상 금액이 줄어드는 점음 비트코인과 같음
- 스크립트라는 비교적 복잡한 합의 알고리즘을 사용해 채굴 독점을 막으려 했으나, 스크립트용 ASIC이 개발되어 실패

익명 암호화폐

- 익명성 강화한 암호화폐: 대시, 모네로, Z캐시, 코인: DASH, XMR, ZEC
- 대시: 송금의 익명성을 높이려고 믹싱(Mixing)이라는 방식으로 거래를 실행
- 믹싱: 어떤 두 사람이 직접 거래하는 것이 아니라 거래 풀을 이용. 거래풀 이용하는 사용자가 어느 정도 있어야 효과
- 모네로: 링 서명(Ring Signature)으로 사람 사이의 거래 익명성을 높임. 링 서명은 여러 사람이 그룹 하나를 형성해서 거래에 서명 => 거래 하나를 여러 거래로 나눈 후 그룹에 있는 사람이 개별적으로 서명
- 크립토노트: 모네로의 이중 지급의 막는 프로토콜
- Z캐시: 대시, 모네로와 달리 거래 내역을 완전히 숨겨 거래 익명성 보장. 정보가 있는지를 제3자가 증명하는 암호화 기술

비트코인 캐시

- 비트코인의 블록 용량 제한을 없애려고 기존 비트코인을 하드포크한 알트코인
- 예: BCH 코인
- 비트코인의 블록 용량은 약 1MB로 설정되어 있음. 블록 하나를 생성하는 10분 동안 1초에 최대 7번 거래만 처리 가능.
- 비트코인 단점: 중간에 블록 용량을 변경하면 이전 블록과 호환하지 않아 잘못된 블록으로 처리
- 하드 포크: 기존 사용자가 찬성하면 하드 포크한 블록체인 시스템을 인정
- 아니면 새로운 블록체인 시스템으로 나뉨 (예: 블록 용량을 늘리는 것 => BTC와 BCH)
- 포크 코인: 기존의 암호화폐를 하드 포크해 만든 새 암호화폐, 기존 비트코인이 있는 사람은 포크 코인을 자동으로 받음

4.1.3 알트체인

- 블록체인 네트워크를 구축해 암호화폐 발행과 거래 증명 등의 기능을 제공하는 플랫폼

Nxt

- 독자적인 암호화폐 발행, 메시지 전송, 투표, 오픈마켓 등의 기능을 제공하는 플랫폼
- Nxt 오픈마켓은 온라인 디지털 콘텐츠를 안전하게 판매하는 기능, 상품 도착 확인 못하면 자동적으로 환불
- 특징: 블록 생성에 작업 증명 대신 지분 증명 알고리즘 적용 => 암호화폐 잔액에 따라 채굴로 블록 생성할 확률를 동적으로 설정하여 많은 연산 필요 없고, 채굴 보상 독점 막음
- 아이젠트러스트 알고리즘: 어뷰징으로 XEM을 주고 받았을 때 중요도가 높아지지 않도록. 부정행위 노드 중요도 낮춤

웨이브

- 기존 온라인 금융 거래 플랫폼과 대등한 블록체인 기반 암호화폐 플랫폼 프로젝트
- 온라인 뱅킹과 비슷한 UX => 누구나 자유롭게 암호화폐 발행
- 기존 화폐 구조에 암호화폐 거래를 이용할 수 있는 플랫폼을 제공해 시장 가치를 키우는 전략
- 원, 달러 등의 법정 통화나 BTC, ETH등의 암호화폐를 송금하면 1:1로 대응하는 WAVES 암호화폐를 발행하는 기능
- 포인트 카드 발행, 다른 블록체인 플랫폼으로 암호화폐를 발행하는 서비스가 웨이브 플래솜 도입 할 것

4.2 스마트 계약 플랫폼

- 이더리움: 다양한 디지털 자산의 소유권을 블록체인에 저장한 후 스마트 계약으로 자산을 관리하거나 이동시킬 수 있는 오픈 플랫폼
- [그림 4-9] 스마트 계약 플랫폼과 개발 도구 분류

4.2.1 이더리움과 스마트 계약 플랫폼

이더리움 클래식

- 이더리움의 원형. 코인: ETC
- DAO 크래킹 사건: 2016년 6월. 이더리움의 탈중앙화 네트워크 계약 취약점을 공격해 약 360만 이더 (약 640억) 도난 => 하드포크
- 이더리움과 많은 기능 호환. 독자적 변화
- 이더리움 - 작업 증명에서 지분 증명 알고리즘으로 변경 고려, 클래식 - 작업 증명 유지
- 이더리움 - 암호화폐 발행 제한 없음, 클래식 - 채굴 보상으로 받는 암호화폐의 양을 500만 블록마다 20%씩 단계적으로 감소, 최대 발행량 2억 3천만 ETC로 제한

유비큐

4.2.2 비트코인에서 실행하는 이더리움 호환 스마트 계약 플랫폼

카운터파티

- 비트코인 확장 프로젝트
- 다양한 암호화폐 프로젝트의 기능을 적극적으로 도입
- 이더리움과 호환하는 스마트 계약 실행 가능 => 스마트 계약 플랫폼으로 활용
- 소각 증명 (Proof of Burn): 비밀 키가 발견되지 않은 비트코인의 주소에 BTC를 보낸 후 비활성 (Burn) 시키면 새로운 XCP 발행

루트스톡

- 비트코인을 사이드 체인에서 거래할 수 있게 만드는 호환 플랫폼
- 토큰을 양방향으로 교환 기능 (2 Way Peg)
- 사이드 체인: 메인으로 생각하는 암호화폐를 교환해 거래할 수 있는 다른 블록체인, 다시 메인 체인 암호화폐로 교환 가능

