

비트코인의 모든 것



홍성욱 (디지털 자산)
02)768-7657
songukhong@nhqv.com



김연애 (부동산/디지털 자산)
02)768-7426
fruitism@nhqv.com



“비트코인의 기본 특징부터 투자에 이르기엔 필요한 질문을 하나씩 다루어보았습니다”

“각국 중앙은행의 긴축으로 디지털 자산시장 전반에 가격 변동성이 높아진 가운데 비트코인부터 다시 돌아볼 시점”



CONTENTS

I. 비트코인의 역사와 개념	/ 6
II. 비트코인 네트워크의 꽃, Proof-of-Work	/ 15
III. 블록체인 Trilemma로 본 비트코인의 특징	/ 22
IV. 비트코인을 둘러싼 쟁점들	
1. 비트코인을 법정화폐로 도입하는 국가들 등장	/ 32
2. 비트코인과 ESG, 과연 전력난과 기후위기의 공범일까	/ 39
3. 비트코인 투자 접근법과 걸림돌	/ 47
4. 비트코인 밸류에이션 난제	/ 62

I. 비트코인의 역사와 개념

- 비트코인 첫번째 블록은 2009년 1월 3일에 생성되었음. 분산 원장 기반 블록체인 기술을 활용하므로 중앙화된 주체 없이도 거래 확인 가능. 비트코인은 블록 생성과 채굴 과정에 SHA-256 해시 알고리즘을 활용하며, 생태계 주요 구성원은 원장을 기록하고 관리하는 노드(node)와 블록을 생성하는 채굴자(miner). 금과 자주 비교되며, 교환 수단이자 가치의 척도로 쓰여온 금과 유사한 역할을 비트코인도 수행하고 있다고 믿기 때문

II. 비트코인 네트워크의 꽃, Proof-of-Work

- 작업증명(Proof-of-Work) 합의 방식에 의한 채굴은 비트코인 블록을 생성하고 비트코인 네트워크의 보안을 강화하며 새로운 비트코인이 시장에 등장하는 통로. 채굴에 성공해서 블록을 생성할 경우 블록당 일정량의 신규 비트코인과 해당 블록에 포함되는 거래 수수료를 보상으로 받음. 비트코인 채굴자들은 전용 장비를 통해 비트코인을 채굴하며, 통제 가능한 변수 중 전력 비용이 채굴 사업 수익성에 가장 영향력을 미치는 바 저렴한 전력 사용이 중요

III. 블록체인 Trilemma로 본 비트코인의 특징

- **탈중앙화**: 설립자가 자취를 감췄으며 오픈소스 프로젝트와 같은 거버넌스 형태를 보이고 있음. 채굴자의 경우 과거 중국 집중도가 높았으나 현재 미국 등지로 다변화. 대다수의 비트코인을 소수가 보유하고 있는 점은 비판을 받기도 하지만, 이는 할당된 것이 아니라 초기부터 채굴 한 결과
- **보안**: 디지털 자산 해킹 관련 뉴스플로우가 많지만, 비트코인 네트워크 등 주요 디지털 자산을 해킹하는 것은 현실적으로 어려움. 비트코인 네트워크를 해킹하기 위해서는 전체 해시레이트(hash rate, 연산력)의 과반인 51%가 필요. 해킹 사례들은 대부분 부주의로 인해 비밀번호 격인 개인 키(private key)가 노출되며 발생
- **확장성**: 비트코인은 초당 거래 수(transaction per second)가 7회 이하로 느리며 네트워크 혼잡 시 거래 수수료도 상승. 비트코인의 탈중앙화와 보안을 위해 라이트닝 네트워크라는 확장성 솔루션 활용 중. 이를 통해 비트코인의 약점으로 꼽히는 느린 속도 개선 시 일상에서의 소액결제도 용이해질 수 있음

