블록체인

https://www.banksalad.com/contents/블록체인-개념-완벽-정리-dh1do

개념

블록체인은 데이터 분산 처리 기술 입니다.

네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술입니다.

블록을 체인 형태로 묶었기 때문에 블록체인이라 불립니다.

블록체인에서 블록은 개인과 개인의 거래 P2P 데이터가 기록되는 장부가 됩니다. 이런 블록들은 형성된 후 시간의 흐름에 따라 순차적으로 연결된 사슬, 체인의 구조를 가지게 됩니다.

모든 사용자가 거래내역을 보유하고 있어 거래 내역을 확인할 때 모든 사용자가 보유한 장부를 대조하고 확인합니다.

이 때문에 블록체인은 공공거래장부, 분산 거래 장부라고도 합니다.

사람끼리 거래를 하면 은행이 중간 역할을 수행해서 거래 내역을 저장합니다. 블록체인은 거래 내역을 은행이 아닌 네트워크에 있는 여러 명이 나눠서 저장합니다. 거래 내역을 확인할 때는 블록으로 나눠 저장한 데이터들을 연결해 확인합니다.

특징

블록체인은 분산저장한다는 점이 특징입니다.

기존의 거래 방식을 위, 변조하기 위해서는 은행을 공격했습니다. 하지만 블록체인은 거래내역을 여러 사람이 가지고 있어서 위, 변조하기 위해서는 모든 사람을 공격해야하는데 사실상 불가능에 가깝습니다.

블록체인은 중앙 관리자가 필요 없는 점도 특징입니다.

은행이나 정부 등 중앙관리자가 증명, 등기, 인증을 했지만 블록체인 다수가 데이터를 저장, 증명하기 때문에 중앙관리자가 존재하지 않습니다.

블록체인은 비트코인과 같은 가상화폐를 등장에 기여했습니다.

중앙기관의 역할이 블록체인은 없기 때문에 중앙은행이 없더라도 화페발행이 가능해집니다. 비트코인을 원하는 사람들은 채굴을 통해 발행하고 이는 중앙은행 없이도 화페 발행, 유통이 가능하다는 것을 보여주었씁니다.

활용

https://luniverse.io/2021/01/25/ten-blockchain-usecases/?lang=ko

블록체인은 거래정보를 기록한 원장 데이터를 중앙 서버 없이 모든 참가자가 공통으로 기록하고 관리하는 탈중앙화 기술입니다.

누구나 열람할 수 있는 디지털 장부에 거래 내역을 투명하게 기록하고, 이 기록을 여러 대의 컴퓨터에 복제해 저장하는 분산형 데이터 저장 기술 입니다.

블록체인은 분산처리와 암호화 기술을 동시에 적용해 높은 보안성과 투명성을 특징으로 합니다.

블록체인의 안정성과 투명성은 여러 산업에 다방면으로 사용되고 있습니다.

식품원산지 추적

식품의 원산지와 유통 정보 등을 확인할 수 있는 식품 안전망 시스템이 진화하고 있습니다.

모든 유통과정을 실시간으로 업데이트함으로서 소비자에게 투명하게 공개해 신뢰도를 높였습니다.

보험금 청구

보험금을 청구하려면 여러 서류들을 인증해야 해서 시간이 소모되고 불편함을 겪었습니다.

병원서류를 블록체인에 저장해 필요할 때 꺼내서 쓰는 인증기술의 보급으로 간편하고 빠르게 보험금 청구가 가능해졌습니다.

보험사 입장에서도 문서를 하나하나 검증할 시간을 아낄 수 있고 위, 변조가 불가능하다는 점에서 보험 사기를 예방할 수 있습니다.

이 밖에도 청산결제, 온라인 중고 거래 플랫폼, 무역, 건강여권 등등 여러 분야에서 활용되고 있습니다.

핵심은 안정성과 투명성으로 보증을 통해 서비스의 질을 올립니다.

