작성자:
Matt Kunke
리서치 애널리스트

날짜: 2021년 11월 10일
주제: 디지털 자산

Global X ETFs 리서치

비트코인의 기초

2008년 10월, 혁명적인 통화 개념의 가능성을 홍보하는 생소한 백서가 암호작성술 메일링 리스트에 발송되었습니다. 잘 정돈된 아홉 쪽짜리 백서에서 사토시 나카모토(Satoshi Nakamoto)란 필명을 가진 어떤 개인, 어쩌면 단체가 세계 최초로 분산된 피어투피어(P2P) 화폐 시스템을 소개하였습니다. 인터넷에 연결된 사람은 누구나 이용할 수 있으며, 완전히 공개된 시스템 참가자는 신뢰할 수 있는 중개 기관 없이도 언제든지 전 세계적으로 가치를 교환할 수 있다고 이 백서는 주장했습니다.

몇 달 후인 2009년 1월, 비트코인 소프트웨어의 첫 번째 버전으로 이 보고서에서 대문자 'B'로 설명된 비트코인 네트워크가 탄생하였습니다. 이 네트워크는 블록체인 기술의 첫 적용 사례로서, 거래를 기록하고 자산을 추적하는 데 완전히 투명하고 거래를 공유하며 지속적으로 대사하여 배포하는 원장이었습니다. 또한 네트워크의 시작과 함께 비트코인 디지털 화폐가 만들어졌습니다. 보고서에서 소문자 'b'로 설명된 비트코인은 분할 가능하고 대체 가능하며 쉽게 이전할 수 있고 프로그램으로 정의된 통화 정책에 의해 희소성이 보장된 디지털 화폐입니다.

비트코인의 발전: 소규모에서 메인스트림으로

비트코인은 적절한 시점에 만들어졌습니다. 비트코인은 많은 개인들이 자신의 돈을 보관하던 대형 은행과 통화 정책을 결정하는 정부에 대한 신뢰를 잃어버렸던 글로벌 금융위기의 정점에 시작되었습니다. 비트코인은 중앙집권식 기관이 조정하거나 통제할 수 없는 새로운 형태의 '경화'입니다. 전 세계의 정부가 대규모 양적 완화 프로그램을 시행하여 명목화폐의 공급을 늘렸기 때문에 이러한 특징과 비트코인의 희소성이 금융위기 후유증 속에서 반향을 일으켰습니다.

비트코인 가격(대수 척도)

출처: Blockchain.com. 2021 년 10 월 21 일

비트코인, 주요 구성요소 및 작동 방법에 관해 알아야 할 것

비트코인의 성장 상황과 잠재적 투자 영향을 논의하기 위하여 본 보고서에서는 비트코인과 작동 방법에 관한 기초 질문에 답하고자 합니다.

- **비트코인이란 무엇인가?** 이전이 더 용이한 디지털 버전의 금입니다.
- **비트코인 네트워크란 무엇인가?** 완전히 공개되어 있고 허가가 필요 없으며 신뢰 확인 과정이 최소화된 첫 금융 생태계입니다.
- **노드란 무엇인가?** 비트코인의 소프트웨어를 구동하고 네트워크의 안전성 확보를 지원하는 컴퓨터를 말합니다.
- **채굴은 어떻게 이루어지나?** 특수한 노드가 수학적 퍼즐을 풀어 체인의 다음 블록을 생성합니다.
- **왜 메인 블록체인이 중요한가?** 메인 블록체인이 네크워크 대기 시간 때문에 발생하는 문제점들을 해결하기 때문입니다.
- **언제 거래가 진정으로 성사되는가?** 거래가 충분한 수의 확인을 거칠 때 성사됩니다.

또한 본 보고서에서는 아래의 세 가지 광의의 질문에 초점을 맞추어 경제 환경 속에서의 비트코인 포지셔닝에 대해 논의하려고 합니다.

- **비트코인이 제공하는 것은 무엇인가?** 독립적인 원천의 신뢰 및 금융 시스템에 대한 접근성.
- **비트코인에 대한 규제 환경을 어떻게 보아야 하는가?** 진화하는 과정의 일부분.
- **왜 지금 비트코인인가?** 이러한 경제적 시기를 위해 구축된 자산이기 때문입니다.

비트코인: 이전이 더 용이한 디지털 버전의 금

통화로서 비트코인은 단일 집단이 통제하거나 변경할 수 없는 형태의 화폐이며 그 가치에 대해 합의한 사용자들이 형성한 네트워크 내에서 공급이 한정된 자산입니다. 블록체인 기술을 처음 적용한 사례인 비트코인은 비트코인 블록체인 원장에 잔액 형식으로 존재합니다. 정부가 보증하는 전통적인 명목화폐와 달리 비트코인은 실물 지폐나 동전이 없습니다.

비트코인 사용자는 계좌의 비밀번호에 해당하는 프라이빗 키를 가지고 있습니다. 또한 사용자는 퍼블릭 키와 주소를 가지며 둘 모두 암호작성술을 통해 프라이빗 키로부터 생성되며 이와 연결되어 있습니다. 중요한 점은 퍼블릭 키 또는 주소로부터 프라이빗 키를 알아낼 수 없다는 사실입니다. 사용자의 주소는 비트코인 거래의 목적지를 식별하는 데 사용되는 퍼블릭 사용자 이름과 기능이 유사합니다. 본질적으로 비트코인을 사용하려면 사용자는 퍼블릭 키와 연계된 프라이빗 키와 비트코인이 보관된 주소가 필요합니다. 사용자가 비트코인을 받으려면 간단히 지급인에게 비트코인 주소를 제공하면 됩니다.

퍼블릭 키 및 주소 도출

출처: Global X ETFs, 비트코인 마스터 하기: 오픈 블록체인 프로그래밍.

프라이빗 키를 공공연하게 보여주는 것은 문제가 될 수 있습니다. 비트코인은 무기명 디지털 자산입니다. 즉, 프라이빗 키를 가지고 있으면 어느 개인이든 비트코인을 사용할 수 있습니다. 따라서 프라이빗 키를 보여주면 이를 본 어느 누구든 연관된 주소에서 비트코인을 훔칠 수 있다는 것입니다. 비트코인을 사용할 때에는 실제 프라이빗 키가 네트워크에 노출되지 않습니다. 비트코인 사용에는 서명자가 프라이빗 키를 소유하고 있다는 점을 암호를 통해 검증하는 디지털 서명이 표시됩니다.

