5.0 사토시 나카모토의 수수께끼**:** 비트코인**(Bitcoin)**과 프라이버시 혁명

사토시 나카모토라는 신비롭고 뛰어난 혁신가는 금융 거래가 국경을 초월하고, 투명하며, 안전하게 이루어지는 미래를 꿈꿨습니다. 정부와 은행의 통제로부터 자유로운 그런 미래를 말이죠. 2008년, 사토시는 비트코인 백서를 통해 자유 혁명을 촉발했습니다. 이 백서에서는 블록체인 기술의 첫 실용적 구현을 설명했습니다. 비트코인은 금융 위기와 중앙집권적 기관들에 대한 신뢰가 무너지고 있는 세상에서 희망과 회복력의 상징으로 떠올랐습니다. 첫 번째 비트코인 거래는 2009년 1월에 이루어졌습니다.

탈중앙화된 금융 시스템을 구축하려는 열망에 이끌려, 사토시의 비트코인은 권력을 사람들에게 돌려주고, 기존의 질서에 도전하며 금융 자유를 옹호하는 세계적인 운동을 촉발시켰습니다.

5.1 지캐시**(Zcash)**와 비트코인 소개

7년 후인 2016년에, 과학자들과 연구자들로 구성된 한 그룹이 지캐시를 출시했습니다. 그들의 목표는 사토시의 비트코인이 가져온 혁신적인 힘을 개선하는 것이었으며, 특히 프라이버시 기능을 추가하는 것이었습니다. (이에 대해서는 나중에 더 다룹니다.)

지캐시는 비트코인을 포크(fork)한 코인입니다. 이는 비트코인의 코드를 본질적으로 복사하고 수정했다는 것을 의미합니다. 지캐시에 대한 아이디어는 2014년에 MIT, 존스홉킨스 대학, 테크니온, 그리고 텔아비브 대학의 교수들과 학술 연구자들에 의해 발표된 백서에서 처음 설명되었습니다. 이 아이디어는 여러 해에 걸쳐 Zooko Wilcox-O'Hearn과 그의 팀이 이끄는 Electric Coin Co. (ECC; 이전에는 Zcash Company라고 불림)에서 개발되었습니다.

사람들은 지캐시를 사용하여 낮은 수수료로 효율적이고 안전하게 거래합니다. 지캐시는 프라이버시를 보호하며, 빠르고 유연하며 누구나 접근할 수 있도록 디지털 시대를 위해 설계되었습니다. 베이글부터 해변 휴가까지 거의 모든 것을 구매하는 데 사용할 수 있습니다.

당신은 모바일 폰을 사용하여 지캐시로 친구에게 비공식적으로 결제하거나, 해외로 송금하거나, 식료품을 구매하거나, 기부할 수 있습니다. Flexa SPEDN과 같은 제3자 앱을 사용하여 Lowe’s, Nordstrom, Baskin Robbins 등에서 지캐시로 결제할 수 있습니다. Moon과 같은 서비스는 비자(Visa)가 사용 가능한 곳에서 온라인으로 지캐시를 사용할 수 있게 해줍니다.

5.1.1 비트코인이란 무엇입니까**?** 지캐시란 무엇입니까**?**

비트코인은 비트코인 네트워크를 통해 누구나 송금하고 수신할 수 있는 전자 현금의 형태입니다. 비트코인은 분산 원장 시스템에 연결된 디지털 지갑에 저장할 수 있으며, 이는 모바일 폰이나 데스크톱 컴퓨터에서 사용할 수 있습니다. 이를 모두가 접근할 수 있는 거대한 온라인 스프레드시트처럼 생각하면 됩니다. 이 스프레드시트에는 모든 거래가 기록됩니다.

비트코인과 마찬가지로 지캐시는 오픈 소스 블록체인 기반 원장에 기반한 디지털 통화이지만, 비트코인과는 달리 복잡한 영지식 증명(zero-knowledge proof) 시스템을 특징으로 하여 원장을 사기/해킹으로부터 보호하면서 사용자가 거래 정보를 비공개로 유지할 수 있도록 합니다.