문제점 & 해결방안

https://www.itworld.co.kr/news/107168

1. 잠재력은 있지만 초기단계라 적절한 모니터링이나 점검을 받지 않고 있다. (미숙한 기술과 미흡한 소프트웨어)

블록체인 기술은 여러 산업 분야에서 신뢰 모델과 비즈니스 프로세스를 혁신적으로 바꾸어 놓을 수 있는 잠재력을 지니고 있다. 그러나 이 기술은 아직까지 초기 단계에 있으며, 블록체인 기술에 사용되는 분산 원장 기술 역시 적절한 모니터링이나 점검을 받지 않고 있다.

미숙한 기술과 미흡한 소프트웨어로 인해 도입 과정에 예기치 못한 문제가 발생할 수 있다. 프로젝트를 갈아엎어야 할 수도 있다. 코딩 상의 문제로 인해 큰 문제가 발생하기도 한다.

2. 비용이 많이 들고 도입 시간이 오래 걸린다.

블록체인 기술이 중앙집권화된 관계형 데이터베이스와 같은 기존의 거래 기술에 비해 더 비싸고 도입 시간도 오래 걸린다

3. 모든 블록의 암호 확인 절차로 인해 효율성을 버리고 자율성을 얻는 시스템이라고 말한다.

새로운 블록이 블록체인에 추가되기 위해서는 모든 블록의 암호 확인 절차가 요구된다. 이 때문에 빠른 거래가 필수인 비즈니스 분야에 적용하기에는 효율적이지 못합니다.

4. 직렬화된 삽입으로 인해 기존의 병렬 삽입에 비해 업데이트 속도가 느리다.

블록체인은 체인형태이기 때문에 블록 삽입이 직렬화되어야 한다. 업데이트 속도가 병렬적인 업데이트를 하는 전통적인 데이터베이스보다 느리다.

5. 데이터 저장에 적합하지 않을 때도 있다.

한 번의 데이터 생성으로 많은 이들에게 공유할 수 있다는 것이 장점이다. → 조작이 불가능하다.

하지만 이미지와 같은 용량이 큰 경유 데이터량이 급증하고 이는 네트워크 오버헤드로 이어지게 된다.

관계형 데이터베이스만으로 충분한 상황에서 굳이 블록체인 기반 아키텍처를 도입할 이유는 없다라는 것이 전문가의 의견이다.

6. 생각만큼 안전하지 않을 수도 있다.

비트코인은 퍼블릭 블록체인과 프라이빗 블록체인 2가지로 나누어진다.

퍼블릭 블록체인은 누구나 가담할수 있고 비트코인이 대표적인 예 입니다.

프라이빗 블록체인은 중앙권위체에서 단독으로 관리하면 가입을 위해서는 승인이 필요합니다.

퍼블릭이건 프라빗이건 기본적으로 조작이 불가능합니다. 블록을 임의로 변경할 수 없고 다른 모든 블록들과 연결되어 있기 때문이다. 블록을 추가하려면 다른 사람의 동의가 필요합니다.

블록체인을 개발하는 회사들은 검증되지 않은 알고리즘을 사용하고 있다. 새로운 암호화 알고리즘이 안전한 것으로 수용되기 위해서는 수년의 시간이 걸리는데 새로 나온 블록체인은 이런 면에서 검증을 받지 못했다. 전문가들은 블록체인은 해킹으로 깨지기 보다 소프트웨어상의 취약점으로 깨질 확률이 높다고 전망한다.

해결책

좋은 사이트 :

https://medium.com/@ace_3704/makers-basic-6-블록체인의-문제점과-대안-c8893f402a15

작업증명 박식의 문제점과 제안

블록체인은 권위적인 중앙체계를 지니지 않기 때문에 사용하는 다수의 참여자들이 공동으로 의사결정을 내리기 위한 **거버넌스 구조**가 필요하다.

거버넌스 구조 : 다수의 참여자들이 공동의 목표를 위해 서로 논의하고 결정하는 체계 (중앙 체계가 없기 때문에)

블록체인 시스템에서 처음으로 도입한 합의 알고리즘은 **작업증명 방식(PoW)**이다. 작업증명이란 목표값 이하의 해시를 찾는 과정을 수없이 반복해서 해당 작업에 참여했음을 증명하는 방식의 알고리즘이다.