디지털 서명은 사용자의 프라이빗 키와 제안한 거래 정보로부터 도출됩니다. 퍼블릭 키와 주소를 프라이빗 키로부터 얻기 때문에 고급 수학을 통해 디지털 서명을 만든 프라이빗 키가 퍼블릭 키를 만드는 데 사용된 프라이빗 키와 같은지 여부를 검증할 수 있습니다. 암호 관계를 통해 디지털 서명은 네트워크에서 비트코인 소유권을 독립적으로 검증할 수 있으므로 비트코인 사용자는 자신의 비트코인을 자유롭게 사용할 수 있으며, 악의를 가진 다른 사람은 비트코인을 사용할 수 없습니다.

비트코인 네트워크: 진정으로 공개되어 있고, 허가가 필요 없으며, 신뢰성이 최소화된 첫 금융 생태계

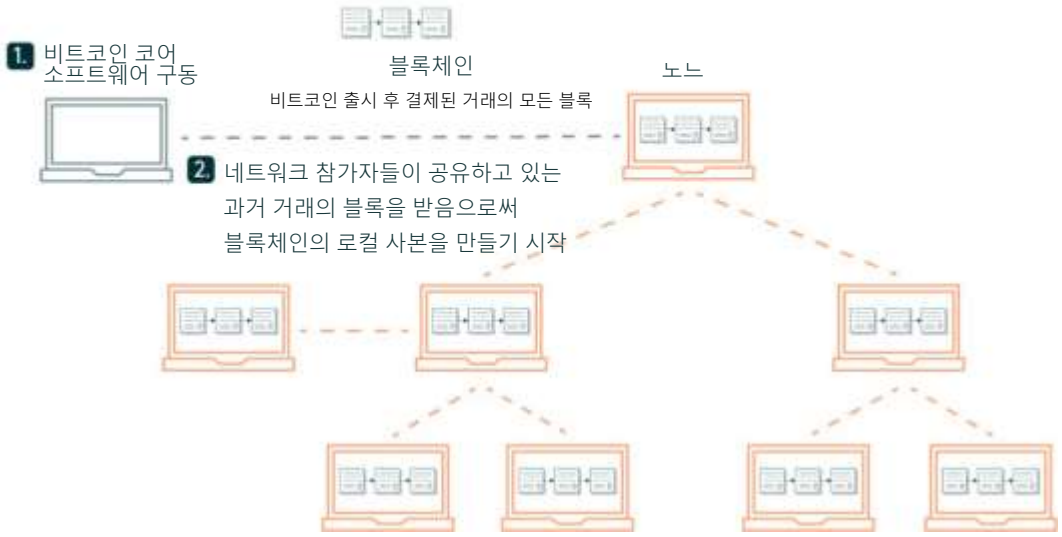
비트코인 네트워크를 통해 금융기관과 같은 중개인 없이도 피어투피어 방식으로 비트코인을 이전할 수 있습니다. 네트워크는 거래 기록과 비트코인 추적을 용이하게 하기 위하여 완전히 투명한 블록체인 기술을 활용합니다. 네트워크 참가자는 프로토콜 규칙을 준수하고 독립적으로 거래와 블록을 규칙과 비교 검증함으로써 블록체인의 분산 원장에 동의하여 합의에 이를 수 있습니다.

네트워크는 참가 여부가 완전 자율적으로 모든 것을 아우르는 소프트웨어 패키지인 비트코인 코어를 사용합니다. 한 컴퓨터가 소프트웨어를 구동하면 네트워크에 있는 노드라 불리는 다른 컴퓨터에 연결됩니다.

그러면 해당 컴퓨터는 네트워크가 만들어진 이후 발생한 거래의 모든 블록을 받기 시작합니다. 해당 컴퓨터는 비트코인 블록체인, 다시 말해 거래에 관한 분산 데이터베이스의 완전한 자체 복사본을 만들 수 있습니다. 비트코인 코어는 내부에 지갑 애플리케이션이 구축되어 있어 참가자들은 소프트웨어를 통하여 직접 비트코인을 거래할 수 있습니다. 지갑은 두 개의 키를 관리하고 비트코인 잔고를 추적하며 비트코인을 사용하기 위한 디지털 서명을 만들어 줍니다.

비트코인 코어 소프트웨어를 구동하는 컴퓨터 노드의 네트워크

출처: Global X ETFs.



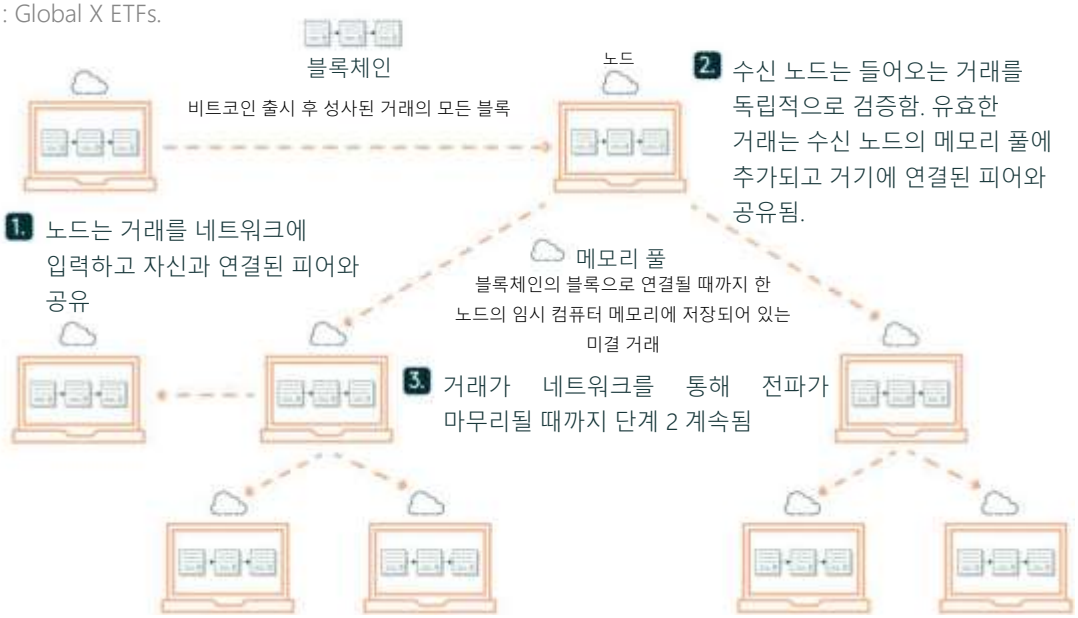
노드: 비트코인 코어를 구동하고 네트워크의 안정성 확보를 지원하는 컴퓨터