IV. 비트코인을 둘러싼 쟁점들

- **비트코인을 법정화폐로 도입하는 국가들 등장:** 엘살바도르와 중앙아프리카공화국이 비트코인을 법정화폐로 채택. 엘살바도르는 비트코인을 법정화폐로 도입한지 1년이 되어가지만 일상에서 쓰이기까진 시간이 필요할 것으로 보임. 최근 하이퍼인플레이션을 경험 중인 신흥국들이 이슈가 되고 있으며, 자국 통화 없이 달러를 대신 사용하는 국가들도 많은 만큼 비트코인을 법정화폐로 채택하는 정부가 추가로 등장할 수 있음. 비트코인을 결제수단으로 받아들이는 기업이 늘어나고 있으며 미국에서는 일부 주들이 비트코인으로 납세를 가능하게 하는 등 제도 변화도 나타남
- **비트코인과 ESG, 과연 전력난과 기후위기의 공범일까:** 비트코인이 불필요하게 많은 전력을 소비한다는 비판이 있음. 비판하는 입장은 네덜란드보다 소비 전력량이 많다는 등의 근거를 제시. 그러나 기타 주요 산업이나 제품에 비하면 아직 소비 전력량은 작음. 또한 이동성과 채굴 중단/재개의 유연성이 높기 때문에 전력 확보를 위해 경쟁하지 않으며 버려지거나 수요가 낮은 전력을 찾아서 이동 가능. 특히 신재생에너지 발전시설로부터 수요가 낮은 시간대의 전력을 구매해주는 수요자로서 신재생 인프라 확대에도 기여한다는 주장 존재. 신재생에너지에서 나온 전력으로만 채굴하는 비트코인 채굴 기업을 통해 ESG에 대한 불확실성 완화 가능
- **비트코인 투자 접근법과 걸림돌:** 현재 비트코인은 나스닥 및 금과 가격 상관관계가 높아진 상황임에 따라 자산 포트폴리오 편입을 서두를 필요는 없다는 판단. 인플레이션 헤지 기능의 경우, 비트코인 탄생 이후 첫 고물가 국면에서 저조한 성과를 거둔 점은 유의할 필요. ‘글로벌 교환수단이 되기 위한 성장 과정에 있는 자산’으로서 성장 자산의 성격이 강하다는 판단
- 다만 비트코인 투자에 있어 수탁, 회계 처리, 과세 등은 불확실성으로 작용. 투자 접근성을 높여줄 수 있는 비트코인 현물 ETF의 미국 출시는 미뤄지고 있음. 미국 기준으로 비트코인 선물 및 비트코인 선물 ETF는 출시된 상황이며, 비트코인 현물 ETF는 캐나다 등 일부 국가에서만 출시된 상황. 미국과 같은 주요 시장에 비트코인 현물 ETF가 출시된다면 자금 유입에 기여할 것으로 보이나, 미국 증권거래위원회의 입장으로 볼 때 승인까지 시간이 필요할 것
- **비트코인 밸류에이션 난제:** 비트코인 가격은 크고 작은 낙폭에도 꾸준히 우상향해왔음. 반감기 시점마다 비트코인 가격은 상승 궤적을 보여왔지만 반감기로 인한 가격 상승 효과는 작아지고 있으며 다음 반감기 이후 가격 급등 가능성은 미지수. 대표적인 비트코인 밸류에이션 방식으로 금 시가총액 대비 비중이 자주 회자되지만, 방식은 다양하며 각의 단점 존재. 비트코인 네트워크를 ‘화폐 플랫폼’에 비유할 경우 DAU(일간활성사용자) 지표와 유사한 일간 활성 주소(Active Address) 수를 핵심 펀더멘털 지표로 간주 가능. 장기적으로 비트코인 네트워크의 가치는 활성 주소 수와 동행할 가능성 존재

디지털 자산

비트코인의 모든 것

- I. 비트코인 역사와 개념

비트코인의 시작

- 나카모토 사토시는 2007년부터 비트코인 관련 작업을 시작해, 2008년 bitcoin.org 도메인을 등록하고 백서(Bitcoin: A Peer-to-Peer Electronic Cash System)를 작성. 2009년 1월 3일 비트코인 블록체인의 첫 블록(genesis block, block 0)을 만들었으며 며칠 후 비트코인 네트워크가 작동하기 시작
- 나카모토 사토시는 백서에 중앙은행 및 금융시스템에 대한 의견을 언급하지 않았으나, 비트코인의 첫 블록에 ‘The Times 03/Jan/2009 Chancellor on brink of second bailout for banks’ 라는 신문 기사 제목을 입력해넣음