이러한 방식이 마치 광산에서 금을 캐기 위한 행동과 비슷하다고 하여 채굴(mining)이라고 부른다. 채굴을 통해 가장 먼저 목표값 이하의 해시값을 얻게 되는 사용자는 해당 블록을 체인에 연결하고 이에 대한 댓가로 신규 코인을 지급받는다.

문제점

이러한 작업증명 방식에 따른 채굴은 막대한 자원과 전기 낭비를 유발한다. 채굴을 통해 코인을 지급받는 사람은 1명이지만 수없이 많은 자원이 경쟁에 참여하기에 낭비가 커진다. 경쟁이 심해지면서 여러 채굴업체들이 **마이닝 풀(mining pool)**을 구성하여 공동 채굴을 함에 따라, 비민주적 의사결정이 우려되고 있다.

채굴기를 운영하는 개인이나 업체들은 공동으로 채굴하고 수익을 배분하는 마이닝 풀을 구성하였다. 마이닝 풀을 통해 네트워크로 연결된 채굴기들은 1대의 슈퍼컴퓨터 성능이 좋게 작동하여 채굴 성공율을 높일 수 있으며 각각의 참여자들은 참여한 자신의 해시 연산력에 비례하여 수익을 배분 받는다.

만약 단순계산으로 상위 마이닝 풀이 담합을 한다면 51% 공격을 통해 기존 거래내역에 대한 위변조도 가능할 수도 있다.

블록체인은 중앙집중적인 기존의 시스템에서 탈피하고자 생긴 기술인데, 이렇게 마이닝 풀을 통하여 소수의 채굴업자들로 하여금 의사결정 권한이 집중되는 현상이 발생할 수 있다.

대안

작업증명 방식에 따른 채굴 경쟁과 그로인한 막대한 전기낭비 및 비민주적 의사결정을 막기 위해 다양한 대안적 합의 알고리즘이 등장하였다.

지분증명(PoS)은 해당 암호화폐를 보유하고 있는 지분율에 비례하여 의사결정 권한을 주는 방식이다.

주주총회에서 지분율에 따라서 권한이 다른 것과 같다. 지분증명방식은 막대한 전기를 소모하는 채굴과정이 필요 없다. 다만 이 방식은 그라인딩 공격에 취약하다는 문제를 가진다.이것은 마지막 블록 생성자가 다음 번 블록 생성에 사용되는 랜덤 변수를 미리 계산해서 본인에게 유리한 결과를 만들 수 있다는 것이다.

에이다는 **우로보로스 지분증명(Ouroborous PoS)**이라는 개선된 알고리즘을 사용함으로써 이 문제를 해결했다. 하지만 이러한 방식의 암호화폐는 많이 소유한 사람에게 의사결정 권한이 크기 때문에 자본에 의한 의사결정구조를 왜곡한다는 점, 암호화폐를 거래에 사용하기보다는 보유만 하는 것이 더 유리하기 때문에 암호화폐 활성화에 악영향을 미칠 수 있다는 점 때문에 비판을 피할수 없다.

이러한 지분증명에 대한 비판으로 **위임지분증명(DPoS)방식**이 등장했다. 암호화폐 소유자들이 각자의 지분율에 비례하여 투표권을 행사하여 자신의 대표자를 선정해서 이 대표자가 합의를 도출해내서 의사결정을 하는 방식이다. 의원을 뽑아서 의회를 구성하는 식의 민주주의 제도와 유사하다. 이오스, 스팀, 보스코인 등이 이 방식을 하고 있다. 그러나 이 방식 또한 직접 민주주의가 아닌 선출된 소수 대표자들에 의해 독과점으로 변질될 우려를 가지고 있기에 이상적인 블록체인의 모습과는 다르다.

작업증명과 지분증명의 장점을 혼합한 하이브리드형 알고리즘인 활동증명(PoA)방식이 등장하기도 했다. 소각증명 방식, 중요도증명(PoI), 신뢰성증명(PoB) 등 다양한 합리적 알고리즘이 등장했다.