자신의 블록체인 사본을 만든 후, 노드는 실시간으로 일어나는 새로운 거래와 블록 정보를 피어로부터 공유 받아 체인의 최신 사본을 유지합니다. 노드는 모든 거래와 블록을 프로토콜 규칙과 독립적으로 검증함으로써 네트워크의 안정성 확보를 지원하고 유효한 거래와 블록만을 연결된 피어에게 보냅니다. 각 노드는 지속적으로 메모리 풀이라 알려진 유효하지만 아직 성사되지 않은 거래의 풀을 업데이트합니다.

노드가 연결된 피어들 중 하나로부터 새로운 거래를 받으면, 소프트웨어는 독립적으로 이 거래의 유효성을 디지털 서명의 평가를 포함하여 종합적인 일련의 기준과 검증합니다. 거래가 유효한 경우, 수신 노드는 임시 컴퓨터 메모리에 해당 거래를 저장하고 수신 노드에 연결된 나머지 노드에 보냅니다. 그 후에는 거래와 연관된 다른 피어가 이 거래를 받아서 검증한 다음 연결된 피어에 보내는 이러한 사이클이 반복됩니다. 이러한 사이클은 정보가 어떻게 피어투피어 방식으로 네트워크를 통하여 이동하는지 보여줍니다.

비트코인 네트워크를 통한 거래 전파

출처: Global X ETFs.



채굴 노드: 수학적 퍼즐을 풀어 다음 블록을 생성하는 특수 노드

모든 비트코인 노드가 거래를 독립적으로 검증하지만 채굴 노드는 블록 생성 목적으로 블록체인에 기록된 블록으로 거래를 취합하는 특수한 형태의 노드입니다. 채굴 노드는 체인에서 블록을 생성하기 때문에 다른 노드와 구별됩니다. 블록은 성사된 거래들이 쌓여있는 층으로 생각할 수 있습니다. 거래는 계속하여 노드 간 전달되고 임시 메모리에 저장됩니다. 임시 메모리의 거래는 채굴자가 해당 거래를 블록으로 블록체인에 포함시킬 때까지 기본적으로 미결 거래입니다.

채굴 노드는 어려운 수학적 퍼즐을 제일 먼저 풀기 위한 경쟁에 대량의 연산 자원을 배정합니다. 퍼즐 솔루션을 작업증명(Proof-of-Work)이라고도 부릅니다. 퍼즐은 채굴자들이 희귀한 산출값 또는 해시를 찾는 암호화 해시 함수를 통해 상이한 입력값을 반복하여 입력하는 무작위 연산을 통해 풀립니다. 작업증명은 찾기가 어렵지만 어떤 노드이든 채굴자가 해답을 찾기 위해 연산 자원을 사용했다는 점을 쉽게 검증할 수 있습니다. 거래에 유효한 디지털 서명이 있어야만 해당 거래가 유효한 것으로 간주되는 것과 마찬가지로 후보 블록이 유효한 블록이 되기 위해서는 작업증명이 필요합니다.

채굴자는 이 퍼즐을 제일 먼저 풀도록 재정적인 인센티브를 받습니다. 유효한 작업증명과 함께 새로운 블록을 먼저 보내는 채굴자는 블록 리워드와 그 블록 내의 모든 거래 수수료를 청구할 수 있습니다. 블록 리워드는 채굴자가 새로 생성한 비트코인의 일정 수량을 자신에게 보내도록 허용하는 특수한 거래입니다. 이러한 과정은 블록 리워드가 처음으로 생성되어 새로운 비트코인으로 인정받기 때문에 지하에서 새로운 금을 채굴하는 과정과 유사하여 채굴이라 부릅니다.

현재 블록 리워드는 6.25 비트코인으로 이는 현재 40만 달러 이상에 해당합니다.[2] 하지만, 블록 리워드는 21만 블록마다 또는 약 4년마다 50%가 감소하여 2140년경에는 블록 리워드가 사라질 것입니다. 이러한 반감 이벤트는 비트코인의 디스인플레이션 통화 정책으로 작동합니다. 다음 반감 이벤트는 2024년에 있을 것으로 예상되며 비트코인 블록 리워드를 블록당 3.125 비트코인으로 감소시킬 것입니다.

