서론

1. 동기 및 목표

가. 블록체인

2017년 가상화폐(비트코인)가 이슈가 된 이후, 블록체인에 대한 사람들의 관심이 급증했다가 폭락하는 상황이 발생하였다. 그럼에도 불구하고, 2017년에 이어서 2019년인 지금까지도 블록체인 즉, 분산 장부 시스템은 주목 받는 신기술의 대목에 올라가 있다. 이처럼 블록체인이 계속 주목 받는 이유가 궁금해졌고, 기술에 대해 더 자세히 공부해보고 싶어졌다.

나. 주제 선정

아직 블록체인 기술은 일반인들이 사용하기에는 어려운 부분들이 많이 있는데, 이번 프로젝트에서는 블록체인의 장점을 최대한 살리면서도, 기업적 측면보단 일반인들이 어떻게 하면 블록체인 기술을 관심 있게 접해 볼 수 있을까에 초점을 맞추었다.

그래서 생각하게 된 것이 학생들이나 지식 습득을 필요로 하는 사람들이 지식을 공유할 수 있는 웹사이트이다. 다른 지식공유 커뮤니티와 다르게 서로 지식습득을 위해 소액을 지불하는 형식으로, 블록체인 가상화폐 사용을 유발하여 블록체인 기술에 대한 관심을 높이려고 한다.

2. 작품 설명

One day Mentor Dapp, 즉 소액을 지불하고 하루 동안 필요한 멘토를 구하는 블록체인 활용 웹사이트이다. 간략히 설명하자면, 누구나 멘토와 멘티가 될 수 있는 기회를 가질 수 있고, 24시간이라는 한정된 시간 동안 댓글창이 활성화 되어 둘 사이의 연결이 가능해진다. 또한 멘토와 멘티의 연결 가운데 멘티의 이더(블록체인 화폐) 소액 지불이 필요하고, 이러한 거래기록을 블록체인 장부 사용함으로써 거래에 대한 신뢰성을 높였다. 더 자세한 설명은 아래에서 계속 하겠다.

본론 1 (일반적 작동원리 – 블록체인)

1. 블록체인
2. 블록체인 개념

‘블록체인’이란 데이터 분산 처리 기술이다. 이는 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산 저장하는 기술을 지칭하는 말이다. 블록에 담긴 장부와 시간 순으로 밀봉 후 체인으로 연결된 블록이기 때문에 블록체인이라는 이름이 붙었다. 검증된 공공 장부를 만들어 개인에게 분산, 공유하며 관리하는 시스템이라고 할 수 있다.

1. 블록체인 구조
2. 블록체인
3. 블록해시

블록의 헤더 정보를 모두 더하여 합을 구한 후 SHA256(미국 표준 기술 연구소에 의해 공표된 표준 해시 알고리즘 중 가장 많이 채택되어 사용되는 알고리즘)으로 변환한 결과 값이다. 쉽게 블록의 이름 정보라고 생각 할 수 있다.

1. 헤더
2. 버전(version)

해당 블록의 버전이다. 블록 헤더를 만든 프로그램의 버전정보를 의미한다.

1. 이전 블록 해시(previous block hash)

이전 블록의 주소 값을 가리키는 요소다. 이 때문에 각 블록이 서로 연결되어 있는 구조가 된다.

1. 머클루트(merkle root)

바디 부분에 저장된 트랜잭션들의 해시 트리다. 블록이 유효한지 무결성을 검증하기 위한 요소다.

1. 타임(time)

블록의 대략적인 생성 시간을 의미한다.

