모네로(XMR)에 대하여

원문:

https://www.btcc.com/ko-KR/markets/Monero/chat

모네로(Monero)는 익명성을 중요시하는 대표적 암호화폐로, 개발자 및 프라이버시 보호주의자로 구성된 대규모 오픈 소스 커뮤니티에서 지원합니다. 2014년에 론칭한 바이트코인(ByteCoin) 프로토콜의 포크로 시작된 모네로는 프라이버시 보호, 탈중앙화, 대체 가능성을 달성하기 위해 일련의 고급 암호학적 기본 요소를 활용하는 암호화폐인 크립토노트(CryptoNote) 코인 중 하나입니다.

모네로 팀은 프라이버시와 보안이 가장 우선적인 목표이며, 사용의 용이성과 효율성이 그 다음이라고 설명합니다. 모네로는 사용자가 얼마나 기술 분야에 능숙한지와 관계 없이 모든 사용자를 보호하는 것을 목표로하고 있습니다.

XMR은 검열에 대한 두려움 없이 신속하고 저렴한 방식의 지불을 제공하고자 합니다.

모네로(Monero)의 유래

7명의 개발자가 모네로를 만드는 데 참여하였으며, 그중 5명은 익명으로 남기로 결정하였습니다. XMR이 <u>비</u>트코인의 창시자인 사토시 나카모토(Satoshi Nakamoto)에 의해 만들어졌다는 루머가 있기도 합니다.

XMR의 기원은 2012년 출시된 프라이버시 중심의 탈중앙화 암호화폐 바이트코인(Bytecoin)으로 거슬러 올라갑니다. 2년 후, 비트코인토크(Bitcointalk) 포럼의 회원으로서 'thankful_for_today'로만 알려진 한 인물이 BCN의 코드베이스를 포크하였고, 이에 따라 모네로가 탄생하였습니다. 이들은 바이트코인에 다른 사람들이 동의하지 않는 "논쟁의 여지가 있는 변화"를 도입하고자 하였고, 스스로 문제를 해결하고자 했습니다.

수년간 XMR에 공헌한 개발자는 수백 명이 넘는 것으로 추산되고 있습니다.

특징

링서명

모네로는 일회용 공개 대상(destination) 키로 전송된다. 링 서명 메커니즘을 통해 발신인은 다른 그룹 멤버의 개인키들과 함께 해당하는 개인키를 사용할 수 있습니다. 따라서 공개 대상 키와 발신인 그룹에 속하는 구성원의 개인키를 결합한 여러 개의 트랜잭션 키들이 생깁니다.

이 기능은 발신인을 익명으로 유지하는 데 도움이 됩니다.

스텔스 주소

스텔스 주소는 모네로의 고유한 개인정보 보호의 중요한 부분입니다. 이 기능을 사용하면 보낸 사람이 받는 사람을 대신하여 모든 트랜잭션에 대해 임의의 일회용 주소를 만들 수 있습니다.

수신자는 하나의 주소만 게시할 수 있지만 수신되는 모든 지급액은 수신자의 게시 주소 또는 다른 거래 주소로 다시 연결할 수 없는 블록체인의 고유 주소로 이동합니다.

대체 가능성

다른 암호화폐와 달리 모네로는 진정으로 대체 가능한 암호화폐입니다. 대체 가능성을 이해하기 위해 예를 들어 보겠습니다. 두 개의 지폐는 가치가 같지만 동일할 수 있습니까? 아니요, 다른 제품/서비스와 연결될수 있기 때문입니다. 그러나 같은 등급의 1온스 금괴 2개는 대체할 수 있습니다. 모네로는 그 금덩이이고 다른 암호화폐는 1달러 지폐입니다.

모네로(MONERO,XMR) 기능

모네로는 커뮤니티가 탈중앙화를 크게 강조하는 <u>작업증명(PoW)</u> 암호화폐이며, 모네로 ASIC 저항을 만들어내기 위해 다방면의 노력을 기울였습니다. ASIC이란 PoW 네트워크를 위해 특화된 <u>채굴</u> 하드웨어로서, 채굴자의 중앙화로 이어질 수 있습니다. 따라서 모네로는 네트워크에서 ASIC 성능을 제한하기 위해 네트워크 프로토콜의 소프트 포크를 배포했습니다.

