korbit
Research

우리가 믿지 말아야 할 10가지 Myths

2024.8.2

테마

가상자산 시장

관련 자산

가상자산
Cryptocurrency

작성자

최윤영 | Yoonyoung Choy
yoonyoung.choy@korbit.co.kr

김민승 | Min Seung Kim
minseung.kim@korbit.co.kr

주요 자산 가격(2024.7.30)

BTC	
USD	$68,727
KRW	₩93,230,000
김치프리미엄	+1.27%

ETH	
USD	$3,577
KRW	₩4,637,000

가상자산에 대한 10가지 잘못된 생각들

1. 비트코인은 **가치 저장 수단**이 아니다?
   → 비트코인의 변동성은 **점차 감소**하고 있다.
2. 비트코인은 **희소성**이 없다?
   → 비트코인의 희소성은 고유한 네트워크 효과 등에 결정되며, **비트코인 포크(fork)**는 비트코인 네트워크의 영향력과 가치를 희석시키지 못한다.
3. 비트코인은 **환경오염**을 유발한다?
   → 비트코인은 전통적인 은행업과 금 채굴보다 **에너지 효율적**이고, 재생에너지 사용이 증가하고 있다.
4. 비트코인은 **범죄 활동을 조장**한다?
   → 비트코인은 전통적인 금융 수단에 비해 불법 활동에 **훨씬 적게 사용**된다.
5. 비트코인은 **버블**이다?
   → **디지털 금**이라고도 불리는 비트코인은 금의 많은 특성을 공유한다.
6. **마운트곡스발** 대량 매도가 나올 것이다?
   → 조기 지급 비율, 펀드의 보유 및 배분 전략, Bitcoinica의 파산 절차 등 여러 요인으로 인해 실제 시장에 풀릴 비트코인 매도 물량은 **제한적일 것**이다.
7. **비트코인 반감기**가 지나면 가격은 반드시 상승한다?
   → 비트코인 반감기는 공급 감소에 따른 가격 상승 요인이 될 수 있지만, 외부 요인과 시장 역학의 복합적인 영향을 고려할 때 반감기 후 가격 상승이 **반드시 보장되는 것은 아니다.**
8. **양자 컴퓨팅**이 도입되면 비트코인은 없어질 것이다?
   → 양자 컴퓨팅은 프라이빗 키 보안을 위협할 수 있으나, 비트코인 네트워크의 기본 작동 원리와 기록 원장은 그대로 유지되며, **양자 저항성을 개발**하기 위한 노력들이 이루어지고 있다.
9. **CBDC**가 가상자산을 대체할 것이다?
   → CBDC가 금융 접근성 및 효율성을 높일 수 있겠지만, 가상자산은 **금융 간소화 이상의 목적**과 잠재력을 지니고 있다.
10. **알트코인 불장**은 무조건 온다?
    → 이번 상승 사이클에서는 비트코인의 상승이 **알트코인으로 전이되지 않았으며,** 이는 기관 자금의 제한적 유입, SEC의 규제, 그리고 시장 구조 변화 등 다양한 요인 때문으로 판단된다.

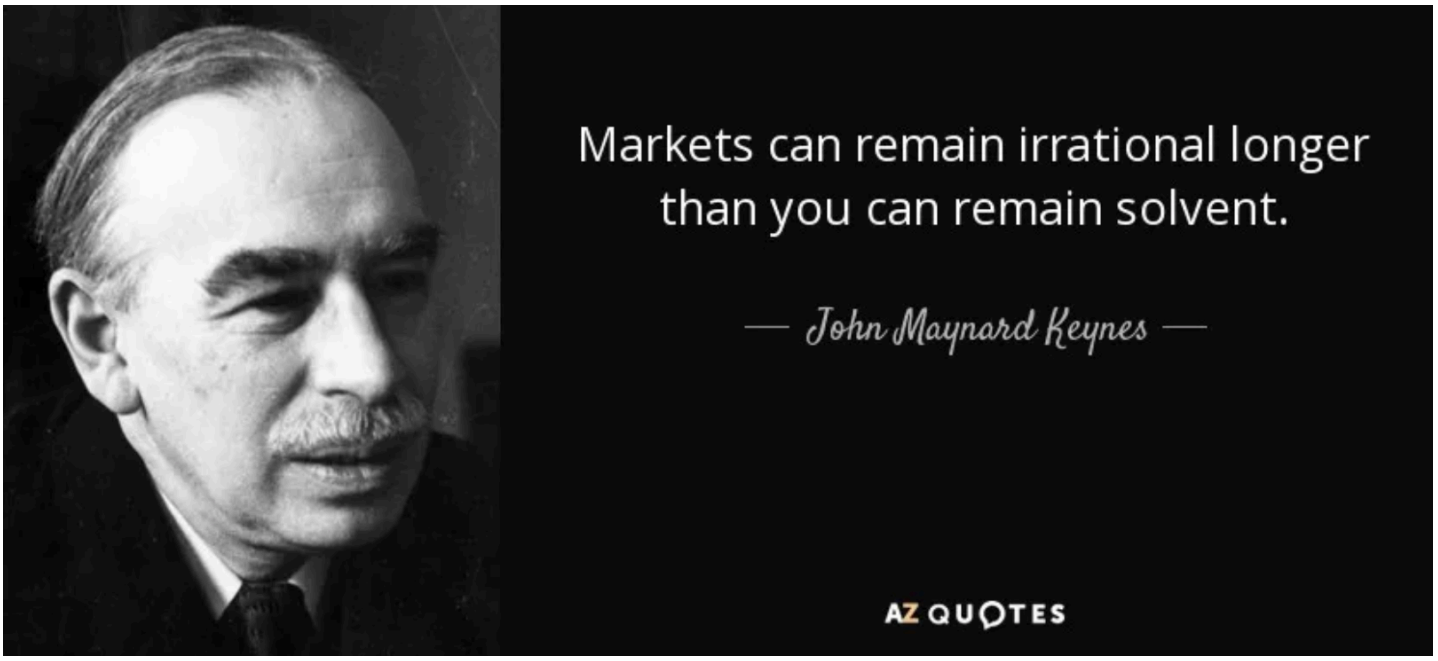
경제학자 존 메이너드 케인스(John Maynard Keynes)는 “시장은 비합리적인 상태를 오래 유지할 수 있다(Figure 1).”고 말했다. 이 말은 변동성과 투기적 열기가 근본적인 진실을 가리는 경우가 많은 가상자산 시장에 깊은 울림을 주며, 정보에 입각한 투자 결정을 내리기 위해서는 사실과 허구를 분리하는 것이 중요함을 시사한다.

기술 혁신과 엄청난 잠재력을 바탕으로 탄생한 가상자산 시장에는 사실에 기반하지 않은 소문과 통념이 많이 존재한다. 이러한 오해들은 투자자의 심리를 흔들 수 있고 시장 상황을 모호하게 만들 수 있다. 따라서 가상자산의 여러 기회를 판단할 때에는 올바른 리스크 평가가 필수적이며, 이는 진실하고 타당한 정보를 기반으로 한 검토를 요구한다.

코빗 리서치의 100번째 보고서인 이번 리포트는 **가상자산과 관련된 10가지 통념(Myths)을 짚어보고 사실이 아닌 부분을 바로잡고자** 한다. 각국 정부와 금융 기관이 가상자산을 어떻게 규제하고 글로벌 금융 시스템에 통합할지 고민하는 지금, 이러한 소문들이 사실에 가까운지 거짓에 가까운지를 바로잡는 것은 더욱 의미가 있다고 생각한다. 코빗 리서치는 앞으로도 더욱 깊이 있는 인사이트와 분석을 제공하여 가상자산 시장의 올바른 이해와 성장에 기여하고자 한다.

Figure 1: John Maynard Keynes[1]

출처: AZ Quotes



[1] 존 메이너드 케인스(1883~1946)는 현대 거시경제 이론의 토대가 된 케인즈 경제학을 탄생시킨 영국의 경제학자이다. 그는 인간의 심리와 비합리적인 행동이 경제 및 금융 시장에서 중요한 역할을 하고, 시장의 비효율성과 불안정성을 초래한다고 주장하기도 하였다.