기존의 작업증명 방식은 탈중앙화라는 블록체인의 이념을 깨는 세력이 생길 수 있다.

댜앙하고 합리적인 알고리즘이 등장

체인 알고리즘의 문제점과 대안

체인(chain)이란 이전 블록의 해시가 다음 블록과 한 구성요소가 되어 연결되는 것을 말한다. 체인 알고리즘은 다수의 거래기록을 해시화하여 체인처럼 연결, 탈중앙 방식을 통해서 데이터 위변조를 방지하는 블록체인의 가장 대표적인 알고리즘이다.

다만 트랜잭션 처리 속도가 느리고 블록의 사이즈가 작아 확장성이 없다는 점, 다른 블록체인과 연결이 어렵다는 단점을 지닌다.

느린 처리속도

하나의 거래가 발생시 이를 즉시 처리하지 못하고 다수의 거래내역이 모여 하나의 블록을 형성할때 까지 기다려야 하기에 처리속도가 느리다. 블록을 형성한 이후에도 다른 노드들에게 이를 검증받아야 하기에 오랜시간이 소요된다.

블록체인을 이용한 암호화폐의 경우 '화폐'의 역할을 하려면 신속해야 하는 데 이런 점 때문에 실생활에서 결제수단으로서 이용하기 어렵다.

확장성 문제

블록체인을 구성하는 하나의 블록은 최대 크기가 정해져 있다. 초기 사용자수가 많지 않았을 때는 문제가 되지 않았지만, 사용자수가 증가함에 따라 하나의 블록안의 담을 수 있는 데이터의 최대 한도를 초과하는 경우가 발생하여 확장성 문제를 야기한다.

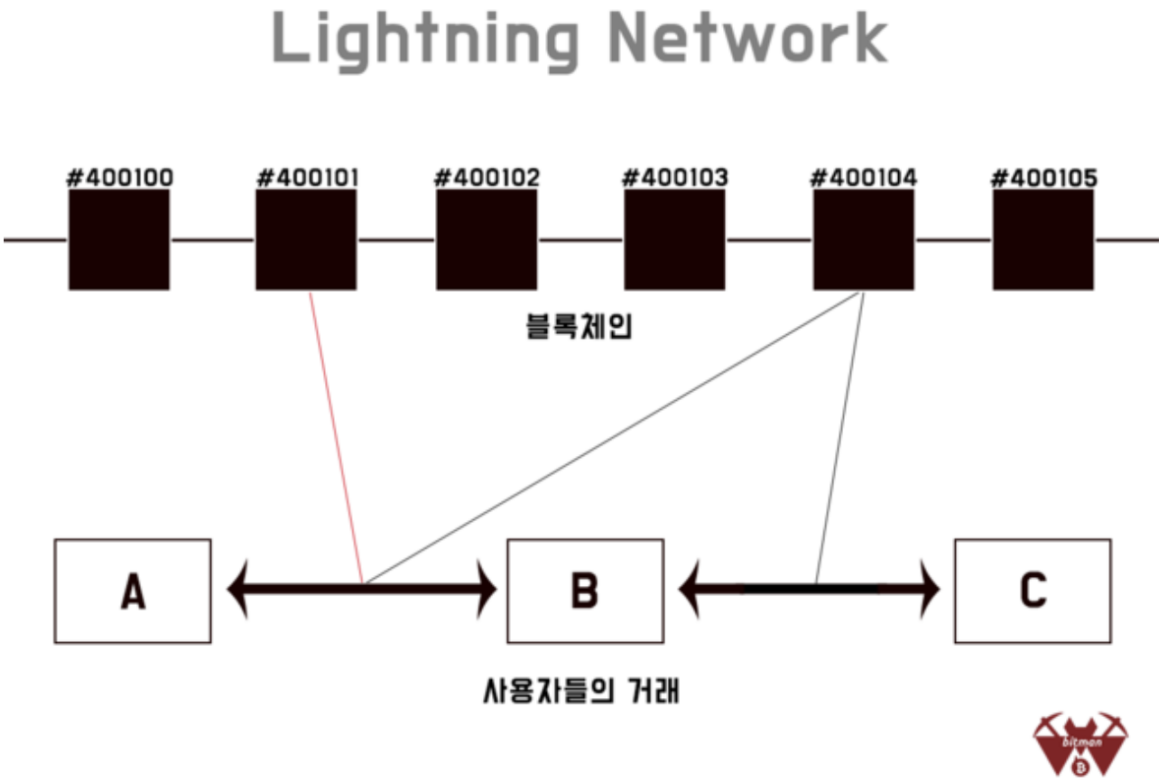
비트코인의 경우 블록 하나의 크기가 1MB로 제한되어 있었기 때문에, 하나의 블록당 2천건 정도의 트랜잭션을 기록하면 공간 부족 문제가 생긴다.