모네로가 배포한 크립토노트 기술은 광범위한 암호화폐 시장에서 가장 심오한 프라이버시 보호의 사례를 보여 줍니다. 이 네트워크는 링 기밀 거래(Ring Confidential Transaction, "RingCT"), 링 서명, 스텔스 주소, 방탄 기능과 같은 암호학적 구성 요소를 사용하여 블록체인 레벨에서 트랜잭션의 세부 정보를 완전히 마스 킹합니다.

모네로 거버넌스는 '대략적 합의(rough consensus)' 모델을 이용합니다. 즉, 주요 개발자와 폭넓은 커뮤니티가 참여하는 일련의 오프 체인(off-chain) 의사결정을 통해 네트워크 업그레이드 및 개발 제안을 처리합니다.

블록 및 마이닝

모네로의 작업증명 알고리즘(최근 CryptoNight에서 RandomX로 바뀜)은 CPU 채굴을 지지하고, GPU 채굴 효과를 감소시켜 시스템을 보다 공정하게 만들고자 합니다.

이는 일반 사용자 수준의 PC가 경쟁력을 갖추게 됨에 따라 마이닝이 더욱 분산된다는 논리를 따릅니다. 그럼에도 불구하고, 해싱 파워는 소수의 마이닝 풀에 의해 상대적으로 집중되어 있습니다.

비트코인과 다르게 모네로는 고정된 한도의 블록 크기를 갖고 있지 않습니다.

대신, 모네로는 동적 블록 크기를 갖고 있으며, 이는 증가하는 수요를 감당하기 위해 블록이 확장될 수 있다는 의미입니다. 따라서, 수요가 감소할 경우 허용 크기가 줄어들 것입니다.

블록 크기는 이전 100개의 블록의 중간 값을 참조합니다(블록은 평균 2분마다 1개씩 마이닝 됨). 마이너는 제한 크기를 초과하는 블록을 생성할 수 있지만, 더 낮은 보상을 받게 됩니다.

