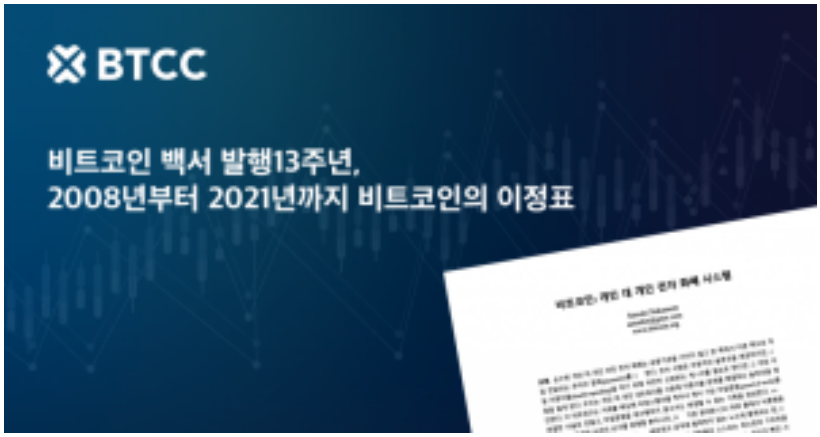
비트코인 백서 발행 2008년부터 2021년까지 13주년, 비트코인의 이정표 -BTCC

원문:
https://www.btcc.com/ko-KR/academy/research-analysis/bitcoin-white-paper



13년 전- 2008년 10월 31일 비트코인(BTC) – 최초의 완전히 분산된 P2P 전자 현금은 익명의 제작자 (사토시 나카모토) Satoshi Nakamoto에 의해 고안되었습니다. 비트코인 백서: P2P 가상회폐 시스템은 비트코인을 세상에 소개되었습니다. 13년이 지난 후에도 비트코인의 백서는 계속해서 비트코인의 능력과 핀테크 세계에서 그 영향력이 커지고 있습니다.

BITCOIN

비트코인의 역사

비트코인 백서 발행 **13**주년을
함께 기념해요!

2008년 10월 31일
사토시 나카모토가 발행한 비트코인 백서

2009년 1월 3일
제네시스 블록 생성

2009년 1월 12일
첫 비트코인 거래

2010년 7월 16일
비트코인 가격
0.008달러에서 0.08달러로 10배 상승

2010년 12월 12일
사토시가 온라인에 마지막 게시물을 올림

2011년 6월 9일
BTCC 거래소 설립

2012년 5월 9일
BTCC 일일 거래량 2,000BTC 초과

2012년 11월 28일
첫 번째 비트코인 반감기, 비트코인 가격 $12.35

2013년 4월 10일
BTCC 일일 거래량 28,600BTC 초과

2013년 10월 29일
최초의 비트코인 ATM 등장

2017년 1월 2일
비트코인 가격 1,000달러 돌파

2017년 10월 31일
CME, 비트코인 선물 출시

2017년 11월 28일
비트코인 10,000달러 돌파

2021년 6월 9일
BTCC 10주년

2021년 10월 21일
비트코인 최고가격 6만6천 달러 돌파

2021년 10월 31일
BTCC와 함께 비트코인의
13번째 생일을 축하해요!

BTCC카카오채널
btcc2011을 추가해주세요!

비트코인 백서, 암호화폐가 시작된 곳

2008년 말 글로벌 금융 위기를 겪으면서 전 세계 은행 업계, 정부 및 기타 중앙 당국에 대한 분노가 최고조에 달했습니다. 금융 기관은 사용자에게 높은 거래 비용을 부과하여 분쟁 해결 및 조정을 위한 노력을 기울입니다. 소액 또는 소액 거래는 비실용적이므로 금융 기관에 지불해야 하는 최소 거래 규모가 사용자에게 적용됩니다. 이 프로세스는 느리고 비용이 많이 드는 것으로 간주됩니다. 소유권 확인 및 이중 지출 문제도 제3자 금융 중개업체와 관련된 주요 문제입니다.

중개 금융 당국에 의존하여 발생하는 문제를 해결하기 위해 비트코인 백서는 새로운 분산형 온라인 결제 시스템을 구축합니다.

문제 및 솔루션

1. 암호화 및 블록체인을 통한 제3자 중개자의 필요성 제거

“저는 신뢰할 수 있는 제3자가 없는 완전한 P2P 방식의 새로운 전자 현금 시스템을 개발하고 있습니다.” 공개된 이메일에 사토시가 쓴 말이었다. Satoshi는 전자 현금 결제가 각 거래를 승인하고 실행하기 위해 은행이나 서비스와 같은 “제3자 중개자”에 의존하기 때문에 문제가 있다고 주장합니다.