1. bits

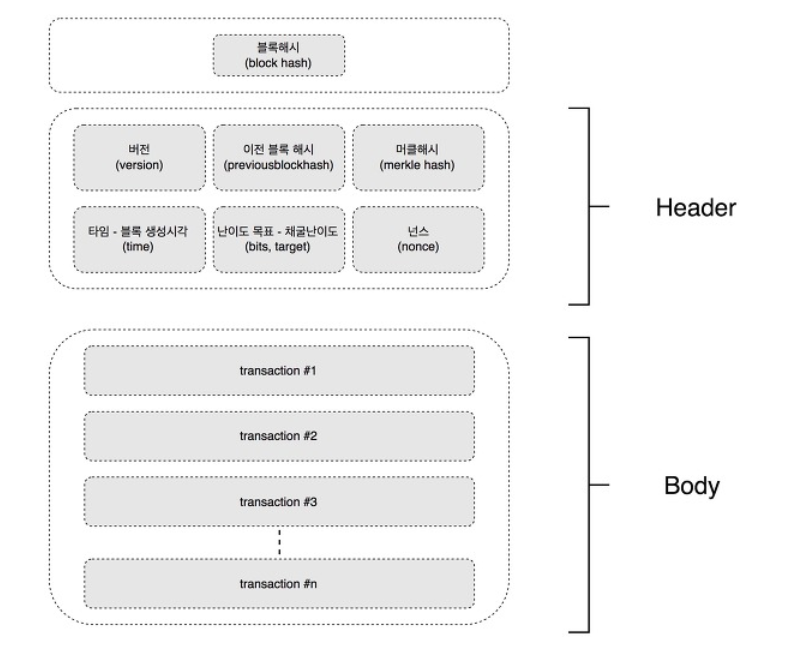
난이도 해시 목표 값을 의미하는 지표다.

1. 논스

블록을 만드는 과정에서 해시 값을 구할 때 필요한 재료 역할이다.

1. 바디

여러 트랜잭션으로 이루어져 있다.



1. 노드
2. 노드란

블록체인은 중앙 서버에 거래 기록을 보관하지 않고 거래에 참여하는 개개인의 서버들이 모여 네트워크를 유지 및 관리하는데 이 개개인의 서버 즉 참여자를 노드라고 한다. 이는 노드에 블록체인이 저장된다는 것을 의미한다.

1. 풀 노드

모든 블록체인 원장을 가진 노드이며 블록체인 데이터를 동기화 하기 위해서 메모리를 사용해야 한다. 모든 거래를 독립적으로 검증하고 실시간으로 데이터를 업데이트 할 수 있다. 제네시스 블록(어떤 블록체인 네트워크에서 생성된 첫 번째 블록)부터 시작해서 현재 블록까지 모든 블록체인 정보를 수집, 저장한다. 자신의 머신에 모든 블록체인의 내용을 가지고 있기 때문에 다른 노드의 도움없이 스스로 거래 검증이 가능하다. 하지만 용량이 너무 크다는 단점이 있다.

1. 라이트 노드

풀노드의 단점을 해결하기 위해 나온 노드다. 모든 블록 정보의 원본을 가지고 있지 않고 블록 헤더에 있는 중요한 데이터만 보유하고 있다. 그렇기 때문에 어떤 거래 정보를 수신 받았을 경우 이 거래가 정상적인지 검증할 수 없다.

1. 블록체인 특징 및 장단점
2. 탈중앙성

블록체인 시스템은 제 3자가 없고 자율적으로 참여자들에 의해서 운영되므로 탈중앙성격을 가진다. 제 3자 없이 네트워크 환경에서 거래가 가능하고 거래의 각 당사자간에 데이터를 분산해서 저장하는 구조다. 따라서 일부 사용자나 시스템에 대한 오류가 성능저하 등 과는 무관하게 전체 네트워크에서 영향을 주는 범위가 미미하다.

1. 안정성

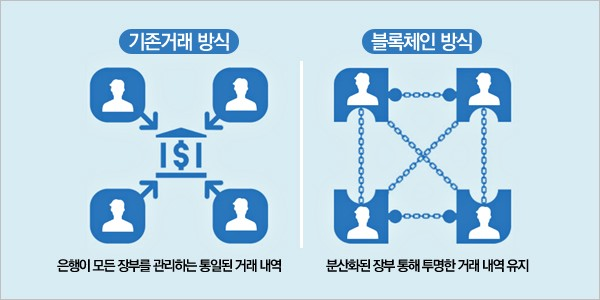
해킹 방법 중 ‘디도스(다수의 일반 pc를 이용해 특정 시스템으로 대량의 유해 트래픽을 전송함으로써 시스템 상에 과부하를 발생시켜 해당 시스템의 정상적인 서비스를 방해하는 해킹방법)’ 공격을 하게 되면 블록체인 시스템은 서버-클라이언트의 구조가 아니기에 특정 노드들을 멈추게 한다 하여도 전체 블록체인 시스템을 마비시킬 수 없다. 또 다른 해킹방법인 ‘랜섬웨어(컴퓨터 시스템을 감염시켜 접근을 제한하고 몸값을 요구하는 악성 소프트웨어의 한 종류)’를 사용하게 된다면 기존에는 서버-클라이언트 구조에서 서버를 감염시켜 클라이언트의 접속을 제한할 수 있었다. 하지만 블록체인 시스템에서는 특정 노드들을 감염시킨다 하더라도 동시에 마비시킬 수 없다면 문제없다.