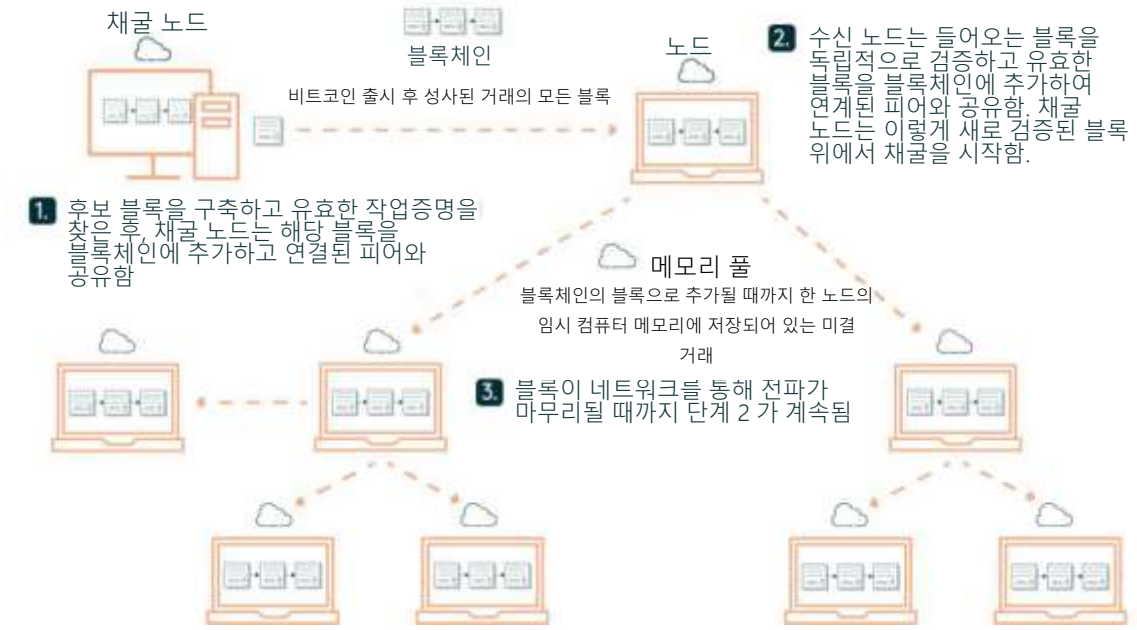
네트워크 시간

또한 사용자는 비트코인 네트워크에서 거래할 때 일반적으로 소액의 거래 수수료를 채굴자에게 지급하여 거래가 성사되어 블록에 포함되도록 인센티브를 제공합니다. 네트워크에서 수요가 많은 기간에는 비트코인 사용자들이 거래를 성사시키기 위해 입찰하기 때문에 거래 수수료가 상당히 증가할 수 있습니다. 예를 들어, 2021년 9월 평균 거래 수수료는 겨우 2.50달러였지만 비트코인이 처음으로 6만 달러를 돌파하고 네트워크가 혼잡하였던 2021년 4월에는 10일 이상의 기간 동안 약 20~65달러였습니다.[3] 일반적으로 블록에는 1,500~2,500 건의 거래가 포함되므로 블록을 해결하는 데 따른 채굴자의 총 보상에서 거래 수수료가 차지하는 비중은 작은 것이 일반적입니다.

한 채굴자가 블록을 해결하고 나면 채굴자들은 네트워크를 통해 해당 블록을 전송합니다. 각 노드는 새로 받은 블록의 유효성을 검증한 다음 자신이 가지고 있는 블록체인의 사본에 추가합니다. 새로운 유효 블록을 받으면 채굴 게임이 다시 시작됩니다. 모든 채굴자는 새로운 후보 블록을 만들고 새로 받은 블록에 연계된 퍼즐을 먼저 풀려고 노력합니다.

비트코인 네트워크를 통한 블록 전파

출처: Global X ETFs.



비트코인 코어 소프트웨어는 이러한 채굴 퍼즐이 평균 10분마다 한번 풀리도록 설계되었습니다. 소프트웨어는 더 많은(더 적은) 해시레이트가 퍼즐을 풀려고 노력하면 이를 더(덜) 어렵게 만들기 위해 약 2주에 한번 퍼즐의 난이도를 조정합니다. 그렇기 때문에 귀금속 채굴과 달리 비트코인의 채굴 속도는 빨라질 수 없습니다. 달리 말하면, 비트코인의 공급은 한정되어 있으며 비트코인에 대한 수요와 무관합니다. 채굴 장비를 늘리기 위해 투자를 늘리면 퍼즐이 그에 비례하여 풀기가 더 어려워지므로 비트코인의 발행율은 일정하게 유지됩니다.

메인 블록체인: 네크워크 대기 시간 때문에 발생하는 문제점들 해결

발생할 수 있는 한 가지 문제점은 두 채굴자가 거의 같은 시간에 작업증명을 풀고 유효한 블록을 보내는 경우입니다. 정보가 피어에서 피어로 흐르도록 하는 글로벌 네트워크의 속성을 고려할 때, 네트워크의 대기 시간 때문에 불가피하게 상이한 노드는 정보를 약간 다른 시간에 받게 됩니다. 이러한 문제는 프로토콜을 통해 각 노드가 가장 긴 체인, 즉 메인 블록체인 또는 좀 더 정확히 말하자면 가장 많은 작업을 한 체인을 식별하도록 하여 해결합니다. 예를 들어, 채굴자 A와 채굴자 B가 거의 같은 시간에 유효한 블록을 생산한 경우 채굴자 C는 채굴자 A의 블록을 맨 먼저 받을 수 있고 채굴자 D는 채굴자 B의 블록을 맨 먼저 받을 수 있습니다.

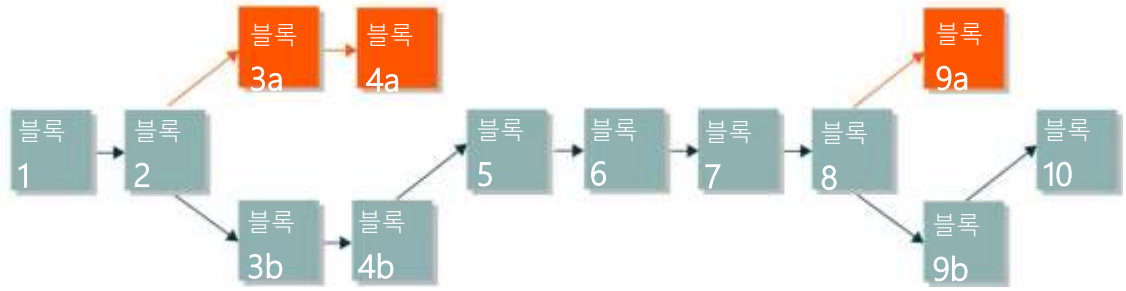
이러한 시나리오는 블록체인에서 임시 포크라 불리는 상황을 만들게 됩니다. 즉, 양 블록체인 모두 잠정적으로 유효하고, 체인 중 하나에 추가되는 후속 블록을 나중에 고려한 다음에야 메인 체인을 식별할

수 있게 됩니다. 그러나 이 시나리오는 채굴자가 후속 블록을 생성할 체인을 선택함에 따라 빠르게 해결됩니다. 기본적으로 채굴자는 자신이 받은 첫 번째 유효 블록을 사용합니다. 따라서 채굴자 A와 채굴자 C는 한 블록체인에서 채굴하고, 채굴자 B와 채굴자 D는 다른 블록체인에서 채굴합니다.

