지캐시(ZEC)란? |이해 및 소개

워문:

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

지캐시(Zcash,ZEC)는 프라이버시와 익명성에 초점을 맞춘 탈중앙화 암호화폐입니다. 지캐시는 zk-SNARK 영지식 증명 기술을 사용하여 트랜잭션 관련 민감한 정보를 노출하지 않고도 네트워크 노드가 트랜잭션을 검증할 수 있도록 합니다.

ZCash는 사용자의 개인 정보를 중요하게 생각하며 영지식 증명(zk-SNARK)을 사용하여 거래를 확인하여 이를 보장합니다. 이러한 방식으로 사용자를 대신하여 정보가 제공되지 않습니다.

지캐시(Zcash)는 2016년 10월 28일에 만들어졌으며, 익명성 보장을 특징으로 하는 모네로, <u>대시</u>와 함께 프라이버시 코인 3대 대장으로 불렸습니다. 지캐시는 영지식 암호(zero-knowledge cryptography) 기술을 사용하여 개인의 거래 정보를 완전히 보호할 수 있습니다. 지캐시는 결제가 퍼블릭 블록체인에서 이루어지지만, 거래의 발신자, 수신자 및 거래 금액은 비공개로 유지됩니다.

비트코인, 이더리움 등 퍼블릭 <u>블록체인</u>의 경우 해당 계정(지갑)의 주인이 누구인지는 알 수 없지만, 해당 계정의 모든 거래 내역이 공개되어 추적이 가능하므로 프라이버시 문제가 생길 수 있습니다. 지캐시는 이러한 추적 가능성 문제를 해결하기 위해 탄생했습니다.

지캐시의 역사

지캐시는 2013년 Matthew Green, Christina Garman 및 Ian Miers 등 암호학자들이 제안한 제로코인(Zerocoin)이라는 프로토콜에서 유래했습니다. 제로코인은 프라이버시 관련 개선사항을 블록체인에 도입한 비트코인의 확장판입니다.

당초 제로코인(Zerocoin) 제안이 비트코인 개발자 커뮤니티 내에서 설득력과 수용력이 부족에 직면하자 핵심 제로코인 팀은 독자적인 암호화폐를 출시하기로 결정했습니다. 그들은 새로운 코인 개발을 위해 유명 암호학자 주코 윌콕스(Zooko Wilcox-O'Hearn)과 협력했고, 일라이 벤 사순(Eli Ben-Sassoon)과 알레산드로 치에사(Allesandro Chiesa)를 포함한 다른 여러 과학자들을 영입했습니다.

월콕스는 현재 **일렉트릭 코인사**의 CEO로 남아 30여 명의 직원과 함께 지캐시의 개발을 이끌고 있습니다. 특히, 채굴된 모든 지캐시의 약 20%는 코인 개발 첫 4년(2021년 종료) 동안 개발자를 지원하는 데 사용되었습니다. 2018년에 윌콕스는 연간 약 360만 달러 상당의 지캐시를 받고 있다고 밝혔습니다. 지캐시를 채굴하면 코인의 20%가 지캐시 개발자들에게 보상으로 돌아가는데, 20% 비율이 채굴자들에게 불리하게 작용되기 때문에 공정성의 문제가 대두되면서 이는 암호화폐 커뮤니티 내에서 논란의 대상이 되었습니다. 일부는 코인이 너무 중앙 집중화되어 있다고 비난했고 다른 일부는 오히려 윌콕스를 옹호하며 그의 투명성을 칭찬했습니다.

지캐시 작동워리

ZEC 거래는 투명 전송, 보안(shielded) 전송의 두 가지 방식으로 전송될 수 있습니다. 투명 거래는 비트코인과 동일한 방식으로 작동됩니다.

지캐시는 암호 산업의 최신 기술 발전을 기반으로 암호 전문가 팀이 개발한 영지식 스나크(zk-SNARK)라는 제로 지식 증명구조를 사용합니다. 이러한 구조를 통해 네트워크에서 사용자 및 거래금액을 공개하지 않고 도 잔액 장부에 대한 보안을 유지할 수 있습니다.

지급 권한 및 거래액을 공개적으로 보여주는 대신 거래 메타데이터를 암호화하고 영지식 스나크(zk-SNARK)를 사용해 부정 행위 및 도용 행위가 없음을 증명합니다.