비트코인 백서: 비트코인을 P2P 전자화폐 시스템으로 정의

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

자료: Bitcoin: A Peer-to-Peer Electronic Cash System, NH투자증권 리서치본부

첫 블록에 아래 내용을 입력해넣음

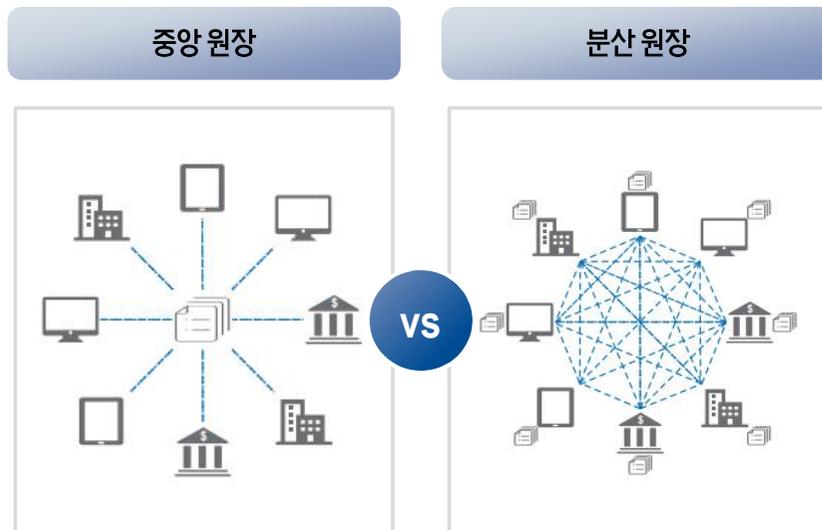


자료: thetimes03jan2009.com, NH투자증권 리서치본부

비트코인과 블록체인의 기술의 특성

- 비트코인이 채택하고 있는 블록체인 기술은 분산 원장(distributed ledger) 기반으로 중앙화된 주체 없이도 송금과 거래 확인을 가능하게 함. 같은 버전의 원장(장부)을 다수가 보유하고 수정되는 경우 모두가 확인하는 방식
- 은행 없이도 계좌(주소)에 해당하는 공개키(public key)와 비밀번호에 해당하는 개인 키(private key) 생성 가능
- 탈중앙화 이외에도 편리한 송금, 중앙화된 금융 주체의 임의 조치 불가, 위변조 불가, 자금 흐름 투명성 등의 특성 보유

블록체인 기술은 분산 원장 기반



자료: BIS, NH투자증권 리서치본부

비트코인 블록체인의 특성



자료: NH투자증권 리서치본부

암호학(Cryptography)과의 관계

- 디지털 자산은 영어로 통상 Cryptocurrency(암호화폐)라고 부르는데, 이는 블록체인이 암호학(Cryptography)에 기반하기 때문
- 비트코인은 SHA-256 해시 알고리즘을 사용해 신규 블록에 넣을 데이터를 고정된 형식의 해시값으로 변환. 비트코인의 작업증명(Proof-of-Work) 채굴 경쟁에도 원하는 해시값이 나올 때까지 해시 알고리즘에 입력값을 입력하는 과정 수반됨

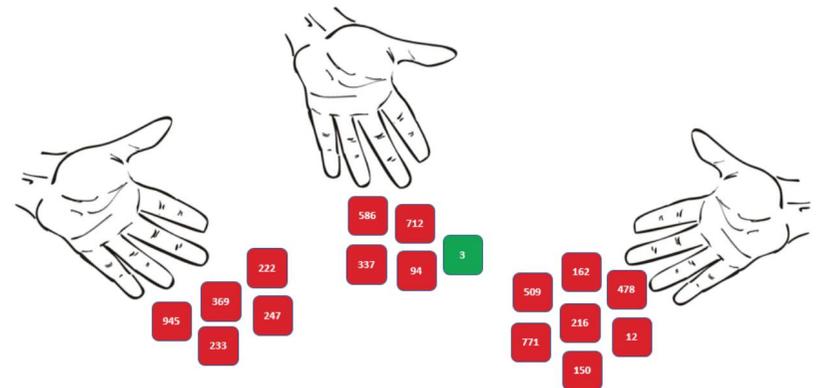
디지털 자산은 암호학에 기반: 비트코인은 SHA-256 사용



자료: NH투자증권 리서치본부

채굴 경쟁은 주사위를 반복해서 굴리는 경쟁에 비유 가능

“난이도가 ‘10’일 경우, 10 이하의 숫자를 먼저 굴리는 사람이 승리”
 “승리 확률을 높이는 법은 주사위를 더 빨리 더 많이 굴리는 것”
 “참가자 수나 주사위를 굴리는 속도에 상관 없이
 평균 문제해결 시간이 10분이 되도록 난이도 조정”

