전사원 필수! 디지털 융합 시대와 블록체인 기술 _ 요약집

- 블록체인이 가지고 있는 기술적 특징
  1. 탈중앙화
  2. 데이터의 보안
  3. 상호 신뢰성
- 컨소시엄 블록체인에 대한 설명
  1. 컨소시엄 블록체인은 동일한 목적을 가진 다수의 기업 또는 조직이 하나의 컨소시엄을 구성해 블록체인 네트워크를 관리하는 것이다.
  2. 컨소시엄 블록체인은 퍼블릭과 프라이빗 블록체인의 요소를 결합한 형태이다.
  3. 컨소시엄 블록체인은 퍼블릭 블록체인보다 트랜잭션을 빠른 속도로 처리할 수 있다.
- 탭루트(Taproot)에 대한 설명
  1. 탭루트는 2016 년에 제안된 '마스트(MAST: Merkelized Abstract Syntax Tree)'를 개량한 것이다.
  2. 스마트 계약을 실행할 때 모든 조건을 확인할 필요가 없으므로 실행 속도도 개선되는 효과가 있다.
  3. 이번 탭루트 업데이트는 32 바이트에 달하는 추가 해시값을 블록체인이나 스마트 계약에서 제외함으로써 효율성이 더욱 향상되었다.
- 합의 알고리즘에 대한 설명
  1. 이오스는 DPoS(Delegated PoS)와 PBFT 를 기반으로 하는 합의 알고리즘을 사용한다.
  2. DPoS 방식으로 플랫폼 전체를 대표하는 21 명의 블록 생성자를 선출하고, 이들 간에는 PBFT 방식의 투표를 통해 0.5 초마다 블록을 하나씩 생성한다.
  3. 소수의 블록 생성자에게 주어지는 권한이 크기 때문에 21 명의 블록 생성자 중의 일부가 담합하여 블록체인을 공격하여 심각한 문제를 초래할 가능성도 있다.
- 이더리움에 대한 설명
  1. 이더리움은 2013 년에 비탈릭 부테린(Vitalik Buterin)에 의해 제안되었다.
  2. 2015 년 중순에 처음으로 공개된 이후 많은 찬사를 받으며 단기간에 두 번째로 규모가 큰 가상화폐로 자리매김을 했다.
  3. 이더리움도 비트코인의 지갑과 동일한 개념인 account 가 존재한다.
- 지분증명(PoS: Proof of Stake)에 대한 설명
  1. 지분을 가지고 있는 만큼 보상받는 방식이다.
  2. 지분이 많을수록 보상이 커지는 방식이므로 화폐로서 유통되는 것보다는 저축용으로 사용될 가능성이 있다.
  3. 일정량은 채굴하고 그 이후에는 가지고 있는 암호화폐의 수량에 따라 더 많은 보상이 지급된다.
- 컨소시엄 블록체인에 대한 설명
  1. 반중앙형 블록체인으로 컨소시엄에 포함된 소수의 주체들만이 참여가 가능하다.
  2. 주체들 간의 합의된 규칙을 통해 공증에 참여할 수 있다.

3. 사전에 합의된 규칙에 따라 거래 검증과 블록 생성이 이루어진다.