5.1.2 비트코인과 지캐시의 차이점은 무엇입니까**?**

지캐시를 가장 간단하게 설명하면, 비트코인과 같은 디지털 화폐이지만, 사용자의 금융 내역을 노출하는 대신 개인 정보를 보호한다는 점에서 차이가 있습니다

비트코인은 2009년에 출시된 최초의 분산형 암호화폐였습니다. 모든 비트코인 거래는 공개된 블록체인(원장)에 검증되고 기록되기 때문에, 전 세계 누구나 사용자 잔액과 거래 데이터를 볼 수 있습니다. 이러한 프라이버시 부족이 지캐시 과학자들에게 더 나은 것을 만들도록 영감을 주었으며, 2016년에 이 암호학 전문가들은 비트코인의 오픈 소스 코드를 사용하고, 영지식 증명(및 기타 개선 사항)을 추가하여 지캐시를 개발했습니다. 지캐시는 비트코인의 모든 편리함을 제공하면서도 사용자의 금융 정보를 보호하기 위해 완전한 암호화를 제공합니다.

지캐시에는 자체 개발 자금 조달 메커니즘, 더 짧은 확인 시간, 비공개 메모 필드, 더 빠른 거래 속도 등과 같은 다른 중요한 차이점들도 있습니다.

5.1.3 지캐시에 대해 왜 배워야 합니까**?**

지캐시는 사람들이 은행이나 정부 기관과 같은 중개자 없이 디지털 현금과 기타 데이터를 비공개로, 그리고 허가 없이 전송할 수 있는 기회를 제공합니다. 비공개 P2P (peer-to-peer) 허가 없는 금융 시스템을 통해 사람들은 중앙화된 기관의 통제나 수수료 없이 돈을 보관하고 다른 사람과 거래할 수 있습니다. 지캐시는 사람들이 자신의 재정 정보를 타인에게 공개할지 여부와 시기를 스스로 결정할 수 있는 자유를 제공합니다.

지캐시는 비트코인의 가장 큰 결점인 데이터의 개인 소유와 전송 문제를 해결합니다. 블록체인 응용 프로그램과 암호화폐가 점점 더 널리 받아들여지는 세상에서, 비트코인과 같은 가명 거래는 더 이상 사용자 프라이버시를 보호하기 위한 실효성 있는 선택이 아닙니다. 감시 기술은 나날이 더 정교해지고 있으며, 사람들이나 기관들이 블록체인 거래를 분석하고 추적하는 데 널리 사용되고 있습니다.

5.1.4 지캐시의 가치는 무엇에서 비롯됩니까**?**

지캐시는 2016년 말 처음 네트워크가 출시된 이후로 큰 발전을 이루었으며, 블록체인과 암호화폐 사용자들에게 계속해서 개인정보 보호에 대한 통제권을 제공합니다. Zk-SNARK 암호학적 증명은 글로벌 시장에서 블록체인 기반 사용 사례에 대한 프라이버시 표준을 설정하는 데 기여했습니다. 다양한 사용자와 기업 고객 모두가 지캐시 프로토콜이 제공하는 프라이버시, 유연성, 성능을 요구하고 있습니다.

5.1.5 왜 지캐시를 신경 써야 합니까**?**

지캐시는 사람들이 검열하거나 착취할 수 있는 중앙화된 시스템 밖에서 거래할 선택권을 제공하며, 자신의 재정 정보를 타인에게 공개하거나 그 정보를 비공개로 유지할 수 있는 권한을 줍니다.

이 검열 저항형 디지털 결제 메커니즘은 언론의 자유와 결사의 자유, 그리고 인간으로서의 자유, 사용자는 어리석게 굴거나 원하는 어떤 모습이든 될 수 있는 자유를 보호합니다**!** 지캐시 사용자들은 자신의 정체성을 노출하지 않고 보복에 대한 두려움 없이 단체에 기부하거나, 해외로 돈을 보내거나, 친구에게 돈을 보낼 수 있습니다.

그리고 지캐시는 비트코인과 마찬가지로 2,100만 개의 한정된 공급량을 가지고 있기 때문에, 중앙기관의 화폐 찍어 내기와 같은 행위로 인한 가치가 하락은 없을 것이라는 확신을 가질 수 있습니다.

5.2 지캐시는 어떻게 구성되어 있습니까**?**

지캐시는 사용자에게 두 가지 거래 유형을 선택할 수 있는 옵션을 제공합니다: 투명한 거래(누구나 볼 수 있음)와 보호된 거래(비공개). 두 거래 모두 동일한 지캐시 블록체인에서 실행되지만, 거래의 금액과 증명 방식은 다르게 처리됩니다. 보호된 거래를 비공개로 유지하기 위해 지캐시는 영지식 증명 기술을 활용합니다.