더 많은 블록이 생성됨에 따라 나누어진 체인의 양측이 계속해서 동시에 작업증명을 풀 가능성은 0에 가까워 집니다. 한 쪽이 다른 한 쪽보다 일찍 다음 블록을 찾는 즉시, 이 블록을 생성했던 체인은 메인 블록체인으로 간주되고 다른 체인 상대방은 프로토콜 규칙에 따라 포기하게 됩니다. 이러한 프로토콜 규칙을 통해 노드에서는 블록체인의 상태와 발생한 거래에 대한 합의와 동의가 이루어 집니다. 아래 예시의 오렌지색 블록은 유효하지만 후에 전체적으로 보면 파란색으로 표시된 메인 블록의 일부가 아닙니다.

블록체인에서의 임시 포크

출처: Global X ETFs.



진정한 거래 성사 및 불역성: 거래에 충분한 수의 확인이 있을 때.

흔히 거래는 블록에 포함될 때 성사되었다고 말합니다. 그러나 일부 상황에서는 블록체인이 임시로 포크 상태로 남은 다음 얼마 후 재조직되므로 거래가 진정으로 성사되고 거래의 불역성을 확보하려면 일부 조건이 충족되어야 합니다.

충분한 수의 확인을 받은 후에야, 즉 체인에 특정한 거래를 포함하고 있는 블록 외에 블록들이 추가되어야만, 진정한 거래 성사와 불역성이 확보됩니다. 사후적으로 여섯 번의 확인을 거친 블록이 일반적으로 불역성 또는 불가변성이 있는 것으로 간주됩니다. 거래 규모가 작은 경우에는 통상 한 번에서 세 번의 확인을 거치면 안전한 것으로 간주됩니다. 블록들이 이전 블록의 해시를 참조하여 새로 채굴된 각각의 블록과 연결되어 있기 때문에 아래에 묻혀 있는 블록의 수가 증가할수록 거래가 더 안전하고 변경이 불가능해집니다.

예를 들어, 여섯 번의 확인을 거친 거래를 뒤집으려 하는 악의적인 사람은 여섯 블록을 뒤로 돌아가야 조작하려 하는 거래가 포함된 블록에 갈 수 있을 것입니다. 그런 다음 해당 블록과 포크 체인에 있는 다섯 개의 후속 블록을 다시 채굴하고 이러한 여섯 블록 각각에 대하여 유효한 작업증명을 찾아야 합니다. 그와 동시에 프로토콜 규칙을 따르는 모든 선량한 사람들은 예전에 정의된 메인 블록을 채굴하고 확대할 것입니다. 메인 블록 대비 여섯 블록의 하자를 극복하려면 악의적인 사람은 상당히 오래 동안 총 네트워크의 연산 처리능력의 50% 이상을 통제할 필요가 있을 것입니다.

비트코인이 제공하는 것: 독립적인 접속 원천 및 신뢰

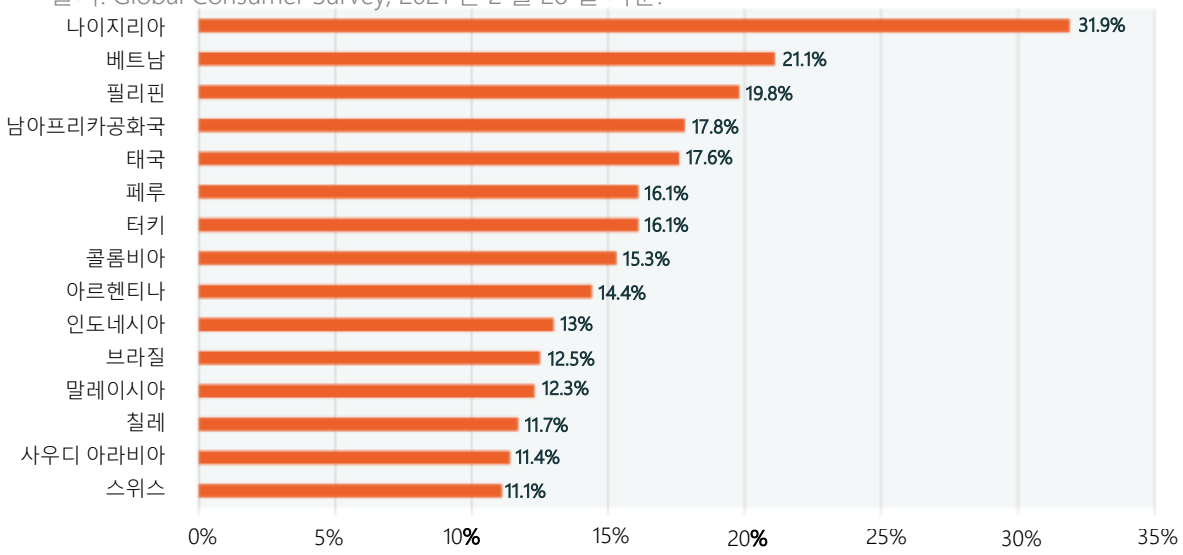
비트코인 네트워크는 정부가 통화를 보증하거나 화폐 공급을 책임감 있게 관리하는지에 대해 참가자가 신뢰할 필요가 없는 금융 생태계입니다. 선진국의 경우, 이러한 특징의 중요성을 이해하기가 특히 어렵겠지만 최근의 경제 위기가 이해를 도울 수 있습니다. 투자자를 보호하는 강력한 규제 체계 안에서

작동하는 신뢰 받는 금융기관의 혜택은 전 세계에서 동등하게 누릴 수 없습니다. 특히 신흥 경제에서는 더욱 그러합니다.

비트코인 네트워크는 특히 정치적 불안, 부패 또는 심한 인플레이션과 씨름하고 있는 국가에서 은행 서비스를 아예 못 받거나 충분히 받지 못하는 사람들에게 금융 활동에 참여할 수 있는 기회를 제공합니다. 시장 및 소비자 데이터 회사인 Statista가 실시한 2021년 2월 설문조사에 따르면 대중들 사이에서 암호화폐를 가장 빈번히 사용하는 상위 10대 국가는 모두 신흥시장 국가였습니다. 응답자의 32%가 비트코인이나 암호화폐를 더 광범위하게 사용하고 있다고 답한 나이지리아가 선두이고, 21%의 베트남과 20%의 필리핀이 그 뒤를 이었습니다.[4]

국가별 암호화폐 사용

출처: Global Consumer Survey, 2021 년 2 월 28 일 기준.