코인 전망

비트코인 BTC 전망

리플 XRP 전망

이더리움 ETH 전망

도지코인 DOGE 전망

에이다 ADA 전망

솔라나 SOL

솔라나 SOL 전망

이오스 EOS 전망

이오스 EOS

아발란체 AVAX 전망

아발란체 AVAX

체인링크 LINK 전망

라이트코인 LTC 전망

폴리곤 MATIC 전망

대시 코인 DASH 전망

스테픈 GMT 전망

스테픈 GMT

비트코인캐시 BCH 전망

스텔라루멘 XLM 전망

연파이낸스 YFI 전망

웨이브코인 WAVES 전망

비트코인SV BSV 전망

파일코인 FIL 전망

옵티미즘 OP 전망

트론 TRX 전망

갈라코인 GALA 전망

엔진 코인 ENI 전망

디센트럴랜드 MANA 전망

샌드박스 코인 SAND 전망

이뮤터블 X IMX 전망

엑시 인피니티 코인 AXS 전망

플로우 FLOW 전망

프로젝트 갤럭시 GAL 전망

마스크 네트워크 MASK 전망

에이프코인 APE 전망

<u>이더리움 네임 서비스 ENS 전망</u>

1인치네트워크 1INCH 전망

커브코인 CRV 전망

DYDX 전망

팬케이크스왑 CAKE 전망

유니스왑 UNI 전망

테라코인 전망

알고랜드 ALGO 전망

<u>팬텀 FTM 전망</u>

셀로 CELO 전망

블러 BLUR 전망

미나프로토콜 MINA 전망

NEAR 전망

톤 TON 전망

퀀텀코인 QTUM 전망

인터넷 컴퓨터 ICP 전망

폴카닷 Polkadot 전망

메인넷 출시한 앱토스 Aptos 전망

코스모스 ATOM 전망

네오코인 NEO 전망

바이낸스코인 BNB 전망

바이낸스 코인 BNB 전망

시바이누 SHIB 전망

알케미페이 ACH 전망

콘플럭스 CFX 전망

CORE 전망

아르위브 AR 전망

신세틱스 SNX 전망

메져러블 데이터 토큰 MDT 전망

어드벤처골드 AGLD 전망

아비트럼 ARB 전망

아라곤 ANT 전망

멀티버스 X 엘론드 EGLD 전망

이더리움 PoW ETHW 전망

더 그래프 The Graph GRT 전망

후크드 프로토콜 HOOK 전망

클레이튼 KLAY 전망

룩스레어 LOOKS 전망

렌 REN 전망

스토리지 Stori 전망

쎄타 Theta 전망

넴 NEM XEM 전망

모네로 XMR 전망

지캐시 코인 ZEC 전망

메타버스 코인 RNDR 전망

레이븐코인 RVN 전망

질리카 Zilliqa ZIL 전망

월간 최고치 경신한 페페코인 PEPE 전망

아비도지 AIDOGE 전망

<u>반등세 보이는 수이 SUI 전망</u>

플로키 이누 FLOKI 전망

<u>싱귤래리티넷 AGIX 전망</u>

ALPHA 전망

앵커 Ankr 전망

알파체인 ARPA 전망

<u>아스타 네트워크 Astar ASTR 전망</u>

밸런서 BAL 전망

밴드 프로토콜 BAND 전망

벨라프로토콜 BEL 전망

바이너리엑스 BinaryX 전망

파산 신청한 셀시우스 CEL 전망

셀러네트워크 CELR 전망

코코 스왑 COCO 전망

컴파운드 Compound COMP 전망

셴투 Shentu CTK 전망

카르테시 Cartesi CTSI 전망

시빅 Civic CVC 전망

도도 DODO 전망

오픈캠퍼스 EDU 전망

AI 코인 페치에이아이 Fetch.AI 전망

플로키 이누 FLOKI 전망

프랙스쉐어 FXS 전망

기프토 Gifto GFT 전망

지엠엑스 GMX 전망

헤데라 HBAR 전망

하이스트리트 HIGH 전망

아이콘 ICON ICX 전망

ID 정망

재스미 JasmyCoin 전망

트레이더조 IOE 전망

쿠사마 KSM 전망

리니어파이낸스 LINA 전망

리퀴티 LOTY 전망

루프링 Loopring 전망

메이커 MKR 전망

오션프로토콜 Ocean 전망

RDNT 전망

아이젝 iExec RLC 전망

로켓풀 Rocket Pool 전망

리저브 라이트 Reserve Rights 전망

SSV 네트워크 전망

스타링크 Starlink 전망

스타게이트 파이낸스 STG 전망

스톰엑스 StormX 전망

Stacks Stx 전망

솔라 SXP 구 스와이프) 전망

토모체인 TomoChain TOMO 전망

텔러 Tellor TRB 전망

우마 UMA 전망

테라클래식USD USTC 전망

비체인 VeChain VET 전망

우네트워크 WOO 전망

일드길드게임즈 YGG 전망

제로엑스(0x) ZRX 전망

신흥 밈코인 페페2.0 PEPE 2.0 전망

뱅코르 Bancor BNT 전망

저스트 Just JST 전망

스몰 러브 포션 SLP 전망

스텝앱 Step App FITFI 전망

<u>치아 네트워크 XCH 전망</u>

뱃저 다오 Badger DAO 전망 퍼페츄얼프로토콜 PERP 전망 크로노스 CRO 전망 하모니 Harmony ONE 전망 코티 COTI 전망 바이코노미 Biconomy BICO 전망 도라팩토리 DoraFactory DORA 전망 <u> 갓즈 언체인드 GODS 전망</u> 스웨트코인 SWEAT 전망 스펠 토큰 SPELL 전망 플레어 Flare FLR 전망 카데나 Kadena KDA 전망 <u>카바 Kava 전망</u> 크레딧코인 Creditcoin CTC 전망 일루비움 Illuvium ILV 전망 아크로폴리스 Akropolis AKRO 전망 트러스트 월렛 토큰 TWT 전망 <u>에일리언 월드 TLM 전망</u> 화제 중심의 월드코인 WLD 전망 캐스퍼 Casper CSPR 전망 에이브 Aave 전망 에이피아이쓰리 API3 전망 라이브피어 Livepeer LPT 전망 토르체인 RUNE 전망 블루젤 Bluzelle BLZ 전망 세이네트워크 Sei 전망 카스파 Kaspa KAS 전망 퀀트 Quant QNT 전망 사이버커넥트 CYBER 전망 아이오텍스 IoTeX IOTX 전망 ETH2.0 전망 너보스 네트워크 CKB 전망

백서

오토마타 네트워크 ATA 전망 플라밍고 Flamingo FLM 전망

테조스 Tezos XTZ 전망



공식 웹 사이트