구체적으로, 지캐시는 zk-SNARKs라는 영지식 증명 방식을 사용합니다. zk-SNARKs는 "Zero-Knowledge Succinct Non-Interactive Argument of Knowledge"의 약자로, 이는 비밀 키와 같은 특정 정보를 드러내지 않고 해당 정보를 소유하고 있음을 증명할 수 있는 증명 구조를 의미합니다. 이 과정에서 증명자와 검증자 간의 상호작용이 전혀 없이 이루어집니다.

더 간단히 말하면, 영지식 증명은 어떤 정보가 참임을 그 정보를 공개하지 않고도 증명할 수 있는 암호학적 방법입니다. 예를 들어, 지캐시에서 두 당사자 간에 거래가 이루어질 때, 영지식 증명은 송신자가 발송 금액을 충당할 만큼 충분한 돈을 지갑에 가지고 있음을 증명하는 데 사용되지만, 수신자, 블록체인 또는 다른 누구에게도 송신자의 지갑 잔액을 공개하지 않습니다.

한번 상상해 보세요. 당신은 눈가리개를 하고 두 개의 체커 말을 등 뒤로 들고 있습니다. 그들이 같은 색인지, 다른 색인지는 알 수 없습니다. 당신은 하나를 꺼내 상대방에게 보여줍니다. 상대방은 눈가리개를 하지 않았기 때문에 그 색을 알려줍니다. 하지만 상대방이 거짓말을 하는지 아닌지 알 수 없습니다. 그러고 나서 그 말을 다시 등 뒤로 가져가고, 말을 바꾸거나 그대로 두고 과정을 반복합니다. 이렇게 여러 번 반복하면 상대방이 거짓말을 하고 있는지에 대해 점점 확신을 가질 수 있습니다. 예를 들어, 같은 말을 두 번 내놓았는데 상대방이 처음에는 "검정"이라고 하고 두번째에는 "빨강"이라고 말하면, 상대방이 거짓말을 하고 있다는 것을 알 수 있습니다. 상대방의 답이 당신이 내놓은 말을 알고 있는 정보와 일치한다면, 상대방이 정직한 정보를 주고 있는지에 대해 꽤 확신을 가질 수 있게 됩니다.

이러한 과정은 무한한 복잡성을 가진 방대한 양의 정보를 보호하는 데 사용될 수 있습니다(예를 들어, 재귀적 SNARKs를 사용하여 블록체인의 글로벌 상태의 Merkle root를 저장하는 것 등; 하지만 이는 이 책의 범위를 벗어납니다).

5.2.1 새로운 지캐시 코인은 어떻게 네트워크에 진입합니까**?**

지캐시의 화폐 공급량은 2,100만 ZEC로 고정되어 있습니다. 75초마다 새로운 블록이 지캐시 블록체인에 채굴되며, 3.125 ZEC의 블록 보상이 유통에 들어갑니다. 이 블록 보상은 채굴자들과 지캐시 개발 기금에 분배됩니다.

블록 보상의 양은 약 4년마다 절반으로 줄어들며, 2,100만 ZEC가 모두 유통될 때까지 이 과정이 계속됩니다. 지캐시의 인플레이션은 비트코인의 인플레이션을 거의 정확하게 모방하고 있습니다. 중요한 점은 새로운 코인이 생성됨에 따라 인플레이션이 감소하며, 각 반감기마다 그 비율이 크게 떨어진다는 것입니다.

5.2.2 지캐시 프라이버시 소개

보호된 지캐시 주소는 사용자의 재정 정보를 비공개로 유지합니다. 반면에, 투명한 주소는 해당 정보를 공개합니다.

대부분의 블록체인은 모든 거래 및 잔액 정보를 공개합니다. 이는 부끄러운 비밀이 아니라 단지 그들이 설계된 방식입니다. 보호된 지캐시로 자산을 저장하고 거래하면 사용자에게 자산에 대한 더 많은 통제력을 제공하며, 사기꾼이나 다른 악의적인 행위자로부터 보호할 수 있습니다.

지캐시를 디지털 지갑에서 전송할 때, 귀하의 주소는 긴 숫자와 문자로 이루어진 문자열로 나타납니다. 수신자도 마찬가지로 긴 숫자와 문자로 구성된 주소를 가지고 있습니다. 만약 귀하의 주소가 "z"로 시작하고, 수신자의 주소도 "z"로 시작한다면, 거래 정보가 완전히 비공개임을 확신할 수 있습니다. 거래 금액과 각 지갑의 주소는 모두 공공 블록체인에서 보호됩니다. 이는 개인 정보 보호가 필요한 경우 ZEC를 송금하고 수신하는 가장 좋은 방법입니다.