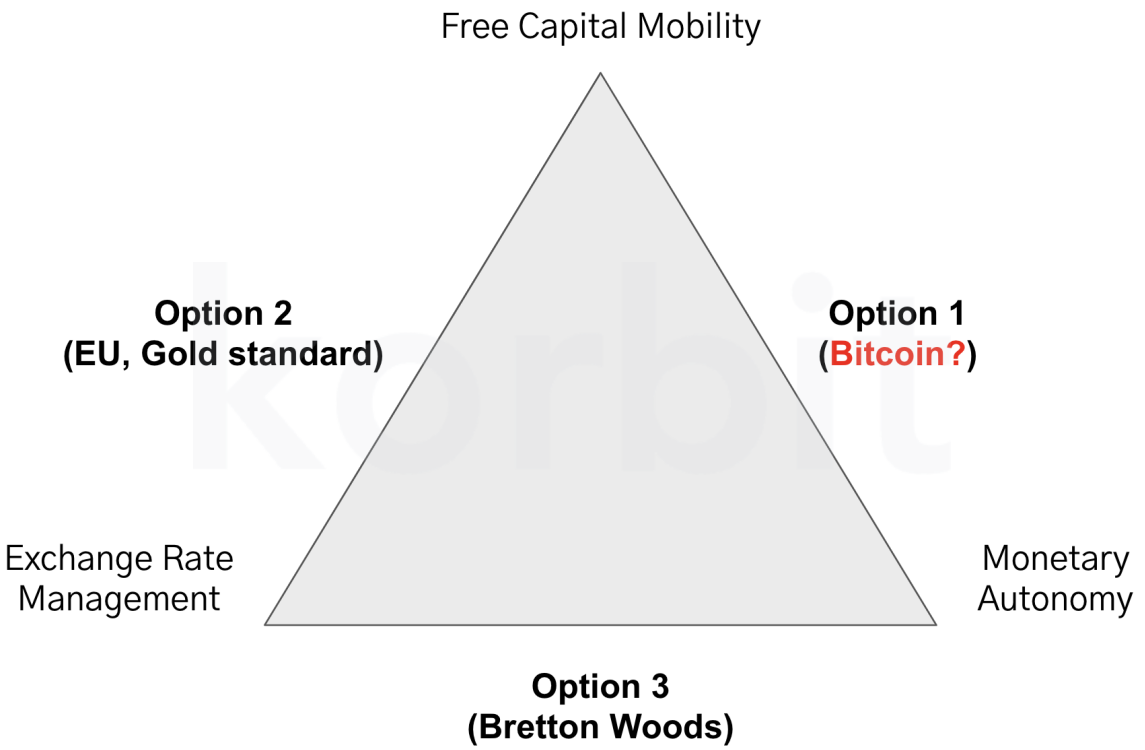
가상자산 시장에 대한 10가지 통념들

1. 비트코인은 가치 저장 수단이 아니다?

비트코인은 변동성이 크기 때문에 가치 저장 수단이 될 수 없다고 비판받곤 한다. 하지만 이렇게 비판하는 쪽에서는 비트코인이 변동성이 큰 이유를 제대로 이해하지 못하고 있다.

비트코인이 가치 저장 수단으로서의 역할을 하는 데 변동성이 방해가 되는 것은 사실이나, 실제로는 이 변동성 때문에 비트코인의 통화 정책에 대한 신뢰성이 강조되기도 한다. 거시경제 정책의 트릴레마(불가능의 삼각정리, 'The Impossible Trinity')는 비트코인의 가격 변동을 이해하는 데 도움을 준다[2]. 이 트릴레마는 정책 입안자가 통화 목표를 수립할 때 환율 안정(Exchange Rate Management), 자본의 자유로운 이동(Free Capital Mobility), 독립적인 통화 정책(Monetary Autonomy)이라는 세 가지 목표를 모두 만족시킬 수 없다고 설명한다(Figure 2). 예를 들어, 환율 안정과 자본의 자유로운 이동을 유지하려는 통화 당국은 통화 정책의 독립성을 포기해야 하고, 독립적인 통화 정책과 자본의 자유로운 이동을 유지하려면 환율 안정을 포기해야 한다.

Figure 2: 거시경제 정책의 트릴레마, 'The Impossible Trinity' 출처: The Economist, Ark Invest, 코빗 리서치



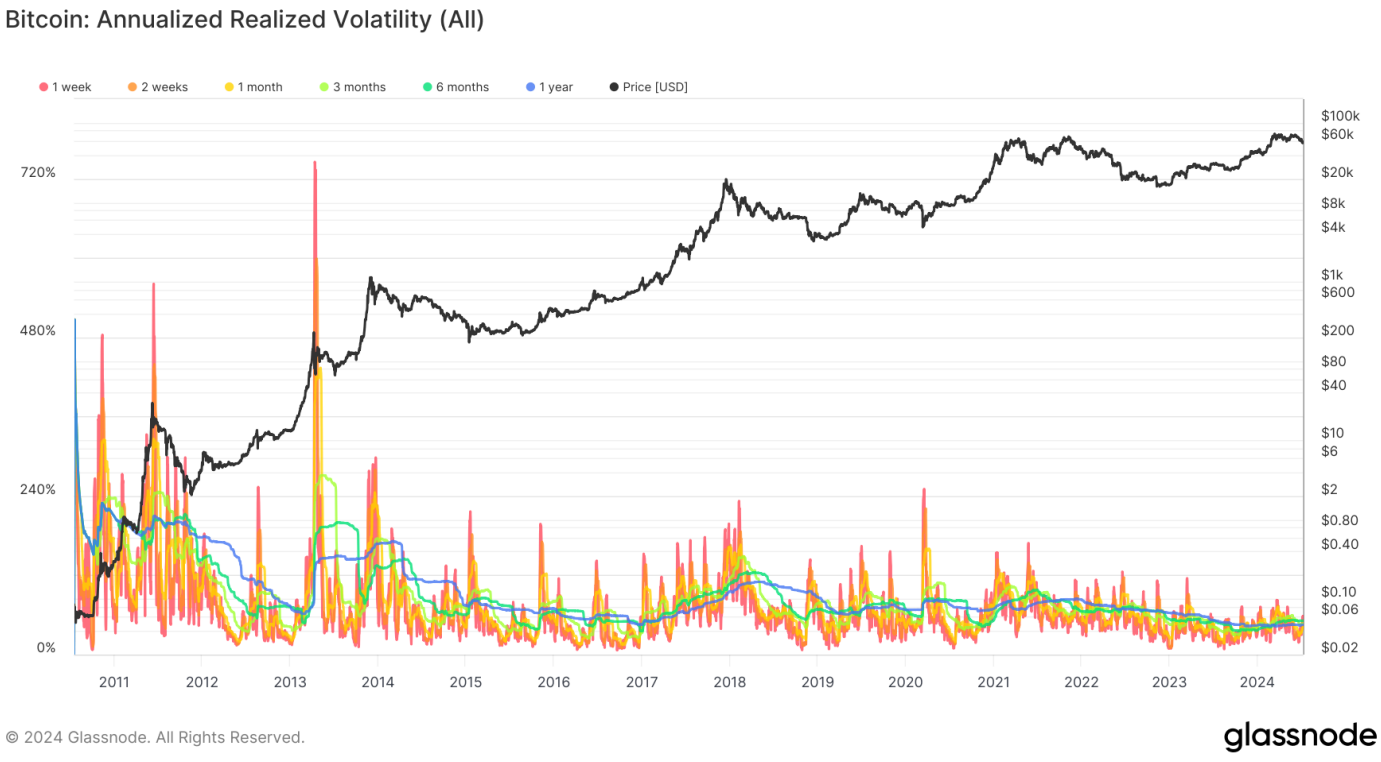
[2] Yassine Elmandjra, "Debunking Common Bitcoin Myths", June 29th 2021, Ark Invest.

이 트릴레마를 통해 비트코인 통화 정책의 변동성이 당연한 결과인 이유를 이해할 수 있다. 중앙은행과 달리 비트코인은 환율 안정성을 염두에 두지 않는다. 대신 비트코인은 화폐의 수량 원칙에 따라 통화 공급을 통제하고 자유로운 자본 흐름을 우선시한다. 그 결과 공급 대비 수요의 함수라 할 수 있는 비트코인 가격은 변동성이 클 수 밖에 없고, 따라서 비트코인의 변동성은 정책 선택의 자연스러운 결과로 간주된다.

더욱이 비트코인의 변동성은 시간이 지남에 따라 감소하고 있다(Figure 3). 비트코인이 더 널리 채택될수록 비트코인에 대한 한계 수요(marginal demand)가 전체 네트워크 가치에 미치는 영향은 낮아지게 되고, 결과적으로 가격 변동성은 감소할 것으로 예상된다. 예를 들어, 다른 모든 것이 동일하다면 네트워크 가치 100억 달러에 대한 신규 수요 10억 달러는 네트워크 가치 1조 달러에 대한 신규 수요 10억 달러보다 비트코인 가격에 더 큰 영향을 미칠 것이다. 즉, 비트코인 네트워크의 가치가 커짐에 따라 새로운 투자나 수요가 큰 가격 변동을 일으키는 데 미치는 영향은 줄어들게 된다. 따라서 변동성은 비트코인의 가치 저장 수단 역할을 방해하는 요인이라고 볼 수 없다.

Figure 3: 비트코인의 변동성 추이

출처: glassnode



2. 비트코인은 희소성이 없다?