- 버추얼박스(VirtualBox)에 대한 설명
  1. 버추얼박스는 x86 과 AMD64/Intel64 하드웨어 시스템을 가상화할 수 있는 프로그램이다.
  2. 현재 윈도, 리눅스, OSX 와 솔라리스 등의 많은 환경(호스트)에서 설치가 가능하다.
  3. 게스트 환경으로는 윈도 제품군을 포함한 도스, 리눅스, 솔라리스 등의 대부분의 운영 체제를 설치할 수 있다.
- 지갑(Wallet)에 대한 설명
  1. 지갑은 본인 지갑의 개인키, 공개키 및 자산을 관리하는 프로그램으로 구성된다.
  2. 지갑의 개인키는 계좌 비밀번호와 유사하고, 공개키는 계좌번호와 유사하다고 생각하면 된다.
  3. 지갑의 종류에는 USB, 하드디스크와 같은 물리적인 장치로 작동하는 콜드월렛과, 온라인으로 연결되어 바로 입출금 및 송금이 가능한 핫월렛이 있다.
- 합의 알고리즘의 표준과 기술과 그에 대한 설명
  1. 균형 작업증명(ePoW: equilibrium Proof of Work) : 이미 사용 중인 네트워크에 들어오는 다른 참여자에게도 기회를 주어 불필요한 에너지의 낭비를 제거하는, 해당 문제점을 극복한 합의 알고리즘이다.
  2. 이중 위임 지분증명(DDPoS: Dual Delegated Proof of Stake) : 기존의 DPOS 에 비해 다양한 보안성 및 가용성을 가지고 개인정보 보호를 위해 검증 단계 및 지분 위임을 이중으로 극복한 알고리즘이다.
  3. 하이퍼 위임 지분증명(Hyper-DPoS) 기존의 위임 지분증명(DPoS) 방식을 기반으로 만든다.

- ◆ 블록체인 기술의 잠재적 편익에 따른 장애 요인에 대한 설명
  1. 거래 속도의 증가
  2. 정확성의 증가와 인적 오류의 감소
  3. 거래의 투명성과 감시 가능성의 증가
- ◆ 해시함수의 특성에 대한 설명
  1. 계산 시간에 대한 합리적인 추정이 가능해야 한다.
  2. 결과값이 중복될 가능성이 거의 없다.
  3. 입력값을 알 수 없다.
- ◆ 트랜잭션의 용량 제한에 의한 문제 해결과 확장성 확보를 위해 이더리움이 도입하고 있는 방법에 대한 설명
  1. 샤딩(Sharding) : 전체 네트워크를 분할한 뒤에 트랜잭션을 영역별로 저장하고, 이를 병렬적으로 처리하여 블록체인에 확장성을 부여하는 기술
  2. 프라즈마(Plasma) : 별도의 체인을 만들고 최소한의 데이터만을 이더리움의 메인 블록체인과 동기화하는 방법

3. 트루빗(TrueBit) : 블록체인의 연산 증가에 초점을 둔 이더리움 스마트 계약의 확장성 솔루션

◆ 샤딩(Sharding)에 대한 설명
1. 샤딩은 블록체인 내 블록 생성 생성자를 소그룹으로 분할하여 소그룹에서 개별로 블록을 생성하게 한다.
2. 이후 이더리움 2.0 에 롤업과 샤딩을 도입해 트랜잭션의 속도를 향상할 계획이다.
3. 이더리움 2.0 은 샤딩을 접목하여 2022 년 4 분기에 출시될 계획이다.

◆ 비트코인 기반 블록체인의 특성에 대한 설명
1. 블록체인은 블록으로 연결되어 있다.
2. 블록은 주기적으로 생성되며 블록체인에 추가된다.
3. 블록은 시간, 난수, 전 블록의 해시, 여러 거래 내역 등을 포함한다.

◆ 작업증명(PoW: Proof of Work) : 스팸 전자 메일을 보내거나 서비스 거부(DoS: Denial of service) 공격을 하는 등의 컴퓨팅 능력의 사소하거나 악의적인 사용을 막기 위해 실현 가능한 노력을 요청하는 시스템

◆ 프라이빗 블록체인에 대한 설명
1. 개인형 블록체인으로 하나의 주체에 의해 내부 전산망이 블록체인으로 구현된다.
2. 한 중앙기관이 모든 권한을 보유한다.
3. 허가받은 사용자만 접근할 수 있다.

◆ 블록의 해시에 대한 설명
1. 데이터의 값을 배열의 인덱스인 정수로 변환하기 위해 해시함수가 사용된다.
2. 블록을 구성하는 정보 중에서 블록의 해시는 아주 중요한 역할을 한다.
3. 계산된 해시값을 이용해 데이터가 변경되었을 때 이를 감지할 수 있다.