모든 지캐시의 거래가 비공개로 처리되는 것은 아닙니다. 지캐시를 사용하면 비트코인처럼 공개적으로 거래할 수도 있습니다. 지캐시는 거래 내역을 공개하는 공개 계좌(transparent account)와 비공개 계좌(shield account)를 모두 지원하므로, 사용자는 지캐시 전송 시 공개 여부를 선택할 수 있습니다. 또한 공개 계좌와 비공개 계좌 간의 거래도 가능합니다. 비공개 계좌에서 공개 계좌로 전송된 내역에서는 공개 계좌로 수신된 정보는 볼 수 있지만, 비공개 계좌의 정보는 확인이 불가능합니다.

지캐시(ZEC) 장점

지캐시의 주요 장점은 선택적인 익명성입니다. 이는 일반적인 가명 암호화폐인 <u>비트코인</u>이나 이더리움을 통해서는 얻을 수 없는 수준으로 프라이버시를 보장합니다.

이러한 퍼플릭 트랜잭션은 명시적인 방식으로 사용자의 신원을 드러내지 않습니다. 외부 관찰자가 블록체 인으로부터 액세스할 수 있는 유일한 식별자는 퍼블릭 주소입니다. 그러나 데이터 과학자와 법 집행 기관들 이 최근 수년간 노력을 통해 블록체인 분석 방식은 이해관계가 있는 당사자는 공정하고 신뢰할 수 있도록 블 록체인 상의 퍼블릭 주소를 소유자의 실제 세계 신원에 연결할 수 있는 수준으로 발전되어, 기본적으로는 프라이빗 트랜잭션을 불가능해졌습니다.

한편 보안된 ZEC 트랜잭션은 영지식증명(zk-SNARK: Zero-knowledge succinct non-interactive arguments of knowledge) 기술을 활용하여 변경 불가능한 퍼블릭 블록체인에서 완전한 익명의 트랜잭션을 가능하게 합니다. 트랜잭션이 발생한 사실은 원장에 기록되지만 송신 및 수신 주소 및 발송 금액은 퍼블릭에 공개되지 않습니다.

이를 통해 지캐시는 사용자들에게 프라이버시 권리를 제공하면서도, 탈중앙화된 무허가성 디지털 통화의 이점을 누릴 수 있습니다.

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

이더리움 네임 서비스 ENS 전망

1인치네트워크 1INCH 전망

커브코인 CRV 전망

DYDX 전망

패케이크스왑 CAKE 전망

유니스왑 UNI 전망

테라코인 전망

알고랜드 ALGO 전망

팬텀 FTM 전망

셀로 CELO 전망

블러 BLUR 전망

미나프로토콜 MINA 전망

NEAR 전망

톤 TON 전망

퀀텀코인 OTUM 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 Zilliga ZIL 전망

월간최고치 경신한 페페코인 PEPE 전망

아비도지 AIDOGE 전망

반등세 보이는 수이 SUI 전망

플로키 이누 FLOKI 전망

싱귤래리티넷 AGIX 전망

ALPHA 전망

앵커 Ankr 전망

알파체인 ARPA 전망

아스타 네트워크 Astar ASTR 전망

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

센투 Shentu CTK 전망

<u>카르테시 Cartesi CTSI 전망</u>

시빅 Civic CVC 전망

도도 DODO 전망

오픈캠퍼스 EDU 전망

AI 코인 페치에이아이 Fetch.AI 전망

플로키 이누 FLOKI 전망

프랙스 쉐어 FXS 전망

기프토 Gifto GFT 전망

지엠엑스 GMX 전망

헤데라 HBAR 전망

하이스트리트 HIGH 전망

<u>아이콘 ICON ICX 전망</u>

ID 전망

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 민코인 페페2.0 PEPE 2.0 전망

뱅코르 Bancor BNT 전망

저스트 Just IST 전망

<u>스몰 러브 포션 SLP 전망</u>

스텝앱 Step App FITFI 전망

치아 네트워크 XCH 전망

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

갓즈 언체인드 GODS 전망

스웨트코인 SWEAT 전망

스펠 토큰 SPELL 전망

플레어 Flare FLR 전망

카데나 Kadena KDA 전망

카바 Kava 전망

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

<u>너보스 네트워크 CKB 전망</u>

오토마타 네트워크 ATA 전망

플라밍고 Flamingo FLM 전망

테조스 Tezos XTZ 전망

백서

<u>고</u>

공식 웹 사이트