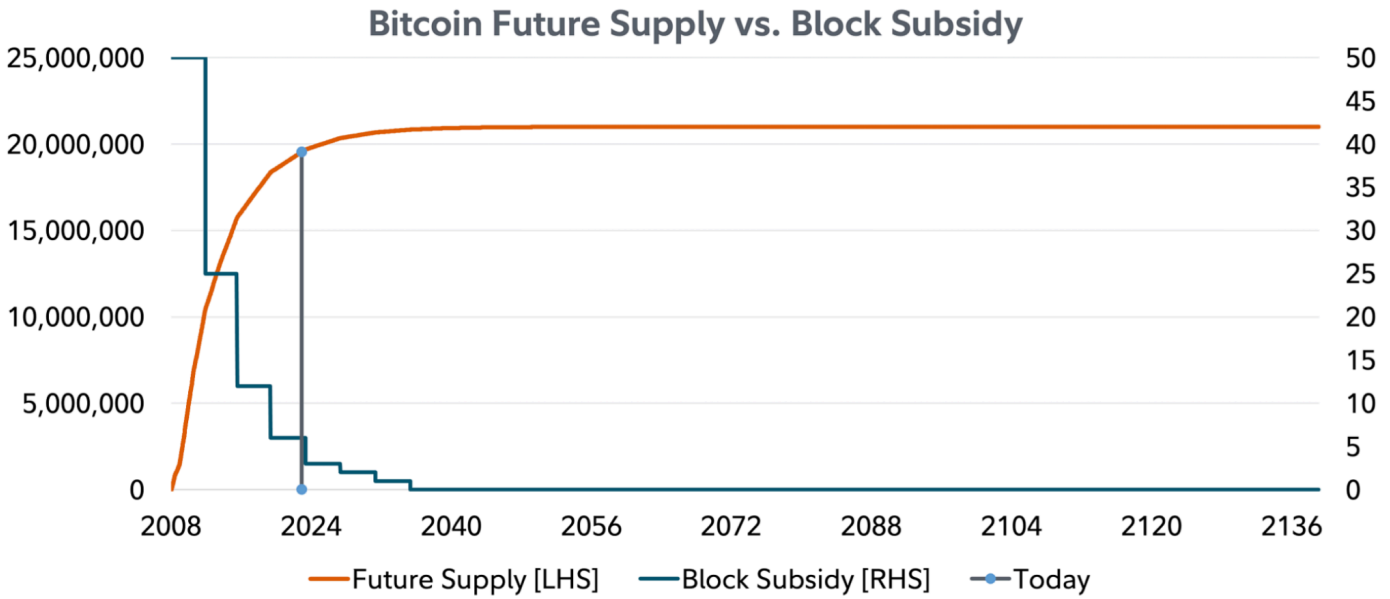
디지털 영역에서의 상품은 무형이고, 원본을 변경하지 않고도 쉽게 복사할 수 있다. 예를 들어, 워드 문서를 여러 사람에게 이메일로 전송해도 원본 파일은 그대로 유지된다. 마찬가지로 수백만 명이 동시에 동일한 디지털 상품(예: 음악)을 사용할 수 있고, 다른 작곡가들이 차별화된 사운드를 비슷하게 적용할 때 원본의 인지도(가치)가 높아질 수 있다. 이는 물리적 세계의 상품에서는 불가능한 특성이다.

비트코인의 소프트웨어도 마찬가지이다. 코드가 오픈 소스로 공개되어 있기 때문에 누구나 자신만의 버전을 제작해서 "네트워크 포크"를 하는 것이 가능하다. 혹자는 비트코인이 '복사'가 가능한 오픈 소스 소프트웨어라면 어떻게 희소성이 있을 수 있는지 의문을 가질 수 있다.

하지만 비트코인 네트워크를 포크하면 그 시점부터 새로 만들어진 네트워크는 독립적인 기록을 쌓아 가게 된다. 즉, 포크를 한다고 해서 기존 비트코인 수량이 늘어난다거나 시장 가치에 영향을 주는 것이 아니라 새로운 네트워크 시스템이 생겨나는 것이다. 베네수엘라에서 자국 통화(VES)를 인위적으로 늘린다고(인플레이션) 해서 미국의 통화 기반(monetary base)에 달러가 추가적으로 만들어지지 않고 미국 경제에 직접적인 영향을 미치지 않는 것과 비슷한 논리다. 비트코인을 포크한 네트워크는 포크 시점까지의 비트코인 기록을 공유하기 때문에 기존 비트코인 보유자는 새로 만들어진 네트워크의 고유자산(native asset)에 대한 권리를 가지지만, 포크된 네트워크는 고유한 이해관계자가 지원하는 독립적인 규칙에 따라 운영된다. 오픈 소스 소프트웨어는 기존 네트워크의 화폐 공급을 희석시키지 않고, 저비용으로 다양한 실험을 가능하게 하기 때문에 새로운 네트워크, 새로운 코인의 탄생을 가능하게 하고 혁신과 경쟁을 촉진한다.

비트코인의 희소성은 비트코인 네트워크의 정체성과 비트코인의 가치를 결정하는 매우 중요한 요소이다. 비트코인의 총 공급량은 2,100만 개로 고정되어 있으며 시간이 지나면서 채굴을 통해 이 한도에 도달하게 된다(Figure 4). 비트코인은 특정 시점에 하나의 지갑에만 연결되며 복사가 불가능하다. 사용자의 비트코인을 제어할 수 있는 유일한 방법은 해당 비트코인 지갑에 연결된 프라이빗 키에 액세스하는 것이다.

Figure 4: 비트코인 미래 공급량 vs 블록 보상 출처: Coin Metrics, Fidelity



Source: Coin Metrics, 11/20/2023.

그렇다면 비트코인 2,100만 개가 비트코인 캐시(BCH)처럼 포크된 코인 2,100만 개보다 더 가치가 있는 이유는 무엇일까? 비트코인 캐시의 가치를 비트코인의 가치와 동일시하는 것은 페이스북이나 인스타그램의 소스 코드를 '포크'하면 페이스북과 인스타그램의 사용자들과 광고주들, 콘텐츠를 그대로 복제할 수 있다고 믿는 것과 같다[3]. 비트코인과 페이스북의 가치는 소스 코드에만 있는 것이 아니라 사용자의 네트워크 효과에서 비롯된다. 블록체인 보안과 해시레이트의 상관관계, 비트코인의 전세계적 유동성, 그 외 비트코인의 채택과 사용을 지원하는 인프라 등 모든 것이 네트워크 효과에 포함될 수 있다. 포크된 코인이 비트코인의 네트워크 효과를 희석시키려면 비트코인의 해시파워, 사용자, 유동성의 상당 부분을 독점적으로 가져가야 할 것이다. 하지만 비트코인에서 포크된 코인들의 경우는 비트코인 네트워크에 대한 유의미한 영향이 미미했던 것으로 보인다[4].

3. 비트코인은 환경오염을 유발한다?

비트코인은 채굴 과정에서 많은 자원과 에너지를 소비한다고 비판받는다. 이는 비트코인 네트워크를 유지하는 데 드는 비용이 그로 인한 이익보다 크다는 비판으로 이어지기도 한다. 하지만 비트코인의 에너지 소비는 단순한 낭비가 아니라 네트워크의 보안을 유지하는 데 필요한 요소로 작용하며, 이는 비트코인의 설계 의도에 부합하는 특징 중 하나이다. 비트골드의 창립자이자 비트코인 선구자인 닉 사보(Nick Szabo)[5]는 "비트코인의 성공 비결은 엄청난 리소스 소비와 낮은 계산 확장성 대신 더 가치 있는 것, 즉 사회적 확장성을

[3] Yassine Elmandjra, "Debunking Common Bitcoin Myths", June 29th 2021, Ark Invest.
[4] Coin Metrics, "A Comparative Analysis of Bitcoin Forks", July 29 2019.
[5] Nick Szabo, "Money, blockchains, and social scalability", Feb 09 2017.

확보했다는 점이다(The secret to Bitcoin's success is that its prolific resource consumption and poor computational scalability is buying something even more valuable: social scalability.)."라고 강조했다.

비트코인은 탈중앙화되거나 신뢰를 최소화하는 방식으로 결제 확정성을 제공할 수 있다. 이는 특수한 전용 하드웨어(ASICs: Application-Specific Integrated Circuits)[6]를 통해 비용이 많이 드는 계산을 수행했음을 투명하게 증명할 수 있기 때문이다.

비트코인은 현실 세계의 자원을 채굴에 할당함으로써 확실한 결제를 보장한다. Chaincode Labs의 Hugo Nguyen은 "작업 증명 채굴 방식은 전기를 소모하여 복잡한 계산을 수행하고, 이를 통해 블록체인에 블록을 추가한다. 이 과정에서 소모된 에너지는 블록에 실질적인 '형태'를 부여하여, 블록이 물리적 세계에서 실질적인 영향을 미칠 수 있게 한다.[7]"라고 설명하기도 했다.

비트코인의 에너지 소비는 쉽게 측정할 수 있기 때문에 자주 피상적인 비판에 노출되는 것 같다. 그러나 전기 비용을 기준으로 비교했을 때에는 비트코인이 전통적인 은행업이나 금 채굴보다 훨씬 효율적이다. 전통적인 은행업은 연간 1,368Mtoe의 탄소를 배출하고, 금 채굴은 144Mtoe를 배출한다. 비트코인의 탄소 배출량은 연간 61.2Mtoe로 은행 배출량의 4.5%, 금 배출량의 43%에 불과하다(Figure 5).

일반적인 사람들의 인식과 달리 비트코인 채굴은 환경에 미치는 영향이 미미하다[8]. 비트코인 채굴에서 사용되는 에너지 중 많은 부분이 재생에너지, 특히 수력 발전에 의해 공급된다. 채굴자들은 가장 저렴한 형태의 전기를 찾기 위해 재생에너지가 풍부한 지역으로 계속 몰려들 것이고 이는 해당 지역의 전력원에 대한 기본 수요가 창출되는 효과가 있다[9]. 결론적으로 채굴자들의 노력이 환경적 및 사회적으로 긍정적인 영향을 미칠 수 있으며, 이는 고립된 에너지 자산을 효율적으로 활용하는데 기여한다.

[6] ASICs는 특정 용도에 맞게 설계된 집적 회로로 해당 작업을 수행하기 위해 특별히 설계된 맞춤형 하드웨어를 말한다.