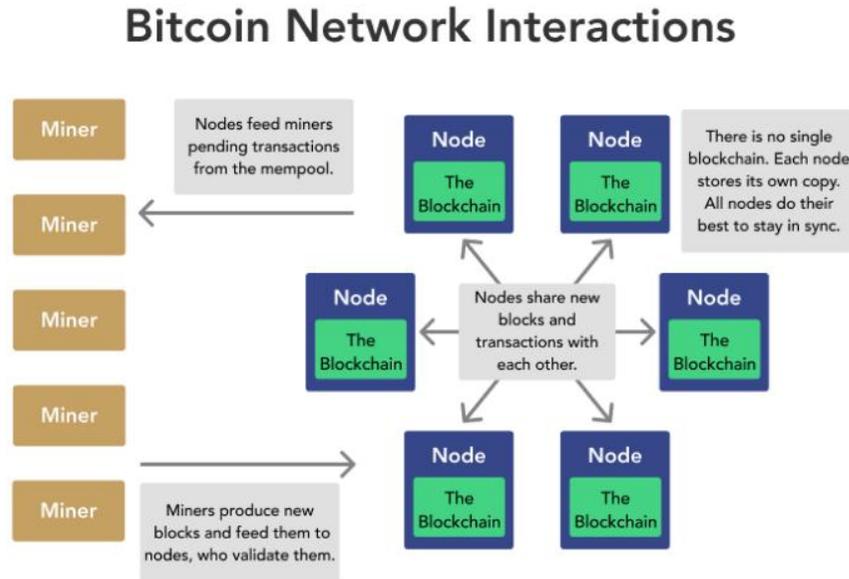


주: 블록이 평균적으로 10분에 하나씩 생성되도록 채굴 난이도는 2016블록(약 2주)마다 변경
 자료: Braiins, NH투자증권 리서치본부 정리

생태계 구성원: 노드(node), 채굴자(miner)

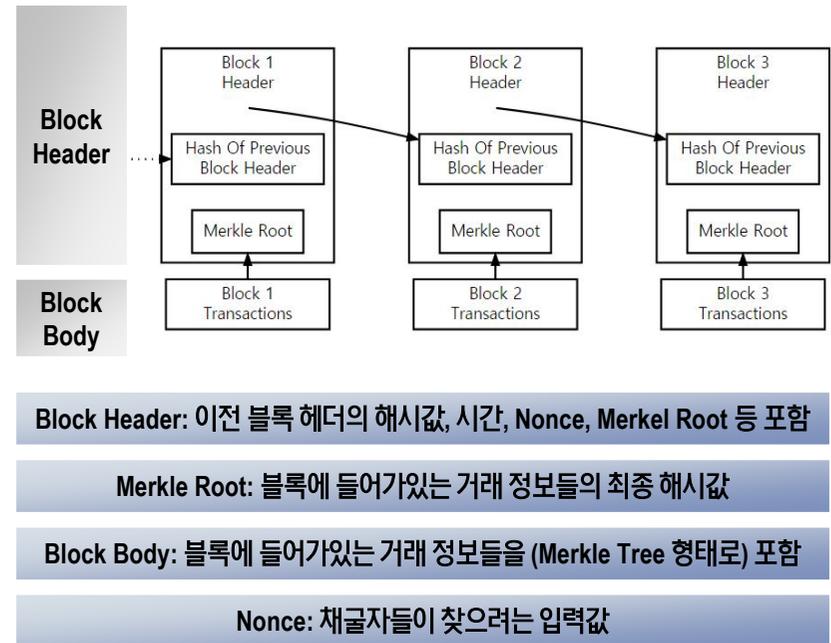
- 채굴(mining)은 새로운 블록을 생성하는 과정. 블록을 생성할 권한을 앞서 설명한 퍼즐을 해결하는 것으로 결정. 채굴자(miner)는 보조금 개념으로 블록당 일정량의 비트코인을 보상으로 받으며 퍼즐을 풀기 위해 사용하는 해시레이트(hash rate, 연산력)는 비트코인 네트워크의 보안을 강화
- 노드(node)는 모든 거래의 기록(원장)을 관리하고 새로운 블록을 검증. 네트워크 안정성 확보를 위해서는 충분한 수의 노드 필요. 노드 운영 시 직접적인 보상은 없지만 타인에 의존하지 않는 비트코인 블록체인 무결성 검증 및 네트워크 안정성에의 기여 가능