비트코인 통화 시스템은 사용자를 위조로부터 보호하기 위해 변경할 수 없고 암호화 증거를 기반으로 하는 P2P 거래를 허용함으로써 제3자 중개자에 대한 신뢰의 필요성을 제거합니다. 은행은 거래를 용이하게 하기 위해 필요하지 않습니다. 정부는 또한 통화의 생성과 보급에 필요하지 않습니다. 이것은 비트코인이 분산 데이터베이스 네트워크에서 디지털 거래의 공개 장부인 블록체인 기술에 의해 뒷받침되기 때문에 가능합니다. 수천 대의 컴퓨터에서 동시에 실행되어 전 세계에 기록을 배포합니다. 네트워크의 모든 사람은 이 시스템을 지속적으로 확인하고 업데이트합니다.

2. 타임스탬프 서버 및 작업 증명을 통한 이중 지출 문제 해결

비트코인 화폐 시스템 이전까지는 디지털 화폐가 2회 이상 거래되는 이중지불이 디지털 화폐 거래에서 큰 문제였다. 이는 수취인이 제3자 검증 서비스를 거치지 않고는 이미 지출된 자금이 이미 지출되었는지 여부를 확인할 수 없기 때문입니다. 사용자가 통화를 이중으로 사용하면 전체 공급이 부풀려지고 다른 모든 사람의 돈은 평가절하됩니다.

백서에서 Satoshi는 P2P 분산 타임스탬프 서버의 사용을 솔루션으로 제안했습니다.

타임스탬프 서버는 암호화 해시에 포함하기 위해 실시간으로 트랜잭션을 기록하는 소프트웨어입니다. 해시는 거래가 블록체인에 추가되기 전에 채굴자가 해결하는 복잡한 수학 문제 역할을 하는 일련의 고유한 숫자와 문자입니다. 이 프로세스를 작업 증명 또는 마이닝이라고 합니다. 이것은 거래를 검증하기 위한 합의 시스템입니다. 이를 통해 각 노드(암호화 네트워크에 연결된 컴퓨터)는 트랜잭션 검증에 함께 참여하여 동일한 트랜잭션 레코드 세트를 유지하고 공유하여 분산형 P2P 네트워크 시스템을 형성할 수 있습니다. 작업 증명 문제(솔루션은 올바른 해시)를 성공적으로 해결한 광부, 새 블록이 블록체인에 추가됩니다. 채굴자들은 비트코인(인센티브)으로 보상을 받습니다. 새로운 거래는 이후에 비트코인 네트워크의 모든 컴퓨터 또는 노드로 브로드캐스트됩니다.

거래를 되돌리려면 값비싼 하드웨어 장비와 전력 사용을 비롯한 막대한 비용이 필요하므로 사기 거래가 불가능합니다. 예를 들어 1시간의 거래를 되돌리려면 비트코인 전체 해시파워의 51%가 필요합니다. PoW를 해결하고 대중적인 합의 메커니즘으로 운영하는 데 어려움이 있기 때문에 모든 후속 블록을 다시 채굴해야 하기 때문에 블록체인을 변경하는 것은 불가능합니다. 블록체인은 노드의 분산 네트워크에 의해 유지되며 모든 참가자는 합의에 도달하기 위해 협력해야 합니다. 더 많은 채굴자가 네트워크에 참여할수록 한 개인이나 그룹이 블록체인에서 거래를 되돌릴 수 있는 충분한 계산 능력을 얻을 확률이 감소합니다. 위에 설명된

요소는 블록체인을 매우 안전하게 만듭니다.

비트코인의 13번째 생일을 축하합니다!

비트코인 백서 중 발췌

순수한 개인 대 개인 버전 전자 화폐는 금융기관을 거치지 않고 한 쪽에서 다른 쪽으로 직접 전달되는 온라인 결제를 실현한다. 전자 서명은 부분적인 솔루션을 제공하지만, 만일 이중지불을 막기 위해 여전히 신뢰받는 제3자를 필요로 한다면 그 주된 이점을 잃게 된다. 우리는 개인 대 개인 네트워크를 사용해 이중지불 문제를 해결하는 솔루션을 제안한다. 이 네트워크는 거래를 해싱해 타임스탬프를 찍어서 해시 기반 작업증명을 연결한 사슬로 만들고, 작업증명을 재수행하지 않고서는 변경할 수 없는 기록을 생성한다. 가장 긴 사슬은 목격된 사건의 순서를 증명할 뿐아니라, 그게 가장 광대한 CPU파워 풀에서 비롯했음을 증명하기도 한다. 과반의 CPU파워가 네트워크 공격에 협력하지 않는 노드에 통제되는 한, 그 힘은 가장 긴 사슬을 만들어 내며 공격자를 압도한다. 이 네트워크 스스로는 최소한의 고조만을 요구한다. 메시지는 최선의 노력을 다해 퍼져나가고, 노드는 자기가 빠진 사이에 벌어진 거래의 증명으로 가장 긴 작업증명 사슬을 채택함으로 뜻대로 네트워크를 떠났다가 재합류할 수 있다.