공간이 부족하면 기록되지 못하고 뒤로 밀리게 된다. 더 높은 수수료를 지급하면 순서에 상관없이 맨앞으로 이동하여 블록에 기록될 수 있으나 수수료 인플레이션 문제가 발생할 수 있다. 블록 하나의 크기를 증가시킬 수 도 있으나, 미사용 공간이 커지고 전체 블록체인의 사이즈가 커저 느려지는 문제가 생길 수 있다.

비트코인의 경우 2017년 8월1일자로 사용자의 디지털 서명부분을 블록에 기록하지 않고 제외하여 한 블록당 더 많은 데이터를 저장할 수 있도록 세그윗(SegWit)이라는 일시적 조치를 하였지만, 근본적 문제는 해결되지 않았다.

해결방안

느린처리속도와 확장성 문제를 해결하기 위한 다양한 알고리즘이 등장하고 있다.



(위쪽은 블록체인을 나타내고 아래쪽은 사용자 A.B.C를 나타냅니다.)

출처 : steemit

그 중 하나는 **라이트닝 네트워크(lightning network)**라는 알고리즘은 개별 거래를 다른 채널에서 처리하여 결과만 체인에 기록하는 방식으로 속도 문제를 해결한 알고리즘이다.

이와 유사하게 모든 거래내역을 메인 체인에서 처리하지않고 별도의 차일드체인(child chain)에서 처리하여 결과만 메인체인에 전달하는 방식인 **플라즈마(plasma)알고리즘**이 개발되었다.

이를 또 개량한 **플라즈마캐시 알고리즘**이 개발되었다. 이는 모든 사용자가 모든 블록을 다운로드해서 검증하는 것이 아닌 개별 사용자가 관심을 가진 특정 코인이 포함된 블록만 추적하여 속도를 증가시킨 알고리즘이다.

이와 같이 다양한 장점을 가진 블록체인이지만 한계 또한 가지고 있다. 이를 극복하기 위하여 알고리즘 기반으로 일부 기능을 개선했지만 여전히 한계를 지니고 있다. 그렇기에 이를 근본적으로 해결하기 위하여 블록체인 자체의 구조를 바꾸려는 시도가 생기고 있다.

블록체인의 속도가 느린 것은 거래내역이 발생한 즉시 처리하지 않고 블록을 구성할 때까지 기다리기 때문인데, 블록을 구성하지 않아야 근본적인 속도 개선이 가능하다.

이에 따라 블록이 없는 데이터 처리 알고리즘으로 탱글(tangle)과 해시그래프(hashgraph) 알고리즘이 나타났다. 탱글은 새로 발생한 거래가 이전에 발생한 2개의 거래를 확인해주는 방식이고, 해시그래프는 하나의 노드가 다른 불특정 노드에게 가십(gossip)을 전달하는 방식으로 작동하는 알고리즘이다. 이런 알고리즘은 블록이 존재하지 않지만, 기존 블록체인의 장점인 탈중앙화와 데이터 위변조 방지가 가능하면서도 속도 또한 빠르다.

블록에서 작업을 처리하는게 아니라 다른 네트워크에서 작업을 처리하고 결과만을 블록에 저장하는 알고리즘이 있다.