4.2.3 기타 스마트 계약 플랫폼

- 네오: 중국 중심. 다양한 프로그래밍 언어에 대응하는 가상 머신 NeoVM으로 블록체인 이외의 환경에서 스마트 계약을 실행
- 리스크: 사이드 체인을 이용하는 분산 스마트 계약 플랫폼. 자바스크립트로 개발 가능.
- 이오스: 블록체인 노드의 투표로 선정한 대표 노드에게 블록 생성 및 거래 확정 권한을 위임하는 '위임 지분 증명 (Delegated Proof Of Stake)' 합의 알고리즘. 처리 속도 빠름. 대표 토드를 블록 프로듀서라고 함.
- 보스코인: 한국에서 생성. 스마트 계약 구현에 온놀로지 웹 언어, 타임드 오토마타 언어 기반의 트러스트 컨트랙트 사용. 스마트 계약 배포 전에 안정성과 실행 결과를 수학적으로 증명

4.2.4 스마트 계약 도구

- 리믹스: 브라우저에서 솔리디티(Solidity) 프로그래밍 언어로 스마트 계약 개발과 구축을 지원하는 통합 개발 환경. 브라우저로 사설망이나 테스크넷의 이더리움 블록체인에 연결해 스마트 계약 배포와 테스트 가능
- 제플린: 블록체인 플랫폼 안에 스마트 계약 구현하는 오픈 소스 프로젝트. 솔리디티 기반 - 프레임워크 오픈제플린, 스마트 계약 관리하고 운영하는 플랫폼 - 제플린
- 이더파티와 블록캣: 웹 UI 기반으로 쉽게 스마트 계약 구현. 사용자가 템플릿에 내용을 채우는 방식으로 스마트 계약을 구현하며, 테스트넷 검증과 블록체인 배포까지 처리하는 것이 목표

4.3 기업용 블록체인 플랫폼

비즈니스에 활용할

[그림 4-10] 프라이빗 환경이나 PaaS 클라우드에서 활용하는 블록체인 플랫폼

4.3.1 프라이빗 블록체인

- 불특정 다수의 사용자로 구성된 P2P 네트워크에서 하나의 원장(Ledger)을 운영하는 기술
- 여러 회사를 연결하는 P2P 네트워크나 한 회사 안의 P2P 네트워크에 적용
- Distributed Ledger Technology (DLT)
- 미리 허가받은 노드만 참여한다고 가정하면 전체 시스템 규모 파악하기 쉽고, 시스템 규모에 맞게 성능을 높일 수 있음

4.3.2 하이퍼레저 프로젝트

- 2015년 12월 리눅스 재단에서 시작한 비지니스용 블록체인 오픈 소스 프로젝트
- 하이퍼레저 패브릭: IBM 주도. 주 기능: 사용자 식별, 시스템 체인코드 서비스. 예) 에버레저: 다이아몬드나 고급 자동차 등의 고액 자산 내역 관리. 분산 노드-제한된 사용자 대상 효율성 높일 수 있는 합의 알고리즘 사용
- 하이퍼레저 소투스: 인텔 주도. 경과 시간 증명을 합의 알고리즘 처리 효율을 향상. SGX-별도의 샌드박스를 만들어 합의 알고리즘을 처리하여 보안성과 처리 효율을 높임.
- 하이퍼레저 이로하: 일본 소라미츠사 주도. 스메라기라는 BFT 기반 합의 알고리즘 => 성능 향상과 빠른 거리 확정 시간에 중점.
- 하이퍼레저 버로우: 영국 모낙스 주도. 최초의 이더리움 기반. 합의 알고리즘: 텐더민

4.3.3 코다

- 글로벌 분산 원장 컨소시엄 R3가 개발하는 금융 분산 원장 플랫폼
- 탈중앙화가 아닌 중앙 집중형 플랫폼
- 블록체인과 다른 점: 블록이나 채굴 등의 개념이 없음, 거래 당사자 사이의 서명으로 거래를 확정한 후 코다를 관리하는 주체가 이중 지급 등이 있는지 확인하는 합의 방식, 별도의 타임스탬프 서버를 구축해 실제 거래 시각과 동기화해야 함.
- 비슷한 점: 비트코인의 블록과 UTXO 개념으로 거래 환경을 제공한다는 점

4.3.4 미진

- 일본의 테크뷰로사가 개발하는 NEM 기반의 블록체인 스마트 계약 플랫폼
- 퍼블릭 블록체인 기반의 NEM과 프라이빗 블록체인을 통합하는 에코 시스템 구축 추진중
- 2018년 3월 베타버전, 5월 오픈소스 공개 예정

4.3.5 블록체인 플랫폼을 위한 클라우드 서비스

- MS Azure: 이더리움과 하이퍼레저 패브릭 기반의 블록체인 플랫폼을 구축하거나 운영하는 Blockchain as a Service (PaaS기반) 제공. 이더리움 스튜디오라는 스마트 계약 통합 개발 환경으로 스마트 계약 개발을 지원
- AWS: 하이퍼레저 패브릭 기반의 블록체인 플랫폼을 구축, 운영하는 템플릿 제공
- IBM 블루믹스: 하이퍼레저 패브릭을 클라우드에 구축하는 플랫폼인 Blockchain on Bluemix를 제공

참고

블록체인 기술의 의료분야 활용

http://hanhyunwook.com/221287082663

http://hanhyunwook.com/221287087193