"t"로 시작하는 주소로 송금하거나 수신하는 경우, 즉 z-to-t 또는 t-to-z 거래의 경우, 개인 정보 보호 수준이 항상 높지 않습니다. 블록체인에서 일부 정보가 공개되기 때문입니다. t-to-t 거래는 비트코인 거래와 마찬가지로 완전히 공개됩니다.

지캐시 사용자들은 "u"로 시작하는 지갑 주소도 접할 수 있습니다. 이러한 주소는 통합 주소(unified addresses)라고 하며, 이는 보편적인 여행 어댑터와 같은 역할을 합니다. 통합 주소를 사용하면 지갑이 자동으로 코인을 최신 보호된 풀로 이동할 수 있습니다. 예를 들어, 사용자가 거래소에서 지캐시를 구매한다고 가정해 보겠습니다. 그 거래소는 t-주소에서 귀하의 통합 주소로 투명한 지캐시를 보낼 수 있습니다. 그러나 귀하의 지갑이 자동 보호 기능을 지원한다면, 해당 자금은 자동으로 비공식 저장소로 이동됩니다.

지캐시 주소의 유형

현재 사용되는 주요 주소 유형은 세 가지가 있습니다. 이들은 다음과 같습니다:

최대의 개인 정보 보호를 위해 항상 Z- 또는 U-주소를 사용하세요.

5.2.3 블록체인은 누가 어떤 지캐시를 사용하는지 어떻게 추적합니까**?**

해시 트리 또는 머클 트리는 데이터 블록의 암호화 해시로 레이블이 붙은 가지와 리프 노드로 구성됩니다. 머클 트리는 암호화 커밋먼트 스킴의 한 예입니다. 트리의 루트는 커밋먼트로 간주되며, 리프 노드는 원래 커밋먼트의 일부임을 증명합니다.

그들은 P2P 네트워크에서 저장되거나 전송된 데이터를 검증하여 피어로부터 받은 데이터가 변경되지 않았음을 보장합니다. 지캐시의 Sapling 및 Orchard 보호 풀에서는 노트 커밋먼트 트리(Note Commitment Tree)가 사용되어 거래가 합의에 대해 유효한지를 검증하면서 송신자, 수신자 및 소비된 금액을 완벽하게 숨깁니다.

5.2.4 지캐시 거래는 안전합니까?

네, 지캐시 프로토콜은 세계에서 가장 철저하게 문서화된 영지식 결제 프로토콜 중 하나로, 매우 안전하다고 간주될 수 있습니다. 이 프로토콜은 Namada 및 Penumbra와 같은 여러 대형 암호화 프로젝트에 사용되었습니다. 또한, 지캐시 사용자들이 사용하는 제품의 지갑 및 암호화 구성 요소에 대한 많은 보안 감사가 진행되었습니다.

5.2.5 실제 지캐시 거래 과정을 설명해 주십시오**.**

> 지갑이 최신 블록 높이에 동기화되었는지 확인합니다.

> 완전히 동기화된 경우, 귀하의 잔액이 전액 사용할 수 있는 금액과 일치함을 확신할 수 있습니다.

> 수신자의 통합 주소를 “주소” 필드에 입력합니다. 주소를 클립보드에서 붙여넣거나 상대방의 QR 코드를 스캔합니다.

> 보낼 금액을 입력합니다; 수수료는 자동으로 계산됩니다.

> 거래와 함께 보호된 메모를 입력합니다. 주의: 투명한 주소는 메모를 받을 수 없습니다.

> 거래 세부 정보를 확인한 후 전송을 클릭합니다.

지캐시의 블록 생성 시간은 75초이며, 수신자가 들어오는 자금을 통지받는데 1-2분이 걸릴 수 있습니다. 수신자의 지갑에서 요구하는 확인 수에 따라, 좀 더 기다려야 할 수 있습니다.

5.2.6 연습**:** 지캐시 거래 실습

지캐시를 친구와 교환해 보려면 다음 단계를 따르세요:

1) 두 사람 모두 지캐시 지갑을 설정합니다.

2) "보내기" 옵션에서 친구의 주소 QR 코드를 스캔하거나 그들의 U 또는 Z 주소를 입력합니다.