전자화폐의 정의

비트코인 백서에서는 “전자 화폐”를 디지털 서명의 연속으로 정의한다.

좀더 풀어서 설명하면 전자화폐는 이전에 거래를 누구 누구랑 얼마만큼 해왔는지, 현재 갖고있는 돈이 얼마인지를 보여주는 장부 또는 증명서로써의 역활을 하는것임.

거래

우리는 서로간의 합의를 통한 전자서명을 코인으로 칭한다. 거래를 할 때, 사용자는 과거의 모든 거래기록과 함께 본인의 새로운 거래기록을 추가하여 공유한다. 하지만, 이렇게 개인이 정보를 기록하고 주고받게 된다면, 서로 동시에 거래를 기록하게 되거나, 누가 먼저 기록을 하였는지 알수 없는 이중지불 문제가 발생하게 된다. 그렇기 때문에 각 사용자(노드)들은 모두 전송된 거래를 확인하여, 한 시장 안에 있는 노드중에 다수의 노드가 동의한 체인을 올바른 거래로 인정하게 된다.

타임스탬프

위에서 본 문제를 해결하기 위해 제시된 해결책이 바로 타임스탬프의 활용이다. 타임스탬프 서버는 그 당시의 기록들을 해싱하여 저장하고 있다. 새로운 기록이 들어올 경우 이 또한 해싱하여 저장을 하게 되고, 이렇게 계속 거래기록들을 이어나가게 된다.

작업 증명(POF)

컴퓨터는 계속하여 nonce값을 찾는 연산을 진행하게 된다. 블록에는 거래내역을 담게 되는데, 이 블록들에 대해 컴퓨터는 작업증명을 진행하게 된다. 작업증명이 완료된 블록은 신뢰되는 블록으로 변하게 되고, 이는 체인에 연결된다. 작업증명의 난이도는 채굴이 진행될수록 올라가게 된다.

네트워크

블록체인 네트워크의 진행과정은 이렇다

새로운 거래내역이 모든 노드로 발송된다.

각 노드들은 새로운 거래내역을 블록에 넣는다.

각 노드들은 블록에 맞는 작업증명을 거친다.

작업증명을 먼저 끝낸 노드는 그 블록을 다시 다른 노드들에게 모두 전송한다.

노드는 그 블록이 유효한 경우에 블록을 수락하고 기록한다.

블록을 퍼트린 노드는 블록체인에 다음 블록을 추가하게 된다.

인센티브

앞서 소개했던 노드들은 모두 채굴을 진행하게 되는데, 이중에서 처음으로 작업증명을 끝낸 노드에게는 인센티브가 주어진다. 비트코인 형식으로 보상을 줌으로서 노드들이 계속하여 작업증명을 할 수 있는 환경을 만든다.

디스크 공간 회수하기

블록체인 상에 기록들을 계속 저장해두게 되면, 이는 용량을 굉장히 많이 차지하게 될 것이다. 이 때문에 블록체인은 계속하여 필요없는 부분들의 자료를 간소화하고 쳐내면서 용량을 유지하게 된다.

간단한 결제 검증

풀 네트워크 노드를 가동하지 않아도 결제들을 검증 할 수 있다. 가장 긴 체인의 블록 헤더의 사본만 가지고 있으면 검증을 할 수 있다. 하지만, 만약 블록체인 네트워크 상의 50프로 이상이 공격자로 구성되어 있다면 네트워크가 위험해 질 수 있다.

가치 합치기

블록체인 상에서의 거래는 여러개의 입출력 공간을 둠으로서 거래를 합치고 나눌 수 있다.

보안

기존에 은행과 같은 제 3자가 거래에 개입하는 경우에는 공개되어 있는 정보를 제한하여 보안을 유지했다. 하지만, 블록체인 상에서는 이와 다르게 거래정보를 공개하지만, 이 데이터를 암호화 하여 누가 거래를 하였는지는 모르게 하여 보안을 유지하게 된다.

결론

블록체인은 단순히 신뢰를 기반을 하는 거래에서 벗어나는 기술이다. 제 3자의 개입이 없이 p2p 방식으로 개인과 개인이 거래를 주고받고, 아무때나 들어갔다 나올 수 있는 단순하면서도 안정적인 시스템이다.