비트코인 생태계 구성원인 노드와 채굴자



자료: River Financial, NH투자증권 리서치본부

비트코인 블록체인 도식화



자료: bitcoin.org, ResearchGate, NH투자증권 리서치본부

비트코인의 거버넌스

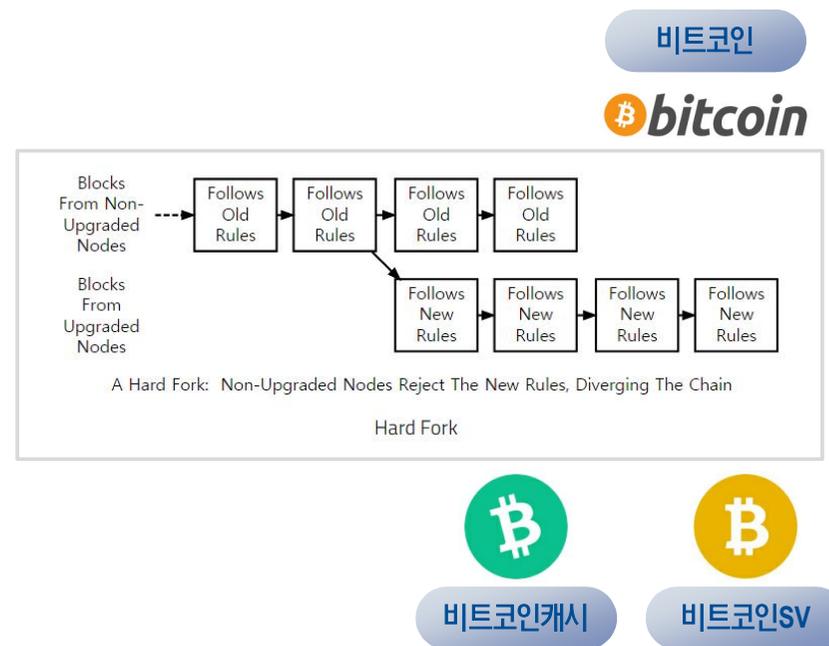
- 비트코인은 오픈소스 프로젝트로 상주 개발자가 없으며 무급으로 개발에 참여하거나 기업이나 학계 등의 후원을 받는 구조
- 개선방안을 적용할 때 Bitcoin Improvement Proposal(BIP)을 개발자가 제시. 이는 peer review, 테스트 등을 통해 커뮤니티 다수의 동의를 획득. BIP를 적용한 새로운 버전의 Bitcoin Core를 노드들이 설치함으로써 적용 완료. 의사결정 반영에 긴 시간이 필요
- 비트코인 개발 방향에 합의하지 못할 경우 하드포크(hard fork, 블록체인의 분리)가 발생할 수 있으며 비트코인캐시와 비트코인SV가 그 대표적인 예

주요 개발자 리스트: 비트코인 개발은 무급이거나 후원에 의존

Bitcoin Core contributors		
(Ordered by number of commits)		
Wladimir J. van der Laan (7361)	MarcoFalke (5276)	fanquake (2113)
Pieter Wuille (2013)	hebasto (1159)	gavinandresen (1101)
jnewbery (788)	achow101 (784)	jonasschnelli (772)
practicalswift (715)	Cory Fields (608)	jonatack (583)