◆ 채굴 : 블록 해시를 찾기 위해 지속적으로 계산하는 행위

◆ PoS(작업증명합의) 기술 수행 과정에 대한 설명
1. 합의에 대한 권한을 가져가려면 참여자는 지분을 보유하고 있어야 한다는 철학이 존재한다.
2. 생성된 합의 알고리즘은 향후 지분을 투자한 만큼 합의에 대한 권한을 많이 생성해 주는 비례 관계를 그려서 적용한다.
3. 지분증명이라는 철학은 매우 합리적인 방법이며, 많은 시범 프로젝트에 적용해서 표준화를 연구하는 단계라고 할 수 있다.

◆ 블록체인 지갑의 유형과 그에 대한 설명
1. 하드웨어 지갑 : 개인키와 공용 주소를 저장하고 관리하며 트랜잭션에 서명하는 데 사용되는 하드웨어 장치이다.
2. 종이 지갑 : 암호화 소유자는 개인키를 안전하게 유지해야 한다.
3. 데스크탑 지갑 : 데스크탑 지갑은 주요 PC 에 설치되어 사용되는 소프트웨어 유형이다.

◆ 소프트웨어가 블록체인에서 실행되는 동안에 개인 블록체인 지갑의 지갑 주소는 무작위로 생성된 (32)개의 영문자와 숫자의 조합으로 정의된다.

◆ 블록체인 구성 요소의 특징

1. 상태 전이를 나타내는 트랜잭션 형식의 메시지
2. 트랜잭션의 구성 요건과 트랜잭션의 유효성을 판단하는 합의 규칙의 집합
3. 공개된 환경에서 상태 머신에 경제적인 보안성을 제공할 수 있는 게임 이론적으로 유효한 인센티브 메커니즘

◆ 하이퍼레저 도구와 그에 대한 설명

1. 하이퍼레저 첼로(Hyperledger Cello) : 블록체인 생태계에 수요 기반의 서비스 배포 모델을 제공하여 블록체인의 수명 주기를 관리하는 데 필요한 노력을 줄여준다.
2. 하이퍼레저 퀼트(Hyperledger Quilt) : 기본적인 결제 프로토콜입니다. 분산 원장 및 비분산 원장에서 가치를 이전하도록 설계된 ILP(Interledger Protocol)를 구현하여 원장 시스템 간의 상호 운용성을 제공한다.
3. 하이퍼레저 컴포저(Hyperledger Composer) : 하이퍼레저 컴포저는 블록체인 비즈니스 네트워크를 구축하고 스마트 컨트랙트 개발 및 분산 원장을 통한 배포를 가속화하는 협업 도구 모음이다.

◆ 트러플(Truffle)의 기능에 대한 설명으

1. 스크립팅이 가능하고, 확장 가능한 배포 및 마이그레이션 프레임워크
2. IPFS 에서 관리하는 파일을 업로드하고 검색하는 것을 포함하여 데이터를 저장하며 검색
3. 긴밀한 통합이 지원되는 구성이 가능한 빌드 파이프라인

◆ 메타마스크(Metamask) : 이더리움 지갑의 종류 중 브라우저에서 실행되는 브라우저 확장 지갑

◆ 중앙은행 디지털 화폐(CBDC)에 대한 설명

1. CBDC(Central Bank Digital Currency)는 전자적 형태로 발행되는 중앙은행 화폐를 말한다.
2. 앙은행 디지털 화폐에 대한 논의는 과거에도 논의된 바는 있으나 최근 분산원장 기술의 발전과 가상자산의 확산 등의 계기로 논의가 활발히 진행되고 있다.
3. 인구가 적고 현금 이용의 감소에 따른 부작용이 발생될 우려가 있거나 금융 포용의 수준이 낮은 일부 특수한 환경에 처한 국가들이 CBDC 의 발행을 보다 적극적으로 검토하고 있다.