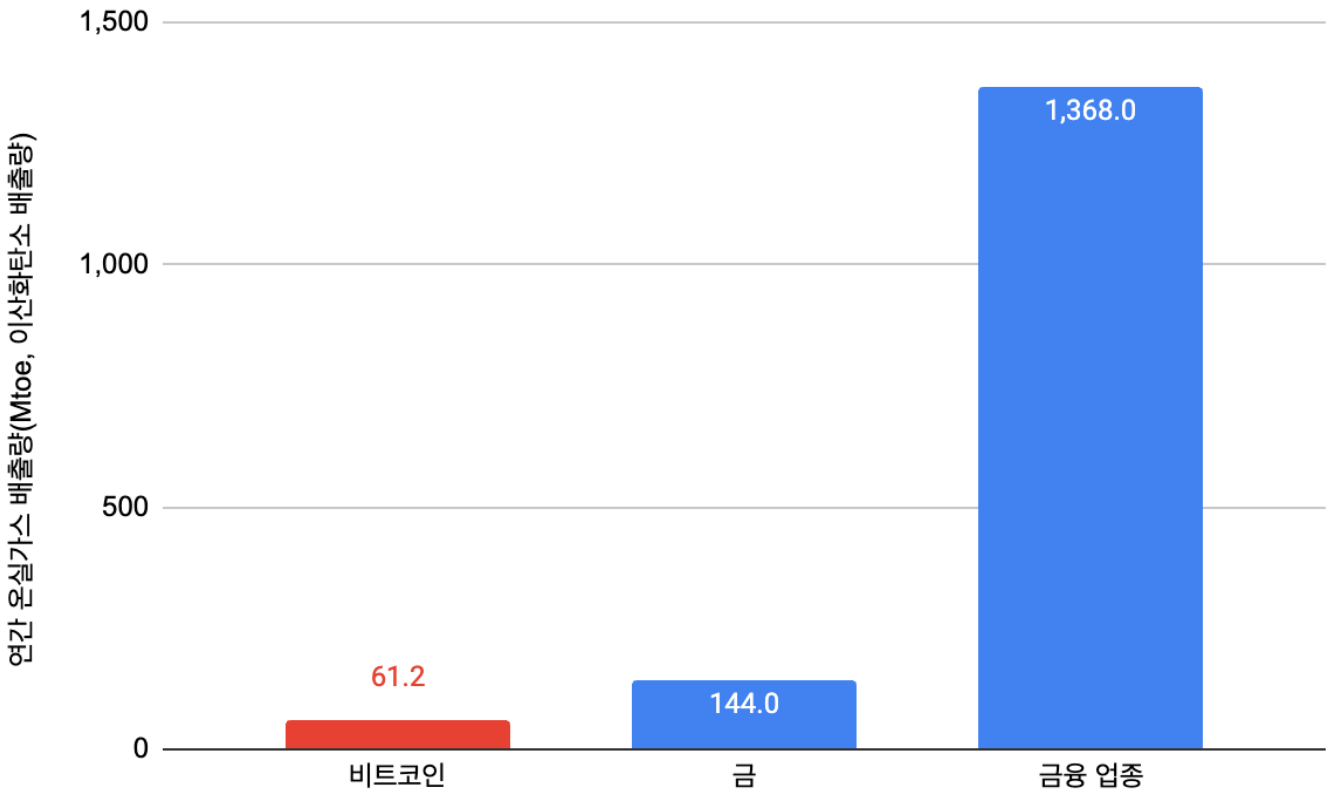
[7] 원문 "Under the hood, proof-of-work mining converts kinetic energy (electricity) into a ledger block. By attaching energy to a block, one gives it 'form', allowing it to have real weight and consequences in the physical world."을 의역.

[8] Dan Held, "PoW Is Efficient", Sep 15 2018; Yassine Elmandjra, "Debunking Common Bitcoin Myths", June 29th 2021, Ark Invest.

[9] Colin Harper, "OIL FIELD ALCHEMY: HOW BITCOIN CAN TURN WASTE, EMISSIONS INTO PROOF-OF-WORK", July 5 2023. Bitcoin Magazine.

Figure 5: 비트코인의 연간 온실가스 배출량 비교

출처: Bitcoin Magazine[10]



4. 비트코인은 범죄 활동을 조장한다?

비트코인은 범죄 활동을 조장한다고 비판받기도 한다[11]. 사실 비트코인은 초기에 불법 마약 거래로 유명한 온라인 암시장 플랫폼인 실크로드에서 거래 수단으로 사용된 적이 있었고, 이는 비트코인이 범죄에 사용된 대표적인 사례로 자주 언급되곤 한다.

하지만 비트코인이 범죄 활동을 조장한다는 주장은 데이터와 사실에 근거하여 반박이 가능하다[12]. 먼저 유럽연합 집행기구인 유로폴(Europol)의 보고서에 따르면 부동산, 명품 등과 같은 전통적인 경로가 유럽 내 주요 범죄 네트워크에 의한 자금세탁의 주요 도구로 사용되고 있다고 한다. 이와 대조적으로 가상자산은 전체 자금세탁에서 차지하는 비율이 매우 적다.

블록체인 분석 회사 체이널리시스(Chainalysis)[13]에 따르면 가상자산을 통해 이루어진 불법 거래의 총액은 전 세계 불법 자금의 1% 미만에 불과하다(Figure 6). 이는 가상자산이 금융 범죄의 주요 도구라는 주장과는

[10] Haas Mccook, “BITCOIN EMITS LESS THAN 5% OF THE LEGACY FINANCIAL SECTOR’S CARBON EMISSIONS”, May 24 2021.

[11] David Adler, ”Silk Road: The Dark Side of Cryptocurrency”, Feb 21st 2018, Fordham Journal of Corporate & Financial Law.

[12] Binance, “Real Estate, Checks, Luxury Items: Things More Likely Than Crypto to Be Instruments of Financial Crime” April 23 2024.

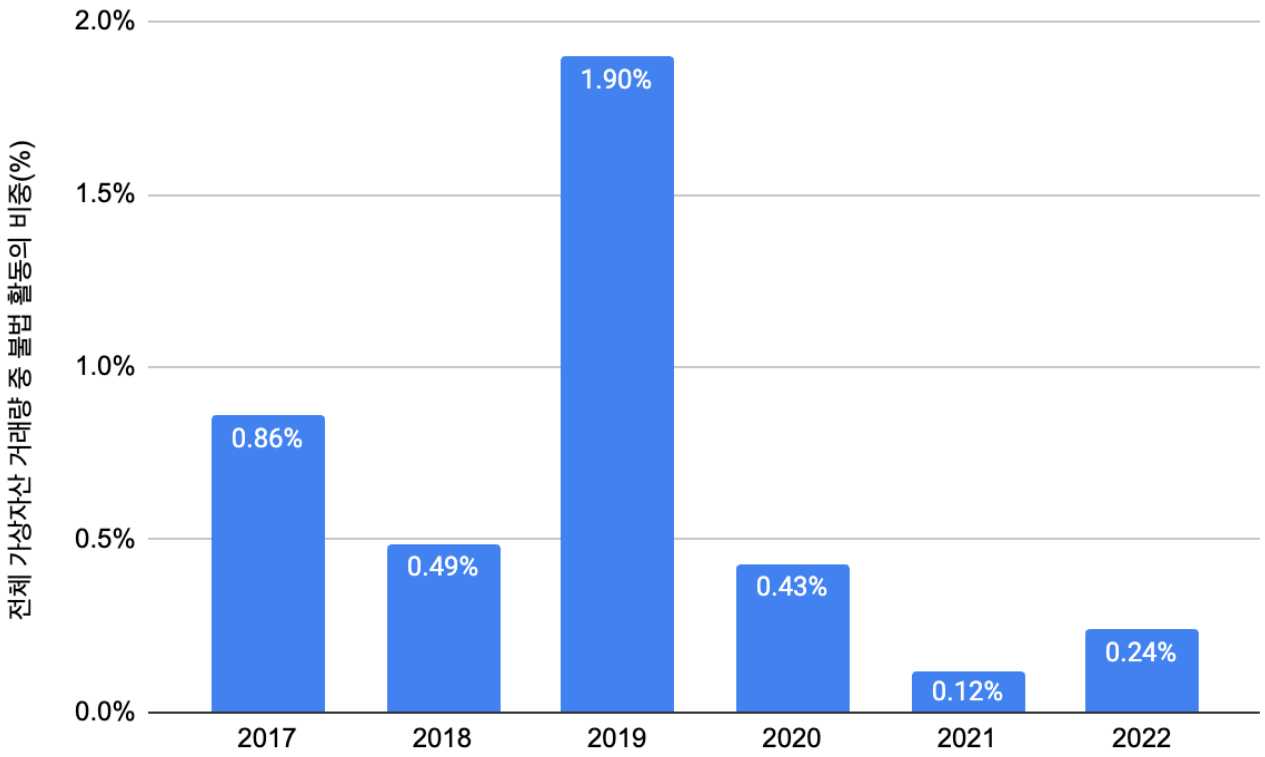
[13] Chainalysis, “The Chainalysis Crypto Myth Busting Report” July 2023.