자료: bitcoin.org, NH투자증권 리서치본부

합의에 실패할 때 하드포크 발생



자료: bitcoin.org, 각 재단, NH투자증권 리서치본부

이더리움과의 비교: 성격이 다른 자산

- 비트코인과 이더리움은 시가총액 1위, 2위 디지털 자산으로 자주 비교됨. 비트코인이 화폐 시스템을 표방하며 탄생했다면 이더리움은 스마트 계약(Smart Contract)을 실행할 수 있는 월드 컴퓨터를 지향
- 모두 블록체인 기술을 활용한 자산이나 성격은 서로 다르며 이더리움의 머지(Merge) 이후에는 합의 방식도 달라지게 됨. 시장이 디지털 자산에 대해 익숙해질수록 둘 간의 가격 상관관계도 낮아질 수 있음

비트코인과 이더리움 비교

	비트코인	이더리움
네트워크 출범	2009년	2015년
설립자	나카모토 사토시	비탈릭 부테린 등
비전	탈중앙화 화폐 시스템	프로그래밍 가능한 범용 블록체인 / 마켓플레이스 / 앱스토어
스마트컨트랙트 유무	없음	있음
다양한 토큰 호스팅	불가능	가능
통화 정책	총 발행량 2,100만개로 고정	발행량 제한 없음
탈중앙화 정도	매우 탈중앙화됨	상대적으로 중앙화됨
합의 방식	작업증명 (Proof-of-Work)	작업증명 (Proof-of-Work) (지분증명으로 변경될 예정)
채굴 보상	블록당 보상, 거래 수수료	거래 수수료

주: 지분증명 전환 이전 기준

자료: Cointelegraph, Ethereum.org, Kraken, NH투자증권 리서치본부

금과 끊임없이 비교되는 비트코인

- 비트코인은 초창기부터 금에 비유됨. 역사적으로 금이 교환수단이자 가치의 척도로 쓰여왔으며 비트코인의 역사가 짧지만 디지털 세상에서 비트코인이 금과 유사한 역할을 수행하고 있다고 믿는 사람들이 증가
- 금은 역사가 오래되어 외환보유고에 포함되며, 귀금속 수요와 산업 수요가 있다는 특징을 지님. 비트코인의 경우, 이동이 편리하며 진위 확인이 용이함. 비트코인이 일상에 더 많이 쓰인다면 결제 용이성이 금 대비 장점이 될 수 있음

금과의 비교: 비트코인은 금과 유사성이 존재하지만 다른 점도 많음

	발행량	이동편의성	산업 수요	귀금속 수요	작은 단위로 나눌 수 있는지	상호대체 가능성 (fungibility)	변동성	내구성	진위 확인 용이성	검열 및 간섭 가능성	외환보유고 활용 여부	물건 구매 가능 여부
비트코인	한정	높음	없음	없음	가능	가능	매우 높음	내구성 저하 없음	높음	낮음	아니오	비교적 어려움
금	한정 (채굴 속도 불규칙)	낮음	중간	높음	대체로 가능	대체로 가능	높음	사실상 내구성 저하 없음	보통	보통	예	어려움
다이아몬드	한정적이거나, 인공적으로 생성 가능	낮음	낮음	높음	불가능	대체로 불가능	높음	보관 유의 필요	보통	보통	아니오	어려움
달러	무한정	비교적 높음	-	-	가능	가능	낮음	내구성 저하 없음	비교적 높음	높음	예	쉬움

자료: NH투자증권 리서치본부

담보로서의 비트코인

- 비트코인은 이미 디지털 자산 대출 플랫폼에서 담보자산으로 활용되고 있음
- 전통 금융권의 경우 담보가치에 대한 심사가 까다로우나 지난 4월 Goldman Sachs가 Coinbase에 처음으로 비트코인 담보 달러 대출을 실행. 구체적인 조건은 공개되지 않았으나, 이는 전통 금융권의 비트코인 수용성을 높이는 계기로 작용할 수 있음

Goldman Sachs는 Coinbase에 비트코인 담보 대출 실행

Bloomberg
Asia Edition

Sign In | Subscribe | Search

• Live Now | Markets | Technology | Politics | **Wealth** | Pursuits | Opinion | Businessweek | Equality | Green | CityLab | Crypto | More

Wealth
Crypto

Goldman Offers Its First Bitcoin-Backed Loan in Crypto Push

- Secured lending facility lent cash collateralized by Bitcoin
- Move comes as Wall Street warms up to digital assets