비트코인이 사용될 수 있는 또 하나의 주요 사용처는 송금 분야입니다. 신흥시장 국가에서는 송금이 GDP 중에서 차지하는 비중이 선진국에 비해 매우 높습니다. 세계은행에 따르면 거래 수수료가 전 세계의 송금 평균 금액을 6.4%나 감소시킵니다. 송금 비용이 더 높은 일부 국가간 송금에서는 수수료가 10% 이상으로 증가할 수 있습니다.[5]

지역별 평균 송금 비용

출처: http://remittanceprices.worldbank.org 에서 얻을 수 있는 세계은행의 전 세계 송금 비용. 2021 년 3 월 31 일 기준.

일부 신흥 경제의 경우 비트코인을 사용하여 자금을 해외 송금하면 상당한 비용을 줄일 수 있습니다. 예를 들어, 엘살바도르는 인구의 약 70%가 송금을 받고 있는 국가입니다. 비트코인을 법정 통화로 채택한 첫 국가가 되기로 한 정부의 결정은 주목할 만한 시험 케이스가 될 수 있습니다. 한 예측에 따르면,

비트코인은 국가적으로 송금 비용에서 일년에 4억 달러를 절약할 수 있습니다.[6]

규제 환경: 진화하는 과정의 일부분

아직 초기 단계인 비트코인은 다른 디지털 자산과 마찬가지로 국가별, 국가 내 관할 지역별로 다르고 불확실하면서도 짜기운 듯한 규제 환경에서 운영되고 있습니다. 예를 들어, 미국의 암호화폐 규제는 연방 차원에서는 거의 없지만 개별 주에는 자체 규칙이 있으며 일부 주의 경우에는 다른 주보다 더 엄격합니다. 뉴욕주 금융서비스부(NYDFS)는 미국의 다른 주보다 매우 엄격한 규제를 갖추고 있습니다.

전 세계적으로 규제, 분류, 세금 처리가 다르기 때문에 비트코인에 대한 규제 환경을 평가하기가 어렵습니다. 시간이 지나면서 더 정교한 규제 체계가 개발될 것으로 예상합니다. 규제 체계가 더 분명해지면 리스크가 줄어들어 비트코인에 도움이 되고 참여가 늘어날 수 있을 것입니다. 비트코인을 받는 곳이 점점 더 많아짐에 따라, 신중한 규제를 실행하지 못하면 비트코인을 사용하여 사업을 운영하려는 회사와 지역의 혁신에 방해가 될 수 있습니다. 예를 들어, 미국 내 최대의 암호화폐 거래소 중 하나인 Kraken은 뉴욕주가 2015년 가상화폐 라이선스(BitLicense) 체제를 실행한 후 뉴욕주 내에서의 운영을 그만두었습니다.[7]

지나친 규제 리스크는 고려할 점이지만 비트코인 네트워크가 가진 분산적, 세계적 성격은 과도한 규제의 영향을 완화할 수 있습니다. 2021년 9월 중국의 전면적인 암호화폐 금지 이후 가격 혼란이 미미했던 점은 하나의 예라고 생각합니다.[8]

왜 지금 비트코인인가: 이러한 경제 시기를 위한 자산이기 때문입니다

비트코인의 커지는 매력을 이해하려면 등장한 시기가 정치사회적 영향이 컸던 과거 두 번의 경제 위기와 겹친다는 점을 고려해야 합니다. 이러한 위기로 인해 전통적인 금융 시스템에 있어서 가장 큰 문제점, 즉 불신과 접근의 어려움이 드러났습니다. 그러나 비트코인의 주요 원칙은 이러한 문제점을 해결합니다.

- 비트코인은 참가자들이 신뢰하는 정부기관이나 금융 중개기관 없이도 전 세계에서 가치를 교환할 수 있는 탈중앙집중식 네트워크입니다.
- 블록체인 기술은 네트워크 참가자들이 완전히 투명한 일련의 프로토콜 규칙을 따름으로써 분산된 원장에서 합의 상태에 이르는 것이 가능하도록 합니다.
- 디지털 통화는 언제든 분할이 가능하고 대체가 가능하며 프로그램으로 정의되어 희소성을 보장하는 통화 정책을 통해 이전이 가능합니다.
- 그리고 참여하려면 인터넷 연결만 있으면 됩니다.

이러한 속성은 개인 투자자들과 주류 금융권에서 상당한 반향을 일으켰습니다. 이제 투자은행과 헤지펀드도 금융 자본과 인적 자본을 비트코인에 배정합니다. 회사는 자신의 대차대조표에 비트코인을 포함시키기 시작하고 있습니다. 심지어 대학도 투자하고 있습니다. 이런 상황에 신뢰를 더해주는 것은 규제를 받는 비트코인 파생상품이 도입되어 잘 운용되고 있다는 점입니다.

2008년 10월, 최대의 수수께끼는 사토시 나카모토의 신원이 아니라 비트코인이 세계 경제에서 어떤

자리를 차지할 수 있는지 여부였습니다. 13년이 지난 후, 나카모토의 신원은 여전히 알려지지 않았지만 비트코인은 더욱 친숙하게 지속적으로 합법성을 얻고 있습니다. 결국, 증가하는 글로벌 사용자들의 네트워크를 갖춘 검증 가능하고 희소한 자산을 소유할 수 있는 가능성으로 인해 투자자들의 관심이 더 커질 것입니다.

—

용어 해설

용어는 나타나는 순서대로 열거하였습니다.

암호작성술: 적대적 행동이 존재하는 상황에서 정보 전송의 보안을 확보하기 위한 기술에 대한 광범위한 연구. 퍼블릭 키 암호작성술을 참조하십시오.

비트코인 네트워크: 비트코인 코어 소프트웨어를 구동하는 P2P 컴퓨터 네트워크. 비트코인 네트워크는 신뢰하는 중개 기관 없이 가치(비트코인)의 이전을 가능하게 합니다.

블록체인(체인): 신뢰하는 중개 기관 없이 거래 기록과 자산을 추적하고 P2P 방식으로 공유하며 지속적으로 대사가 이루어지는 분산된 원장. 노드라 불리는 네트워크 참가자들은 네트워크 규칙에 따라 다른 노드가 검증하는 거래와 블록을 전파합니다. 거래는 블록으로 취합되고, 블록은 거래 시간과 순서를 기록합니다. 블록은 이전 블록과 연결되어 체인을 형성하며, 이러한 체인은 각 후속 블록이 추가됨에 따라 선형으로 커집니다. 평균 10분마다 체인에 블록이 추가됩니다.