크게 배치되는 내용이다. 미국 재무부의 보고서[14]에서도 가상자산을 통한 자금세탁이 법정화폐와 같은 전통적인 방법에 비해 매우 낮은 수준을 유지하고 있음을 확인할 수 있다. 이렇게 여러 보고서와 분석을 통해 알 수 있듯이, 비트코인 및 기타 가상자산은 실제로 전체 금융 범죄에서 차지하는 비율이 상당히 낮으며, 전통적인 금융 수단에 비해 범죄에 사용되는 경우가 훨씬 더 적다.

비트코인은 전 세계적으로 누구나 허가 없이(permissionless) 가치를 교환할 수 있게 해준다[15]. 그렇다고 해서 비트코인이 본질적으로 범죄 도구가 되는 것은 아니다. 휴대폰, 자동차, 인터넷이 범죄 활동에 사용될 수 있지만 그렇다고 해서 이 기술을 금지할 수 없는 것과 같은 논리이다.

Figure 6: 전체 가상자산 거래량 중 불법 활동의 점유율(%)

출처: Chainalysis



5. 비트코인은 버블이다?

일부 경제학자들은 비트코인이 버블 우려가 있고 곧 붕괴될 수 있다고 주장한다. 비트코인은 내재적 가치가 없으며, 도박과 같은 투기이며, 더 높은 가격을 기꺼이 지불하려는 "더 큰 바보 이론(a greater fool theory)"[16] 때문에

[14] U.S. Treasury, "2024 National Money Laundering Risk Assessment", February 2024.

[15] Yassine Elmandjra, "Debunking Common Bitcoin Myths", June 29th 2021, Ark Invest.

[16] 존 메이너드 케인스(John Maynard Keynes)가 만든 "더 큰 바보 이론(The greater fool theory)"은 경제학에서 유래된 말로 주식이나 채권, 부동산 등 특정 상품의 가격이 높은 상태라 하더라도, 더 높은 가격에 차익실현을 할 수 있을 것이라는 기대에 따라 투자에 나서는 것을 말한다. 즉, 이 표현은 투자자들이 실제

가치가 상승한다는 것이 이들의 논리다. 이러한 관점에서 본다면 비트코인은 투자 가능한 자산(investable asset)이 아니다. 하지만 이들의 주장은 비트코인이 시간이 지남에 따라 가치를 창출하는 이유를 간과하고 있다.

주식의 자산 가치는 예상 현금 흐름을 할인하여 결정된다. 성장률 및/또는 투자 자본의 수익률에 따라 미래 현금 흐름이 높아지면 주식은 주주 기반과 무관하게 가치가 상승한다.

그러나 비트코인과 같은 자산은 시간이 지나면서 얼마나 효과적으로 가치를 보존 또는 향상시키는지에 따라 가치가 결정되는 비생산적인(nonproductive) 자산이다. '비생산적'이라는 말의 뜻은 비트코인의 가치가 주식이나 부동산처럼 직접적인 수익을 창출하지 않고, 일종의 순환 논리에 따라 형성된다는 것을 의미한다. Northwestern 대학의 Adam Waytz 교수는 "돈은 공유된 환상(Money is a shared illusion)"이라고 말했다. 이 말은 곧 돈이라는 것이 본질적으로는 가치가 없는 단순한 종이에 불과하지만, 사람들이 그것에 가치가 있다고 믿기 때문에 가치를 갖게 된다는 의미이다. 돈의 가치는 사회적 합의와 신뢰에 기반한 것으로, 사람들 모두가 돈의 가치를 인정하고 그것을 교환 수단, 가치 저장 수단, 계산 단위로 사용함으로써 실제로 기능하게 된다.

화폐의 가치가 공유된 환상에 의존한다는 주장은 화폐의 형태가 자의적이라는 것을 암시한다. 실제로 화폐의 역사에 따르면 가장 보편적이고 지속 가능한 화폐는 그 수요를 지탱하는 특성을 지니고 있었다. 예를 들어, 수천 년 동안 경제학자들은 금의 희소성, 대체 가능성, 내구성 덕분에 금을 가장 성공적인 화폐로 인정해 왔다.

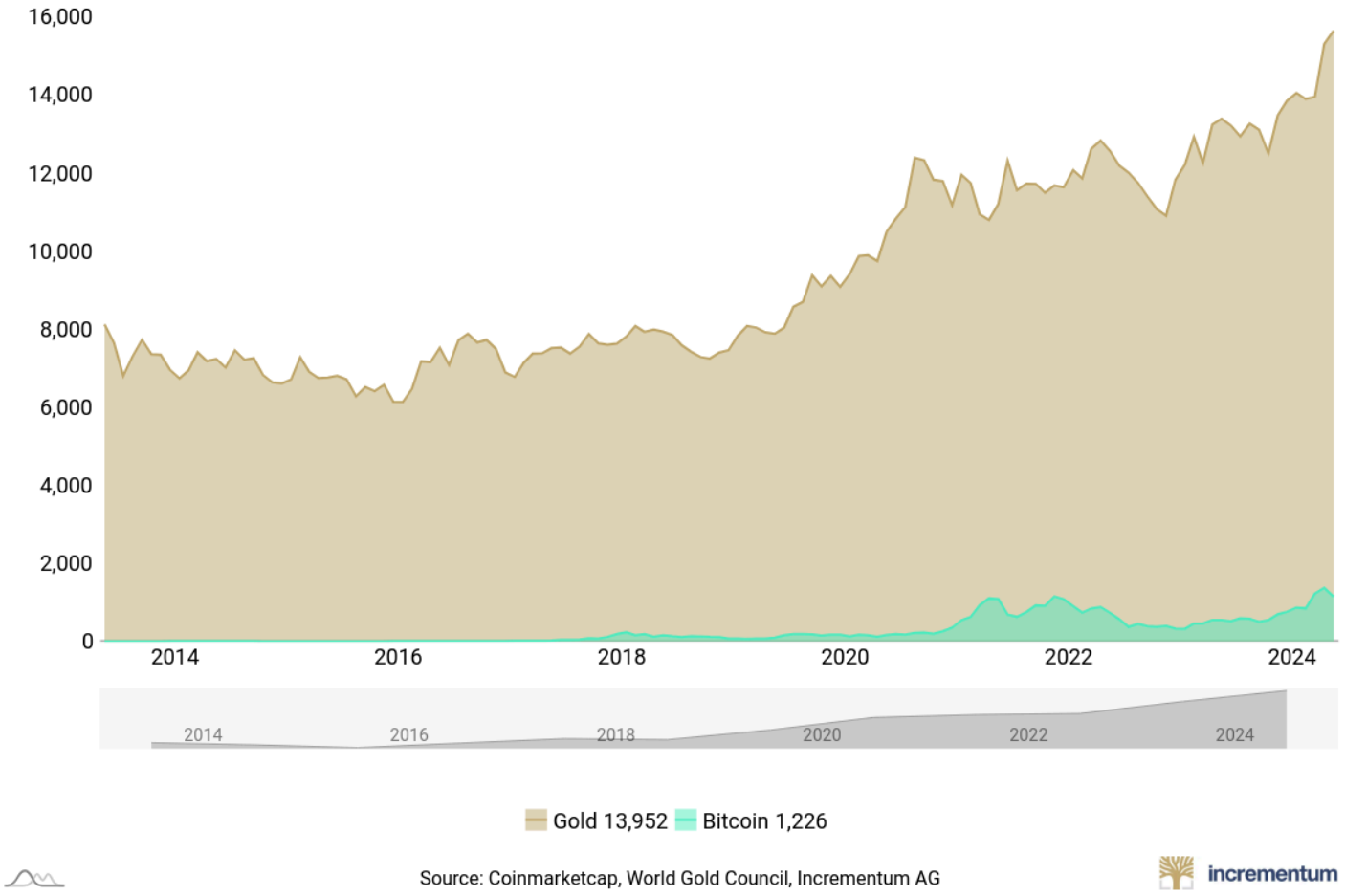
디지털 금이라고도 불리는 비트코인은 금의 많은 특성을 공유할 뿐만 아니라 이를 개선하기도 한다. 비트코인은 내구성(durability)과 희소성(scarcity)이 뛰어나면서도 검증 가능(verifiability)하고, 분할 가능(divisibility)하며, 전송이 가능(transferability)하고, 휴대가 가능(portability)하기 때문에 잠재적으로 금보다 더 큰 수요를 촉진할 수 있으며 글로벌 디지털 화폐의 역할에 더 적합하다고 판단된다[17]. 게다가 비트코인의 네트워크 가치 또는 시가 총액은 금의 7% 정도[18]에 불과하다(Figure 7).

가치보다 높은 가격에 자산을 매입하고, 그것을 더 높은 가격에 팔 의향이 있는 다음 사람을 찾기를 바라는 상황을 지칭한다(출처: Yassine Elmandjra, "Debunking Common Bitcoin Myths", June 29th 2021, Ark Invest).

[17] Yassine Elmandjra, "Debunking Common Bitcoin Myths", June 29th 2021, Ark Invest.

[18] 2024년 5월 기준 금의 시가총액은 15,642 billion USD이고, 비트코인의 시가총액은 1,147 billion USD이다.

Figure 7: 금의 시가총액과 비트코인의 시가총액 비교 출처: Coinmarketcap, World Gold Council, Incrementum AG



6. 마운트곡스발 대량 매도가 나올 것이다?