블록을 구성할 때까지 가디려서 성능이 느려지고 좋지 않았다.

근복적인 문제를 해결하기 위해 블록을 사용하지 않는 데이터 처리 알고리즘을 사용한다.

오라클 문제

블록체인에서 **오라클 문제(oracle problem)**란 블록체인 밖에 있는 데이터를 안으로 가져올 때 발생하는 문제를 말한다. 데이터를 블록체인 안에 넣어주는 사람이나 장치 있어야 하는데 이때 이런 중간 역할을 하는 사람이나 장치를 어떻게 신뢰할 수 있을 것인가 하는 문제이다. 블록체인 기술은 탈중앙 분산화를 추구하기에 권위를 가진 중앙이 존재하지 않기에, 데이터를 입력하는 중간자를 신뢰할 수 잇는 특별한 방법이 있어야 한다.

예시를 통해 알아보면 A와 B의 선택지에서 A가 선택될 경우 C에게 코인이 지급되고, B가 선택될 경우 D에게 코인이 지급되는 스마트 계약이 있다고 가정해보자. 실제로 A가 선택 되었더라도 데이터를 입력하는 중간에서 B가 선택되었다고 임의 혹은 실수하는 상황이 발생할 수 있다. 이 때 스마트 계약에 의해서 D에게 코인이 지급되므로 블록체인 상에서는 데이터 위변조가 일어나지 않은 것이지만 현실 데이터를 등록하는 과정에서 문제가 발생하는 데 이것이 오라클 문제이다.

해결방안

이러한 오라클 문제를 해결하기 위한 방법으로 암호화폐 소유자들이 투표를 통해 결정하거나 데이터의 중간값을 선택하거나 신뢰할 수 있는 데이터를 제공해주는 중간자를 두는 방법

등이 시도되고 있으나 확실한 해결책은 존재하지 않는다.

- **투표** : 암호화폐 소유자들이 지분증명이나 위임지분증명등의 방법으로 투표를 통해 의사결정을 하는 방법이다. 다만 이 방법은 암호화폐 소유자들이 투표 시 진실성에 기초하여 의사결정과정에 참여 하리라고 가정한다. 만약 허위로 투표할 경우에 피해는 암호화폐 소유자들에게 돌아가므로 진실하게 투표 하리라는 가정이다. 하지만 어디에서나 그렇지 않은 사람들이 존재하기 때문에 허위 투표를 할 가능성이 존재한다는 점을 가지고 있다.
- **중앙값** : 현실 세계에 존재하는 다양한 데이터 가운데 중앙값(median)을 선택하는 방안이다. 예를 들어 서로 다른 종류의 암호화폐를 직접 거래하려고 할때 수집한 가격들 중에서 중앙값을 선택하는 등에 대한 방법이다.
- **중간자(middleware)** : 신뢰할 수 있는 데이터를 제공해주는 중간자를 두는 방법으로서, 조직이나 소프트웨어가 데이터를 체계적으로 제공한다. 이러한 중간자의 예로 오라클라이즈(Oraclize), 체인링크(Chainlink), 아이캐시(iCash)등이 있다. 이러한 중간자는 네트워크에 중간에 존재하면서, 신뢰할 수 있는 데이터를 안정적이고 체계적으로 제공하여 오라클 문제를 해결할 수 있다. 하지만 탈중앙화를 지향하는 블록체인에서 중간자 역할을 하는 조직이나 소프트웨어가 새로운 형태의 중앙이 될 가능성이 존재한다.

오라클은 블록체인의 밖에 있는 데이터를 넣을 때 신뢰성을 어떻게 보장해야하는가 하는 문제이다.

100% 해결책은 없고 신뢰성을 높이기 위한 방법이 제안되었다.

투표 암호화페 소유자들이 투표. 허위로 투표하면 망함.

중앙값 거래하려는 값의 중간값을 선택

중간자 신뢰할 수 있는 중간자를 두는 방법(탈중앙화를 지향하는 블록체인에서 새로운 중앙이 될 가능성이 있음)