1. 신뢰성

블록체인에 기록된 내용은 해시함수를 통해서 변환되어 암호화된 상태로 저장된다. 단 한글자만 바꾸더라도 모든 해시 값이 변경되므로 특정 데이터를 변조하는 방식으로는 해킹이 불가능하므로 신뢰성이 확보된다.

1. 기존 거래와의 차이점

기존 거래 방식은 은행이 모든 거래 내역을 가지고 있다. 두 사람이 안전하게 거래할 수 있도록 은행이 중간자 역할을 해준다. 블록체인도 거래 내역을 저장하고 증명한다. 전과 다른 점은 거래 내역을 은행이 아닌 여러 명이 나눠서 저장한다는 점이다. 만약 한 네트워크에 4명이 참여하고 있다면 A와 B의 거래 내역을 4개의 블록으로 생성해 모두에게 전송, 저장한다. 나중에 거래 내역을 확인할 때는 블록으로 나눠 저장한 데이터들을 연결해서 확인한다. 만약 변조된 거래가 일어난다면, 모든 공공장부들을 비교 검증을 하고 과반수 이상이 일치해야 거래가 인정된다. 이 때 필요한 것은 블록체인에 연결된 참여자들의 장부가 사용되기 때문에 중앙 서버가 필요 없다.

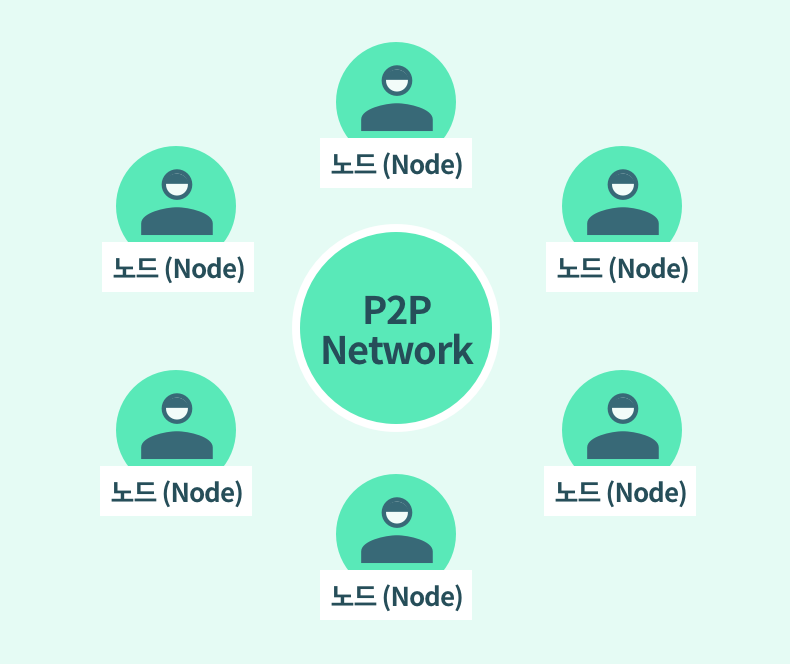


1. 장점
2. 개인 정보를 요구하지 않는다. 기존 지급 수단에 비해 높은 익명성을 제공한다.
3. 은행 없이 P2P 방식으로 거래하기 때문에 불필요한 수수료를 절감할 수 있다.
4. 공개된 소스에 의해 쉽게 구축, 연결, 확장이 가능하다. IT 구축 비용 절감 가능하다.
5. 거래 내역이 공개되어 있어 원칙적으로 모든 거래에 공개적 접근이 가능하다.
6. 장부를 공동 소유하기 때문에 보안관련 비용을 절감할 수 있다.
7. 일부 참가 시스템에 오류 또는 성능저하 발생시 전체 네트워크가 받는 영향이 미미하다.
8. 단점
9. 51% 공격

블록체인의 전체 노드 중 50%를 초과하는 해시 연산력을 확보한 뒤, 거래 정보를 조작함으로써 이익을 얻으려는 해킹 공격을 말한다. 하지만 실제로는 사실상 불가하다.