3) 메모를 보내며: "안녕하세요, 지캐시에 오신 것을 환영합니다!"라고 입력합니다.

5.2.7 지캐시는 중단될 수 있습니까**?**

아니요. 지캐시는 전 세계의 개인들이 운영하는 허가 없는 분산 인터넷 결제 프로토콜입니다. 노드 소프트웨어는 무료이며 오픈 소스입니다. 지캐시 거래의 검증에 중앙 권한이 개입되지 않습니다. 사실, 지캐시의 향상된 개인 정보 보호 기능 덕분에 네트워크를 중단하려는 시도에 대해 더욱 저항력이 있습니다.

5.3 지캐시 세계에는 누가 있습니까**?**

지캐시에서 활동하는 많은 팀과 독립 개발자들이 있지만, 주요 키플레이어들을 소개합니다.

Electric Coin Co. (ECC)는 2016년에 지캐시 디지털 통화를 생성하고 출시했습니다. 현재 ECC는 다른 독립 팀 및 개발자들과 함께 제품 개발, 인식 및 채택, 다양한 연구를 통해 지캐시 커뮤니티를 지속적으로 지원하고 있습니다. ECC는 세계에서 가장 강력한 암호화 팀 중 하나로 널리 알려져 있습니다. 2016년에는 영지식 암호화 기술을 실제 애플리케이션(지캐시)에 성공적으로 처음으로 배포했으며, 2022년에는 ECC 엔지니어들이 Halo를 발견했습니다. Halo는 최초로 진정한 신뢰 없는 블록체인 암호화와 향상된 확장성을 제공하는 혁신적인 재귀적 영지식 증명 메커니즘입니다. 현재 수십 개의 팀이 Halo를 자신의 프로젝트에 구현하기 위해 다양한 독립 프로젝트를 진행하고 있습니다.

The Zcash Foundation (ZF)은 501(c)(3) 공익 자선 단체로, 주로 지캐시 프로토콜 및 블록체인 사용자들을 위해 공공의 이익을 위한 금융 프라이버시 인프라를 구축합니다. ZF는 다른 팀들과 함께 지캐시 프로토콜과 이를 지원하는 열린 네트워크가 분산되고 다양성을 유지하도록 노력합니다. ZF의 생태계에 대한 몇 가지 주목할 만한 기술 기여로는 현대적이고 독립적인 지캐시 노드인 Zebra의 개발과 임계값 서명 체계인 FROST가 있습니다. 재단은 또한 프라이버시 기술과 지캐시 생태계를 중심으로 한 연례 컨퍼런스인 Zcon을 개최하며, Zcon Vozes, A/V 클럽 및 다양한 기타 열린 커뮤니티 전화 회의와 AMA와 같은 풀뿌리 커뮤니티 이니셔티브를 지원합니다. 또한 재단은 Minor Grants 프로그램, 내부 및 외부 연구 프로젝트에 자금을 지원하고, 지캐시 커뮤니티 보조금(ZCG)에 대한 행정 지원을 제공함으로써 지캐시 발전을 도모합니다.

Zcash Community Grants (ZCG)은 지캐시의 사용성, 보안, 프라이버시 및 채택을 촉진하는 프로젝트에 자금을 지원합니다. ZCG는 지캐시 재단의 규약에 따라 구성된 기술 자문 위원회입니다. 보조금은 지캐시 커뮤니티 자문 패널에 의해 선출된 5명의 위원으로 구성된 위원회에 의해 선정됩니다.

ZCG에 의해 승인된 최근 프로젝트는 다음과 같습니다:

Zcash Shielded Assets (ZSA): QEDIT 팀이 주도하여 지캐시에 DeFi를 도입하는 새로운 결제 프로토콜로, 메인넷에 추가 기능을 제공합니다.

Zcash Media의 단편 다큐멘터리**:** Edward Snowden, Zooko Wilcox, Deirdre Connolly와 같은 주목할 만한 지캐시 사용자들이 출연하는 다큐멘터리입니다.

오프라인 상점을 위한 원클릭 보호 결제 및 **Point-of-sale** 시스템**:** ZGo에서 진행 중인 프로젝트입니다.

글로벌 앰버서더 프로그램: 지캐시의 국제적 대표성을 넓히는 데 도움을 줍니다.

ZecHub: 지캐시 중심의 오픈 소스 교육 허브로, 글로벌 기여자 커뮤니티가 기능, 뉴스레터, 블로그, 튜토리얼, 팟캐스트 등을 게시합니다.