7월 5일 시작된 마운트곡스의 상환으로 인해 약 142,000 BTC가 시장에 풀릴 가능성이 제기되고 있다(Figure 8). 특히 2014년 마운트곡스가 파산 신청을 한 이후 약 10년 동안이나 비트코인 상환을 받지 못한 채권자들이 비트코인 현금화를 시도할 수 있기 때문에 단기간에 대규모로 비트코인이 매도 물량으로 나올 가능성을 우려하는 이들이 많은 것 같다. 하지만 당사는 여러 뉴스 헤드라인에서 우려하는 것과 달리 비트코인 매도는 훨씬 제한적일 것이라고 생각한다.

Figure 8: 마운트곡스의 상환 발표문 출처: Mt. Gox

July 5, 2024

To Whom It May Concern:

Rehabilitation Debtor: MtGox Co., Ltd.
Rehabilitation Trustee: Nobuaki Kobayashi
Attorney-at-law

Notice regarding Repayment in Bitcoin and Bitcoin Cash

On July 5,2024, the Rehabilitation Trustee made repayments in Bitcoin and Bitcoin Cash to some of the rehabilitation creditors through a part of the Designated Cryptocurrency Exchanges etc. in accordance with the Rehabilitation Plan.

Repayments to other rehabilitation creditors will be promptly made once the following conditions have been met: (i) confirmation of the validity of registered accounts and other matters; (ii) acceptance of the intention to subscribe to the Agency Receipt Agreement by Designated Cryptocurrency Exchanges etc.; (iii) completion of discussions between the Rehabilitation Trustee and Designated Cryptocurrency Exchanges etc. regarding repayments; and (iv) confirmation that repayments can be made safely and securely. We ask eligible rehabilitation creditors to wait for a while.

End of document

첫째, 현재 회수되어 상환 가능한 비트코인의 총량은 142,000개지만 채권자들이 조기 지급을 선택하면 원래 받아야 할 비트코인 수량에서 일정 비율(약 10-11%)을 차감(헤어컷)해야 한다. Galaxy Digital의 Alex Thorn에 따르면 만약 채권자 중에서 약 75%가 조기 지급을 선택한다면 106,500 BTC가 조기 지급 대상이 되고, 여기에 10~11% 헤어컷을 적용하면 실제 채권자들에게 지급되는 코인은 약 94,785 ~ 95,850 BTC이다.

둘째, 마운트곡스 파산 절차 동안 일부 펀드들은 채권자들로부터 파산 청구권을 매입하였고, 그 총량이 20,000 BTC라고 한다. 이 펀드들은 비트코인을 매도하여 현금으로 변환한 뒤 이를 배분하는 대신, 비트코인 자체를 그대로 LP(Limited Partner)[19]들에게 전달할 가능성이 높다고 한다. 그리고 이 펀드의 LP들 대부분이 고액 자산을 보유한 비트코인 소유자들로 구성되고 있고, 이들은 비트코인을 할인된 가격에 매입하고자 하는 의지가

[19] LP란 투자 펀드, 특히 사모펀드(Private Equity Fund)나 벤처캐피털 펀드(Venture Capital Fund)의 "Limited Partner(유한책임파트너)"를 의미한다. LP는 펀드에 자본을 제공하지만, 펀드의 일상적인 운영에 직접적으로 관여하지 않는 투자자를 가리킨다. LP는 투자한 금액에 한해서만 책임을 지며, 펀드의 운영과 관리는 주로 General Partner(GP, 일반파트너)들이 담당한다. 따라서, 본문의 문맥에서 LP는 비트코인을 보유하고 있는 고액 자산가들이며, 펀드가 매입한 비트코인을 직접 받을 가능성이 높은 투자자들을 지칭한다.

강하며, 비트코인을 단기적으로 매도하여 현금화하는 것보다 비트코인을 계속 보유하며 그 가치를 높이기를 원한다고 한다. 물론 일부 LP가 비트코인을 매도할 수 있지만, 이 또한 전체 LP 그룹 내에서 소수에 불과할 것으로 예상되기 때문에 전체적인 비트코인 매도 압력이 크지 않을 것이라는 점을 시사한다.

셋째, 마운트곡스 상환물량 중 Bitcoinica라는 거래소에게 지급될 10,000 BTC도 즉시 매도할 수 없다. 그 이유는 현재 이 거래소가 뉴질랜드에서 자체적인 파산 절차를 밟고 있기 때문이다. 이 파산 절차가 완료된 후에야 그 비트코인들이 매도될 수 있을 것이고, 따라서 해당 비트코인은 당장 시장에 매도 물량으로 나올 가능성이 낮다고 볼 수 있다.

위에서 언급한 조기 지급 대상 106,500 BTC에서 청구권을 매입한 펀드들의 20,000 BTC를 제하면 86,500 BTC가 된다. Bitcoinica의 보유량 10,000 BTC를 제하면 76,500 BTC가 되며 여기에 10~11% 헤어컷을 적용하면 최종적으로 조기 지급을 선택한 채권자들에게 지급될 비트코인은 약 68,000 BTC임을 예측해 볼 수 있다. 하지만 이들 또한 10년 전부터 비트코인을 소유하고 있었던 투자자들이기 때문에 비트코인에 대한 강한 신념을 갖고 있을 가능성이 높다. 물론 마운트곡스 파산 때보다 비트코인 가격이 많이 올랐기 때문에 매도 유인도 있을 수 있겠으나, 10년 이상 비트코인을 보유하며 100배 이상의 가격 상승을 목도한 개인 투자자들이 상환을 받자마자 시장에 매도할 것이라고 가정할 근거는 희박하다.

7. 비트코인 반감기가 지나면 가격은 반드시 상승한다?

비트코인 반감기는 채굴자에게 지급되는 블록 보상이 4년 주기로 감소하는 것을 말한다. 투자자들이 반감기를 기대하는 이유는 반감기에 따른 공급 감소가 가격에 미치는 잠재적인 영향 때문이다. 분석 기간에 따라 정도의 차이는 있지만 과거 반감기 이후에 비트코인은 랠리를 이어왔다(Figure 9). 그 결과 많은 투자자들이 반감기 이벤트를 가격 상승에 대한 선행 지표로 간주하고 있는 것 같다.

Figure 9: 과거 비트코인 반감기와 가격 상승률

출처: @thescalpingpro X, 매경

역대 비트코인 반감기와 상승률

1차 반감기	2012년 11월 28일	9417%(2013년 11월 30일)
2차 반감기	2016년 7월 10일	2931%(2017년 12월 17일)
3차 반감기	2020년 5월 12일	682%(2021년 11월 10일)
4차 반감기	2024년 4월 21일(예상)	미정

하지만 상관관계가 있다고 해서 반드시 인과관계가 성립하는 것은 아니다[20]. 반감기는 공급량 감소 측면에서 봤을 때 가격 상승 요인 중 하나이다. 하지만 가격 상승을 반감기 이벤트 때문으로만 돌리는 것은 시장 역학을 지나치게 단순화한 것이라고 생각한다. 어떤 자산이 상승 또는 하락하는 데에는 지정학적 관계, 규제 변화, 기술 발전과 같은 외부 요인도 중요한 역할을 한다.

특히 이번 반감기는 과거 세 번의 반감기와는 몇 가지 차이점이 있다고 한다[21]. 첫째, 과거에는 반감기 전후로 비트코인 가격 변동이 크지 않았고 반감기 후 약 6개월이 지나고 나서야 본격적인 가격 상승이 시작되었다. 둘째, 이번 반감기 이후에는 미 연준의 통화정책 변화가 예상된다. 2012년과 2020년 반감기는 연준의 통화정책 완화 중에 이루어졌고, 2016년 반감기는 긴축 정책 중에 발생했다. 셋째, 올해는 미국 증시에 상장된 비트코인 현물 ETF 때문에 반감기가 시작되기 이전부터 비트코인에 대한 큰 수요가 존재했다. 현물 ETF 상장 이후 6개월이 지난 현재 시점까지 비트코인 래퍼(wrapper)에 약 154억 달러가 들어왔다. 현물 ETF 출시는 제도권 자금이 유입될 수 있는 경로가 되기 때문에 비트코인에 대한 명확한 수요 기반이 확보된 상황에서 반감기가 이루어진 것은 올해가 처음이다.

8. 양자 컴퓨팅이 도입되면 비트코인은 없어질 것이다?

양자 컴퓨팅(quantum computing)은 양자 이론(quantum theory)[22]의 원리를 기반으로 컴퓨터 기술을 개발하는 데 중점을 둔 과학 분야이다. 현재

[20] Coinshares, "Halving: Hype or Reality? Debunking Common Myths Surrounding Bitcoin Halving", March 28th 2024.

[21] 올해 반감기의 특징에 대해서는 2024년 2월 16일자 코빗 뉴스레터 참조

[22] 양자 이론(Quantum Theory)은 물리학의 한 분야로, 원자와 아원자(subatomic particles, 원자보다 작은 크기의 입자) 입자의 행동을 설명한다. 이 이론은 에너지가 불연속적인 단위(양자)로 존재하며, 입자가 파동의 성질도 가질 수 있음을 제안한다. 주요 개념에는 양자 상태, 파동 함수, 불확정성 원리, 양자 얽힘 등이 포함된다. 이를 통해 전통적인 고전 물리학으로 설명할 수 없는 미시적 세계의 현상을 이해할 수 있다. 주요 인물로는 막스 플랑크, 알버트 아인슈타인, 닐스 보어 등이 있다.