1. 결제 및 처리 가능한 거래건수가 실제 거래 규모 대비 미미하다.
2. 문제 발생시 책임소재가 모호하다.
3. 개인키의 해킹, 분실 등의 경우 일반적으로 해결방법이 없다.
4. 실시간, 대용량 처리가 어렵다
5. 블록체인 핵심 기술
6. P2P(Peer-to-Peer)

P2P는 중앙 서버없이 각 단말들이 서로 동등한 입장에서 통신을 하는 네트워크다. 각 단말은 서버이기도 하면서 동시에 클라이언트가 된다. 블록체인은 p2p 형태의 이루어진 탈중앙화 네트워크다.



1. 해시(Hash)

해시함수는 입력 값 상관없이 비슷한 길이의 난수가 결과로 출력이 된다. 출력 값으로 입력 값을 예측할 수 없다. 그 때문에 장부가 많을 때도 변조 사실을 쉽게 알 수 있다. 원본의 장부를 해싱 했을 때 나오는 결과와 변조된 장부의 해싱 결과는 다르게 나오므로 이상하다는 것을 알 수 있다.

1. 채굴(Mining, 마이닝)

퍼블릭 블록체인에서 보상과 사용자에게 참여를 유도시키는 기술이다. 작업증명을 통해 블록에 거래 내역을 정리해주고 그 보상으로 코인과 거래 수수료를 받게 한다.

1. 스마트계약(Smart Contract)

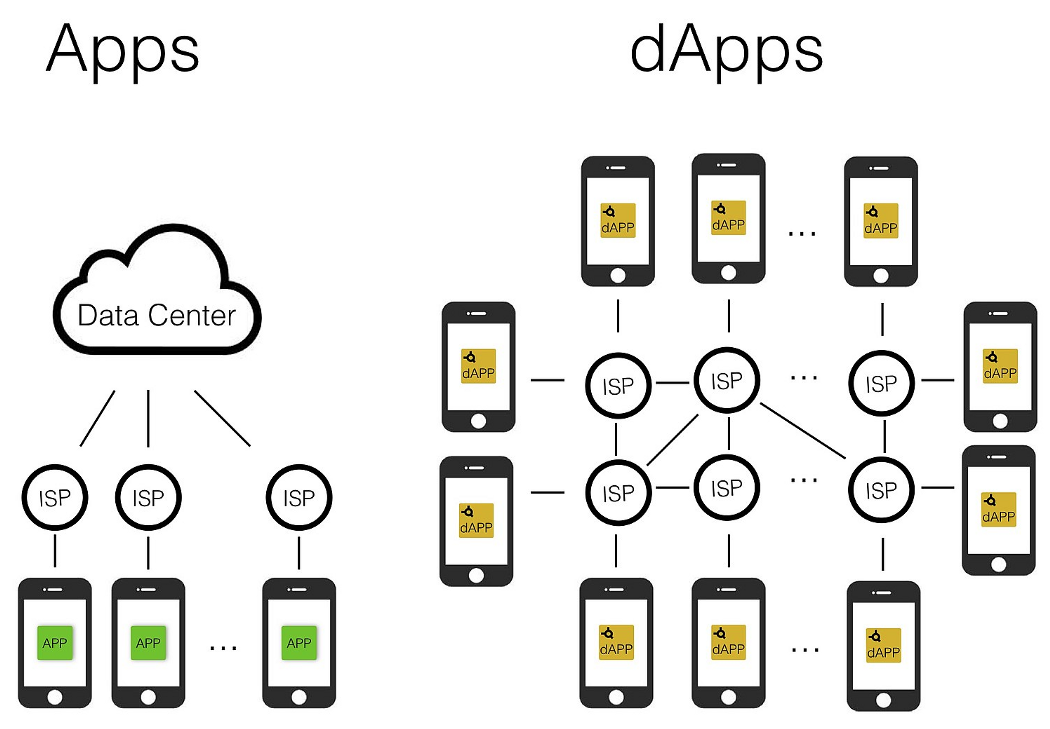
중개자없이 p2p로 쉽고 편리하게 계약을 체결하고 수정할 수 있는 기술이다. 블록체인에서 스마트계약은 계약 이행 및 검증 과정이 자동화되고 신뢰를 바탕으로 안전하게 계약을 실행할 수 있게 한다.