◆ 거액 결제용 CBDC 에 대한 설명

1. 금융기관 간의 결제에 분산원장 기술을 적용하여 1 년 365 일 24 시간 내내 끊어짐 없이 결제가 가능하다.
2. 단일 장애점 문제를 해소하여 사이버 공격 등의 해킹으로 인한 피해를 줄일 수 있다.
3. 결제 및 청산 과정에서 운영위험도가 감소하는 등 결제 시스템의 개선을 도모하는 것을 목표로한다.

◆ 디파이(DeFi)의 시장 동향에 대한 설명

1. 디파이는 블록체인 기술의 스마트 계약을 기반으로 중앙기관 및 중개기관 없이 P2P 형태로 금융 시스템을 구축한다는 데 그 목적이 있다.
2. 실제로 디파이의 생활 수요는 많지 않다.
3. 디파이의 상용화를 위해 인프라를 구축하기도 쉽지 않다.

- 디파이 시장에서 투자자들이 가장 주목하고 있는 것은 (이자농사(Yield Farming))이다. (이자농사(Yield Farming))는 디파이 프로토콜에 유동성을 제공하고 그 대가로 이자를 취득하는 개념입니다.
- 국가별 블록체인의 적용 예
  1. 중국은 블록체인 핵심 기술을 선점하고 블록체인의 생태계 안에서 블록체인을 적극적으로 육성하고 있다.
  2. 미국 정부는 블록체인을 산업 전반에 적용하기 위해 다양한 법률 제정을 추진하며, 다수의 부처가 적극적으로 시범사업과 연구를 추진하고 있다.
  3. 미국은 주정부 및 지방정부는 지방 경제의 활성화, 투표, 의료 서비스, 공공서비스의 향상을 위해 블록체인 기술을 도입하여 산업 경쟁력을 강화하고 있다.
- 블록체인이 적용된 산업 분야
  1. 이토니온(ITTONION) 플랫폼
  2. 블루웨일
  3. 벨릭(VELIC)
- 스마트 시티의 인프라 관리에 대한 설명
  1. 스마트 시티는 통신망을 비롯한 기반 시설이다.
  2. 수집된 데이터를 바탕으로 도시의 여러 문제를 해결하기 위한 서비스가 제공된다.
  3. 인프라를 통해 각종 도시의 정보가 수집된다.
- 스마트 시티의 공간 정보 분야에 블록체인이 적용된 사례에는 위치 정보의 인증과 관련된 공개규약인 (FOAM)이 있다.
- 인터체인 기술에 대한 설명
  1. 서로 다른 블록체인 네트워크 사이에 트랜잭션을 교환할 수 있는 기술이 필요하다.
  2. 지금까지 알려진 인터체인 기술에는 크게 양방향 페깅, 아토믹 스왑, 릴레이어의 세 가지 기술이 있다.
  3. 양방향 페깅은 한쪽 체인에서 토큰을 동결하면, 다른 체인에서 그것을 확인해 동일한 가치를 가지는 토큰을 발행하는 방법이다.
- 영지식 증명(Zero-Knowledge Proof) : 블록체인의 보안 기술 중 거래 상대방에게 어떠한 정보도 제공하지 않은 채 자신이 해당 정보를 가지고 있다는 사실을 증명하는 기술
- DID 에 해당하는 핵심 기술에 대한 설명
  1. DIDs : DID 를 블록체인에 저장하고 이용하기 위한 블록체인의 적용 기술
  2. DKMS : 분산신원증명에 필요한 인증키에 대한 구조와 생명 주기를 관리하는 개인키 관리 기술
  3. Verifiable Credentials: 모바일 디지털 신분증(Verifiable Credential)을 발급하고 증명하는 기술
- 공동주택에서 비대면 커뮤니티 서비스를 위한 DID 는 (발급) 주체, 소유 주체, 비대면 커뮤니티 서비스로 구성 된다.
- 2017 년 크리스토퍼 앨런이 이야기한 자기주권신원의 10 가지 요소
  1. 실존성

2. 지속성

3. 호환성

◆ 미국은 (HIPAA)를 통해 의료 데이터의 사본에 대한 개인의 권리를 인정하고, 개인이 의료 데이터를 다양하게 활용하도록 권장하고 있다.