노트북이나 스마트폰과 같은 고전적인 컴퓨팅 기술에서는 데이터가 2진수 상태로 처리되어야 한다. 이는 컴퓨터 코드로 0 또는 1로 표현되며, 10억 분의 1초 만에 상태(state)를 전환할 수 있지만 얼마나 빨리 상태를 전환할 수 있는지에 대해서는 물리적인 한계가 존재한다. 하지만 양자 컴퓨팅에서는 이론적으로 데이터가 동시에 여러 상태로 존재할 수 있으므로 처리 능력과 속도가 엄청나게 향상될 수 있고, 컴퓨터가 다수의 작업을 순차적으로 수행하지 않고 동시에 수행할 수 있게 된다.

처리 능력이 비약적으로 발전할 것이라는 점에서 양자 컴퓨터가 현재의 암호화 기술을 무용지물로 만들 것이라는 의견도 많다. 양자 컴퓨터에 영향을 받을 수 있는 기술 중에는 비트코인 네트워크에서 프라이빗 키 정보를 암호화하는 알고리즘인 SHA-256 알고리즘도 포함된다. 그래서 양자 컴퓨팅이 결국 비트코인을 무너뜨릴 것이라는 주장이 지난 몇 년 동안 설득력을 얻기도 했다.

양자 컴퓨팅이 비트코인에 어떤 영향을 미칠지 구체적으로 살펴보기 전에 먼저 양자 컴퓨팅이 아직 초기 단계에 있다는 점을 인식해야 한다. 초기 버전의 양자 컴퓨터가 몇 가지 존재하지만, 현재의 암호화 기술을 위협할 만한 양자 컴퓨터는 아직 없다. 오늘날의 양자 컴퓨터는 매우 제한된 일부 작업만 수행할 수 있다.

그렇다면 미래의 어느 시점에 비트코인의 암호화 알고리즘을 깰 수 있을 만큼 강력한 양자 컴퓨터가 개발된다고 가정해 보자. Onramp Invest[23]에 따르면 이론적으로 양자 컴퓨팅은 프라이빗 키의 보안에 잠재적인 위협이 될 수 있다고 한다. 비트코인에는 퍼블릭 키와 프라이빗 키가 있으며, 퍼블릭 키는 누구나 볼 수 있지만 프라이빗 키는 소유자만 알 수 있다. 프라이빗 키를 통해 소유자는 해당 주소의 비트코인에 접근하고 이를 제어할 수 있다. 고유 문자열인 프라이빗 키에 함수 처리를 해서 퍼블릭 키를 추출하고, 퍼블릭 키를 재가공해서 비트코인 '지갑 주소'를 만들어 내는데, 고성능 양자 컴퓨터가 개발되면 지갑 주소나 퍼블릭 키에서 프라이빗 키를 역산해 내는 것이 가능해진다는 것이다.

이론적으로 고전적 컴퓨팅에서도 지갑 주소나 퍼블릭 키를 통해 프라이빗 키를 알아낼 수 있지만, 이는 천문학적 시간이 소요된다. 그러나 양자 컴퓨팅이 발전하면 이 시간을 대폭 단축할 수 있다. 이로 인해 비트코인 지갑 주소만으로 지갑 안에 들어 있는 비트코인을 훔치는 것이 이론적으로 가능해질 수 있다.

그러나 이는 개인 지갑 보안에 대한 이론적 위협일 뿐, 누가 무엇을 소유했는지에 대한 역사적 기록을 유지하는 기본 원장은 손상되지 않고

[23] Onramp Invest, "Will Quantum Computing Break Bitcoin?"

기능할 것이다. 즉, 양자 컴퓨팅은 거래 내역을 네트워크 수준에서 직접 조작하거나 네트워크의 운영 자체를 방해할 수는 없다.

또한 양자 컴퓨팅 기술이 발전한다는 것은 악의적 행위자에게만 유리한 것이 아니다. 그 시간 동안 보안기술도 함께 발전하기 때문이다. 양자 컴퓨팅이 현실적 위협이 된다면 비트코인 개발자는 양자 컴퓨팅이 지갑과 네트워크에 위협이 되지 않도록 시스템을 업그레이드할 것이다. 실제로 비트코인의 "양자 저항성(quantum resistance)"을 높일 수 있는 방법이 이미 개발 중이다.

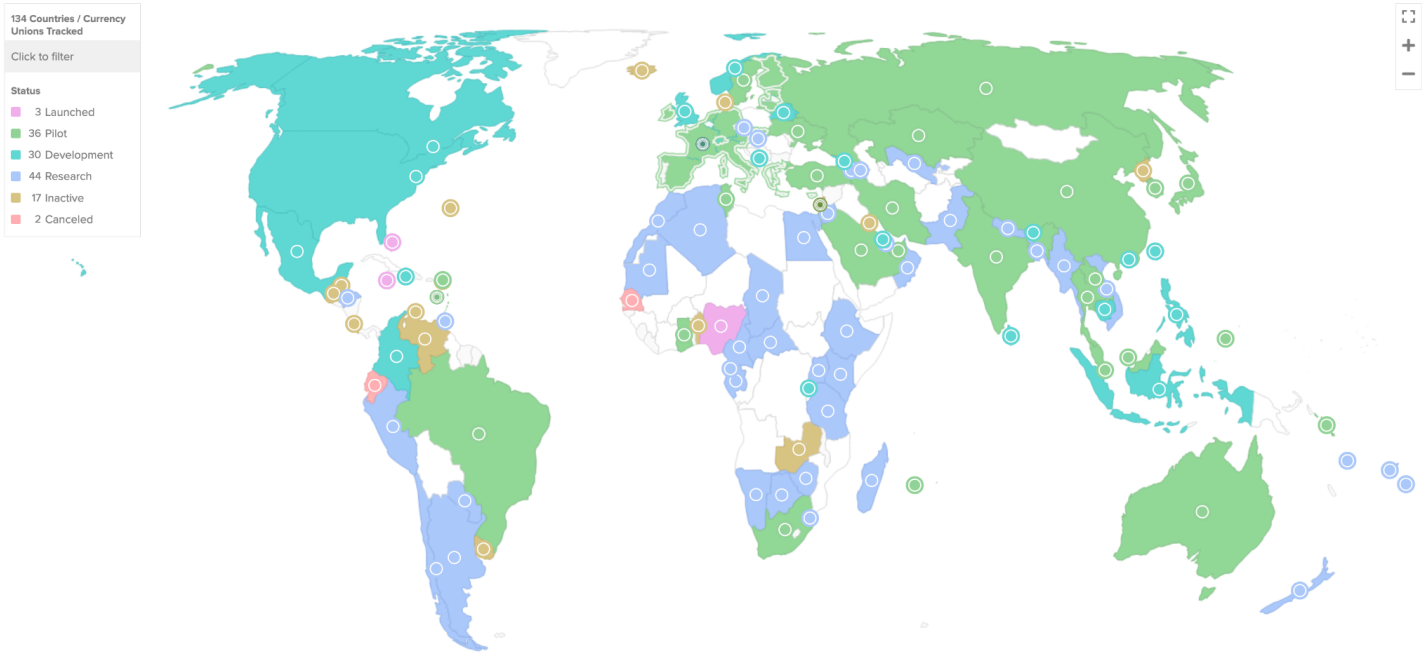
더 나아가 양자 컴퓨팅의 보안 위협은은 가상자산만의 문제가 아니다. 내일 당장 고성능 양자 컴퓨팅이 해킹에 이용된다면 이 세상 모든 디지털 시스템이 위험에 처하게 될 것이다. 은행 인프라, 전력망, 통신 플랫폼, 심지어 인터넷까지 모두 취약해질 것이다. 이러한 맥락에서 보면 양자 컴퓨팅이 발전하면 비트코인만 취약해진다는 논리는 비약이라고 볼 수 있다.

양자 혁신은 오랜 기간에 걸쳐 점진적으로 발전할 가능성이 훨씬 더 높기 때문에 대응책을 개발할 수 있는 기회가 있을 것이다. 비트코인 아키텍처의 장점은 시스템이 이전 버전과 호환되는 방식으로 업그레이드할 수 있도록 설계되었다는 것이다. 새로운 보안 이슈가 식별되고 발견됨에 따라 비트코인은 시대에 맞춰 계속 적응해 나갈 것이다. 새로운 위협이 등장하면 새로운 방어 수단도 등장할 것이다.

9. CBDC가 가상자산을 대체할 것이다?

전 세계의 많은 중앙은행이 결제 시스템에 대한 접근성을 높이기 위한 방법으로 중앙은행 디지털 화폐(CBDC)의 잠재력을 탐구하고 있다. 대부분의 CBDC 프로젝트는 아직 실험 단계에 있지만(Figure 10), 일각에서는 블록체인의 편리함과 중앙은행의 전폭적인 신뢰와 지원을 결합한 CBDC가 기존 가상자산을 쓸모없게 만들 것이라고 주장하기도 한다.

Figure 10: CBDC 프로젝트 진행 상황(2024년 5월 기준) 출처: Atlantic Council



실제로 CBDC는 금융 포용성, 결제 시스템의 경쟁, 금융의 토큰화 등 각 국가가 우선시하는 목표에 따라 개발이 된다. 가상자산과 마찬가지로 CBDC는 금융 접근성을 개선하고 비용을 줄일 수 있다.