비트코인:전적으로 비트코인 블록체인의 원장 잔액으로서 존재하는 무기명 디지털 자산. 이는 비트코인 네트워크에서 탄생한 암호화폐입니다.

암호화폐: 신뢰 받는 제3자가 아닌 암호작성술에 의존하는 탈중앙식 시스템에 의해 거래가 검증되고 기록이 유지되는 디지털 화폐.

온-체인: 실제 블록체인에서 일어나는 거래를 말합니다. 예를 들어, Coinbase와 같은 중앙집중식 암호화폐 거래소에서 거래하는 경우 중앙집중 기관은 자신의 모든 고객을 위해 유지하고 있는 원장에서 단지 비트코인을 이동시킵니다. 이러한 거래는 자산이 해당 플랫폼으로부터 인출될 때까지 블록체인에서는 사실상 거래가 이루어지지 않습니다.

프라이빗 키:무기명 디지털 자산인 비트코인의 소유권을 나타내는 것으로서 계좌 비밀번호와 비슷합니다. 비트코인 소유권을 검증하기 위한 디지털 서명을 만드는 데 프라이빗 키가 사용됩니다. 연관된 프라이빗 키를 찾을 수 있으면 그 주소의 비트코인을 가질 수 있습니다.

퍼블릭 키: 프라이빗 키로부터 수학적으로 얻을 수 있음. 퍼블릭 키와 연관된 비트코인을 사용하려면 퍼블릭 키를 공개해야 합니다. 디지털 서명을 퍼블릭 키와 검증하여 예상 사용자가 퍼블릭 키와 연관된 프라이빗 키를 통제하고 있는지 여부를 확인합니다. 그와 별개로, 퍼블릭 키는 주소를 생성하기 위한 암호화 해시 함수에 대한 입력값으로 사용됩니다.

주소: 퍼블릭 키에서 수학적으로 파생되는 것으로서 비트코인 거래의 목적지를 식별하는 데 사용되는 퍼블릭 사용자 이름과 유사합니다.

디지털 서명: 프라이빗 키 및 거래 해시에서 수학적으로 파생되는 것. 디지털 서명은 프라이빗 키를 노출시키지 않고도 프라이빗 키와 연관된 퍼블릭 키의 소유권을 증명합니다. 디지털 서명은 네트워크 상에서 비트코인 소유권을 독립적으로 검증할 수 있으며, 비트코인 소유자에게 자신의 비트코인을 자유롭게 사용할 수 있도록 하는 반면에 악의를 가진 누군가가 비트코인을 사용하는 것을 방지합니다.

비트코인 코어: 비트코인 프로토콜 및 비트코인 네트워크의 모든 측면을 실행하는 오픈 소스 컴퓨터

소프트웨어.

노드: 비트코인 코어를 구동하여 자신의 블록체인 사본을 유지하는 컴퓨터. 노드는 모든 거래 및 블록을 프로토콜 규칙에 대하여 독립적으로 검증함으로써 네트워크의 보안에 참여하고 유효한 거래 및 블록만을 연결된 피어에게 보냅니다.

퍼블릭 키 암호작성술: 비대칭 암호작성술로도 알려져 있으며, 별개지만 수학적으로 연결된 두 개의 키(하나는 암호용, 다른 하나는 복호용)를 활용합니다. 이는 비트코인 네트워크에서 활용되는 특정한 암호작성술로서, 퍼블릭 키는 비트코인을 받기 위해 사용되며 프라이빗 키는 비트코인을 사용하는 거래에 서명하기 위해 사용됩니다.

피어: 서로 직접 연결된 네트워크에 있는 노드.

메모리 풀: 멤풀이라고도 알려진 것으로, 노드에 의해 검증되었지만 블록에 추가되기 전에 로컬 컴퓨터 메모리에 저장되어 있는 미결 거래의 풀을 의미합니다.

채굴 노드: 거래를 블록으로 취합하고 블록을 블록체인에 연결하는 특수한 노드. 채굴 노드는 암호화 해시 함수에 근거하여 어려운 수학적 퍼즐을 제일 먼저 풀기 위해 경쟁합니다. 채굴자는 가능한 한 빨리 암호화 해시 함수를 통해 상이한 입력값의 결과값을 무작위로 연산하기 위해 대량의 연산 자원을 사용합니다.

작업증명(Proof-of-Work): 암호화 해시 함수를 통해 채굴자들이 풀기 위해 경쟁하는 어려운 수학적 퍼즐에 대한 해답. 암호화 해시 함수의 속성 때문에, 작업증명은 찾기가 매우 어렵지만 어떤 노드이든 채굴자가 이 솔루션을 찾기 위해 컴퓨터 자원을 사용했다는 점을 쉽게 확인할 수 있습니다. 작업증명은 두 블록이 동시에 채굴될 때 이견을 해결하는 데 도움이 되며, 기존의 블록을 조작하는 데 상당한 비용이 발생하게 함으로써 네트워크를 보호합니다.

암호화 해시 함수: 임의의 길이의 데이터를 결정론적으로 확정된 결과값에 매핑하기 위하여 사용할 수 있는 일방 함수. 암호화 해시 함수에는 다음과 같은 키의 속성이 있습니다. 1) 반복적임. 어느 입력값의 경우든 출력값(해시)은 항상 동일합니다. 2) 일방 함수로서 주어진 출력값에서 입력값을 얻는 것이 불가능합니다 3) 시각적으로 랜덤한 함수의 성격 때문에 입력값을 약간 조정하여 출력값을 조정하는 것이 불가능합니다. 채굴 과정은 가능한 한 빨리 반복적으로 암호화 해시 함수의 결과값을 연산하여 일정한 출력값을 얻는 것에 달려 있습니다. 퍼블릭 키로부터 주소를 얻기 위해 이러한 함수가 사용되기도 합니다.

해시: 암호화 해시 함수의 출력값.