1. 플랫폼 종류
2. 디앱(Dapp)
3. 디앱의 개념

기존의 거래만 가능했던 블록체인 1.0을 벗어나서 블록체인 2.0인 이더리움이 등장하며 다양한 분야로 확장이 가능하게 된다. 이는 스마트 계약을 기반으로 각 서비스의 성격에 맞는 탈중앙화된 어플리케이션, 디앱을 개발할 수 있다. 디앱은 블록체인 기술을 활용하여 중앙 서버 없이 네트워크상에 정보를 분산하여 저장 및 구동하는 앱이다.

1. 앱과 디앱의 차이점

일반 앱은 회원가입을 할 때 개인정보를 입력해서 계정을 만들고 로그인 후 즉시 서비스 이용 가능하다. 하지만 디앱은 계정을 만들 때, 블록체인 지갑을 보유해야 한다. 이는 저장 또는 거래에 사용될 암호화폐를 위한 지갑을 의미한다. 가장 큰 차이점은 디앱은 제품 공개 전 엄격한 테스트 후 공개한다는 점이다. 왜냐하면 스마트 계약이 메인넷(블록체인 프로젝트를 실세 출시하여 운영하는 네트워크)에서 한번 실행되면 절대 변경이 안되기 때문이다.



1. 디앱의 전망

2018년 이래 디앱의 전망이 두드러진다. 현금화가 용이한 디앱의 특성상, 게임 분야가 지속해서 강세를 유지할 예정이다. 지금 대부분의 디앱은 게임 분야에 한정되어 있지만, 점차 다른 분야에서 더욱 발전하고 있다. 이에 디앱의 성공이 블록체인 성공에도 서로 기여할 수 있을 것으로 전망된다. 이미 진행되고 있는 사물 인터넷 등 다른 기술과 연계된 디앱의 성공을 기대해 볼 수 있다.

출처

블록체인

<https://banksalad.com/contents/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EA%B0%9C%EB%85%90-%EC%99%84%EB%B2%BD-%EC%A0%95%EB%A6%AC-dh1do>

<http://wiki.hash.kr/index.php/%EB%85%B8%EB%93%9C#.ED.92.80.EB.85.B8.EB.93.9C>

디앱

<https://medium.com/grabityio/dapp-%EB%94%94%EC%95%B1-%EB%8C%91-%EC%97%90-%EA%B4%80%ED%95%98%EC%97%AC-%EC%95%84%EC%A3%BC-%EA%B0%84%EB%8B%A8%ED%9E%88-%EC%95%8C%EC%95%84%EB%B3%B4%EC%9E%90-f852c6b60a75>

<http://wiki.hash.kr/index.php/%EB%94%94%EC%95%B1#.ED.8A.B9.EC.A7.95>

이미지

<https://towardsdatascience.com/what-is-a-dapp-a455ac5f7def>

<https://medium.com/@elamachain/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-blockchain-%EC%9D%B4%EB%9E%80-69eada649cd4>

<https://banksalad.com/contents/%EC%89%BD%EA%B2%8C-%EC%84%A4%EB%AA%85%ED%95%98%EB%8A%94-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8-%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8%EC%9D%98-%EC%9B%90%EB%A6%AC-%EC%B1%84%EA%B5%B4-%ED%95%B4%EC%8B%9C-%EA%B7%B8%EB%A6%AC%EA%B3%A0-%EC%9E%91%EC%97%85%EC%A6%9D%EB%AA%85-qvCud>

<https://brownbears.tistory.com/371>