그렇다고 해서 CBDC와 가상자산이 서로 대체 가능하다는 의미는 아니다. 오늘날 다양한 통화와 결제 수단이 공존하는 것처럼, 미래에는 가상자산과 CBDC가 공존할 수도 있다[24]. 예를 들어 싱가포르와 호주처럼 CBDC 프로젝트가 활발히 진행되고 있는 일부 국가에서는 스테이블코인이 전통 금융을 더욱 효율적으로 만들 수 있다는 가능성을 동시에 강조하기도 한다.

무엇보다 중요한 것은 비트코인과 같은 가상자산이 부분적으로는 전통금융시장의 여러 문제에 대응하기 위해 발명되었지만, 오늘날 그 목적과 잠재력은 금융 간소화 이상으로 확장되었다는 점이다. 가상자산과 블록체인의 사용 사례는 아직 초기 단계이지만 빠르게 성장하고 있는 웹3 분야를 포함하여 계속 증가하고 있고, 이 분야는 CBDC가 대체하기 어려운 부분이라고 생각한다.

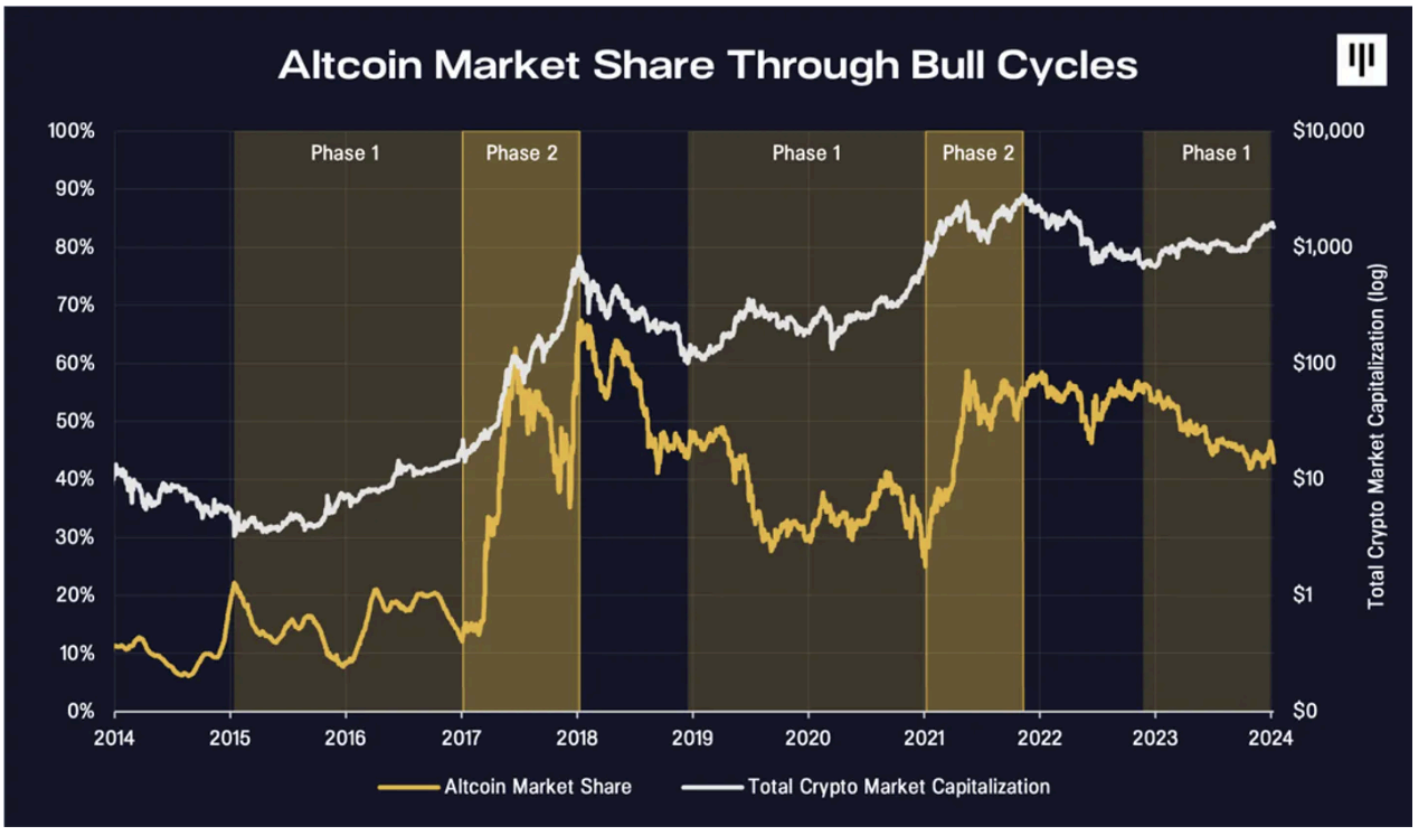
10. 알트코인 불장은 무조건 온다?

과거 가상자산 상승 사이클에서는 비트코인 가격이 큰 폭으로 오르고 나면 이더리움, 솔라나 같은 메이저 알트코인이 뒤따라 상승하고, 그 다음에 소규모 코인들이 상승하는 패턴이 자주 관찰되었다(Figure 11). 과연 올해는 어떨까?

[24] Chainalysis, “The Chainalysis Crypto Myth Busting Report”, July 2023.

Figure 11: 과거 가상자산 상승 사이클

출처: Pantera Capital (Phase 1은 랠리의 초기 단계, 즉 비트코인이 알트코인보다 가격 상승폭이 높은 시기를 말하고, Phase 2는 알트코인이 비트코인보다 더 나은 성과를 내는 후기 단계를 말한다.)



과거 패턴 때문에 시장에서는 올해 알트코인 불장이 일어날 것이라는 기대가 높은 것 같다. 하지만 올해 상승 사이클에서는 아직까지 과거에 관측되었던 패턴이 나타나지 않고 있다. 오히려 비트코인 가격을 알트코인 가격이 추종하는 모습이 지배적이다.

알트코인 상승이 저조한 이유는[25] 표면적으로는 비트코인 가격을 부양한 자금이 증시에서 유입된 자금이기 때문에 다른 자산으로의 전이 효과가 약했을 수 있다고 한다. 또한 연초에 비트코인 가격이 상승했던 주된 이유 중 하나가 현물 ETF 승인에 따른 가상자산 시장으로의 기관 자금 유입이었던 점을 감안하면 기관 자금의 알트코인에 대한 수요는 이전 대비 적을 수 밖에 없다. 알트코인 불장이 아직 도래하지 않은 데는 SEC의 증권성 논란도 큰 영향을 미쳤다고 한다. 리플 소송, 코인베이스나 바이낸스 같은 거래소와 SEC 간의 법적 분쟁에서 증권성 이슈가 문제가 되다 보니 가상자산 업체나 자본의 활동이 제한되는 것이다.

이러한 이유로 이전 사이클과 달리 이번 상승 사이클에서는 아직까지 비트코인 외 다른 알트코인의 상승세가 미미했던 것 같다. 이 시점에서 중요한

[25] 이외에 증권성 이슈가 알트코인에 미칠 수 있는 영향에 대해서는 김민승 센터장의 "'그 코인 상폐된다더라'…지라시에 널뛰는 한국 가상자산 시장 [한경 코알라]" 기고문(2024.06.26) 참조.

것은 알트코인 불장의 도래 여부를 논하기보다 현재 가상자산 시장의 구조적 변화와 규제 환경의 변화를 이해하고 대비하는 것이다. 기관 자금의 흐름, SEC의 규제 방향, 그리고 시장 내 주요 사건들이 알트코인에 미치는 영향을 분석하여 장기적인 전략을 세우는 것이 더 중요하다.

시사점

시장에 대한 잘못된 믿음이나 통념은 허위 또는 과장된 뉴스, 오해의 소지가 있는 발언, 특정 자산 또는 시장 전반에 대한 근거 없는 소문 유포 등 다양한 형태로 발생할 수 있다. 이는 투자자들의 시장 행동에 영향을 미칠 수 있고 심할 경우 패닉 셀링을 유발할 수도 있다. 특히 요즘같이 시장의 방향성을 가늠하기 어려운 상황에서는 FUD(Fear, Uncertainty, Doubt)가 미치는 영향이 더욱 커질 수 있다. 연준의 금리 인하, 미국 대선 등 모든 것이 불확실하다 보니 막연한 상황이 불안이 되고 가격이 조정을 받는 현상이 지속되고 있는 것이다. 이러한 상황에서 올바른 투자 결정을 위해서는 시장에서 신뢰할 수 있는 출처의 정보를 확인하는 것이 필요하다.

작성자

최윤영 | Yoonyoung Choy

2022년 코빗 입사. (現)코빗 리서치센터장.
(前)삼성경제연구소, 하나금융경영연구소, 서울대 증권금융연구소 근무. 서울대 경영학 박사(Finance 전공). 미시간 대학교, 스미스여대 졸업.

김민승 | Min Seung Kim

2021년 코빗 입사. (現)코빗 리서치센터장.
블록체인과 가상자산 생태계에서 벌어지는 복잡한 사건과 개념을 쉽게 풀어 알리고, 다른 관점을 가진 사람들이 서로를 이해하도록 돕는다. 블록체인 프로젝트 전략 기획, 소프트웨어 개발 등의 경력 보유.