후보 블록: 채굴자가 유효한 작업증명을 찾아서 블록체인에 추가하려 시도하고 있는 미결 거래들의 블록. 작업증명을 찾은 후에 후보 블록은 유효한 블록이 되어 체인에 추가됩니다. 이 시점에 채굴자는 새로운 후보 블록을 생성하고 새로 받은 블록에 연결된 퍼즐을 제일 먼저 풀어 유효한 다음 블록을 체인에 추가하려고 노력합니다 일반적으로 채굴자는 거래 수수료가 가장 높은 메모리 풀에 있는 거래를 선택함으로써 후보 블록을 생성합니다.

블록 리워드: 블록 해결에 대한 재정적 인센티브로서 채굴자가 새로 생성된 비트코인의 일정 수량을 자신에게 보내는 특수한 거래. 현재 블록 리워드는 블록당 6.25 비트코인입니다. 블록 리워드는 새로운 비트코인을 생성하는 유일한 방법입니다.

거래 수수료: 채굴자가 성사된 거래를 블록에 포함시킨 데 대해 인센티브를 주기 위한 소액의 거래 수수료. 거래 수수료는 통상적으로 미미하지만 네트워크가 심히 혼잡한 기간에는 상당히 커질 수 있습니다.

반감: 블록 리워드의 규모를 50% 줄이는 것. 21만 블록마다 또는 약 4년마다 반감 이벤트가 발생합니다. 다음 반감 이벤트는 2024년에 발생하며 비트코인 블록 리워드를 블록당 3.125 비트코인으로 감소시킬 것으로 예상됩니다.

난이도: 특정 시점에 비트코인 블록을 채굴하는 것이 얼마나 어려운가에 대한 척도. 비트코인 네트워크는 평균 10분마다 블록을 채굴하도록 설계되어 있습니다. 따라서 채굴자 뒤에 있는 연산 처리능력이 증가(감소)하면 계속 평균 10분마다 블록을 채굴할 수 있도록 난이도가 높아(낮아)집니다. 2,016 블록마다 또는 약 평균 2주마다 난이도가 조정됩니다. 소프트웨어는 단순히 마지막 2,016 블록을 채굴하는 데 소요되었던 실제 분 단위 시간과 2,016 블록을 채굴하는 데 소요되는 예상 시간(20,160분) 비율을 취하여 이전의 난이도를 이 비율만큼 상향 또는 하향 조정합니다.

해시레이트: 한 시점에 비트코인 네트워크 안전성을 확보하는 데 필요한 총 연산처리능력 추정치. 해시레이트는 네트워크 내의 모든 채굴자가 모두 연산할 때 초당 해시의 수로 측정됩니다. 비트코인 네트워크 해시레이트는 2021년에 정점인 초당 약 18,000경 해시에 도달하였습니다.

메인 블록체인(메인 체인): 기초 블록의 난이도에 기초하여 가장 많은 누적 채굴 작업을 한 블록체인. 일반적으로 메인 체인에 블록이 가장 많습니다.

포크: 단일 체인에서 서로 다른 두 개의 체인으로 분기되는 블록체인. 이러한 체인은 이전의 블록은 동일하지만 어느 한 지점에 도달하면 새로운 블록은 더 이상 같지 않게 됩니다. 채굴자가 한 블록을 동시에 채굴하는 경우 임시 포크가 생기지만 프로토콜 규칙에 따라 이러한 임시 포크는 하나의 메인 체인으로 다시 수렴합니다. 프로토콜 규칙이 변경 중인 때에는 포크가 좀 더 오래 지속되기도 하며, 프로토콜 규칙에 대해 커뮤니티가 합의를 이루지 못하는 때에는 운영 중인 소프트웨어의 여러 버전의 포크가 생기기도 합니다.

불역성: 변경이 불가능한 상태 또는 여건.

확인: 한 특정 거래가 한 블록에 포함된 후 블록체인에 더해진 블록의 수. 첫 확인은 한 거래가 블록에 포함될 때입니다. 유효한 새 블록이 체인에 채굴될 때마다 추가 확인이 더해집니다.

1. Blockchain.com, 2021년 10월 21일 기준
2. Coinmarketcap.com, 2021년 10월 21일 기준
3. Blockchain.com, 2021년 10월 21일 기준
4. Statista Global Consumer Survey, 2021년 2월 28일 기준
5. Remittance Prices Worldwide, "전 세계 분기 송금 비용", 2021년 3월 31일 기준
6. CNBC.com, "엘살바도르의 새로운 비트코인 계획은 Western Union과 같은 금융기관 등의 수익을 연간 4억 달러 줄일 수 있다", 2021년 9월 9일 기준
7. Blog.kraken.com, "뉴욕이여 안녕", 2015년 8월 9일 기준.
8. Coinmarketcap.com, 2021년 10월 21일 기준

비트코인과 비트코인 선물은 비교적 새로운 자산군입니다. 비트코인과 비트코인 선물에는 고유하고 중대한 리스크가 수반되며 역사적으로 상당한 가격 변동성이 있었습니다. 이러한 투자 대상에 대한 투자의 가치는 예고 없이 중대하게 하락하여 영(0)이 될 수도 있습니다. 투자자산 전부를 잃는 경우에 대비해야 합니다.

투자에는 원금 손실 가능성을 포함한 리스크가 수반됩니다. 분산투자를 통해 이익이 발생하거나 손실이 발생하지 않는다는 보장은 없습니다. 이 정보는 개인 또는 개인 맞춤형 투자 또는 세무 자문이 아니며, 매매 목적으로 이용할 수 없습니다. 본인의 투자 및 세무 상황에 관한 더 자세한 정보는 재무상담사 또는 세무전문가와 상담하시기 바랍니다.

본 자료는 특정 시점의 시장 환경에 대한 평가를 나타내는 것으로 미래의 사건을 예측하거나 미래의 결과를 보장하려는 것이 아닙니다. 이 정보는 개인 또는 개인 맞춤형 투자 또는 세무 자문이 아니며, 매매 목적으로 이용할 수 없습니다. 본인의 투자 및 세무 상황에 관한 더 자세한 정보는 재무상담사 또는 세무전문가와 상담하시기 바랍니다.

비트코인은 대체로 규제를 받지 않으므로 비트코인 투자는 더 많은 규제를 받는 투자 상품보다 사기 및 조작에 더 취약합니다. 비트코인과 비트코인 선물은 인플루언서와 미디어에 의한 행동과 진술 결과를 포함해 급격한 가격 변동의 영향을 받기 쉽습니다.