Photographer: Angel Garcia/Bloomberg

By Yueqi Yang
2022년 4월 29일 오전 4:42 GMT+9
From **Crypto**

Most Read

- Markets: US Inflation Quickens to 9.1%, Amping Up Fed Pressure to Go Big
- Markets: Fed Could Weigh Historic 100 Basis-Point Hike After Inflation Scorch
- Pursuits: The 10 Worst Airports in Europe for Delays Right Now
- Markets: Euro Drops to Dollar Parity for First Time in Two Decades
- Markets: Stocks Buckle Under Hot CPI as Hawkish Bets Surge: Markets Wrap

자료: Bloomberg, NH투자증권 리서치본부

디지털 자산 업계는 이미 비트코인 담보로 각종 대출 진행 중

See How Much You Can Borrow

Enter the amount you'd like to borrow to find out how much collateral is required.

Credit Amount: \$10,000 USD

Collateral Required: 0.99434879 BTC (50% LTV)

Start Borrowing >

How it works

- Choose what to borrow**
You can borrow as much as 40% of the value of the Bitcoin in your account, up to \$1,000,000¹.
- Get your cash**
Using your bank account or PayPal, get access to your borrowed cash quickly with no fees.
- Make monthly payments**
Each month you only need to pay the interest due (\$10 min). Pay off the balance when you're ready. Additional terms apply⁴.
- Your Bitcoin stays safe**
The Bitcoin you use as collateral remains safely held by Coinbase. It's not lent out or used for any other purpose.

자료: Nexo, Coinbase, NH투자증권 리서치본부

디지털 자산

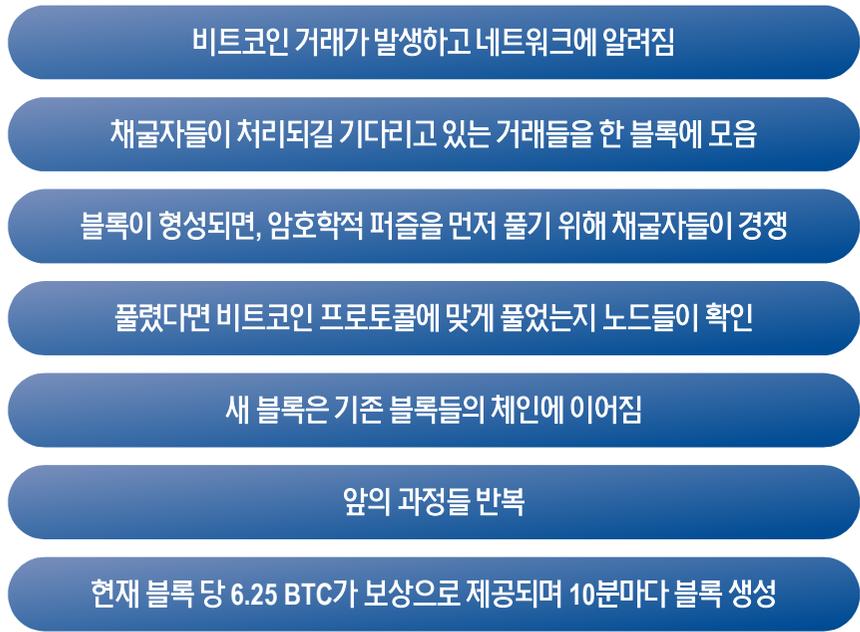
비트코인의 모든 것

- II. 비트코인 네트워크의 꽃, Proof-of-Work

비트코인의 꽃, Proof-of-Work

- 채굴은 비트코인 생태계를 지지하는 엔진과 같은 역할을 함. 채굴은 비트코인 거래를 처리하고 비트코인 블록체인의 보안을 강화하며 새로운 비트코인이 시장에 등장하게 되는 통로. 채굴자는 채굴 전용 기기를 동원해서 비트코인을 채굴
- 작업증명(Proof-of-Work)이란 블록체인 네트워크가 합의에 이르는 방식을 연산(Work)에 기반해서 정한다는 뜻

비트코인 채굴 과정 단계



자료: Marathon Digital, NH투자증권 리서치본부

합의 방식 간의 차이 분명. 작업증명이 보다 오래 검증된 방식

	작업증명 (Proof-of-Work)	지분증명 (Proof-of-Stake)
블록 생성 권한 결정 방식	연산력	지분
탈중앙화	높음	중간*
보안	높음	중간*
에너지 소모	많음	작음
속도(확장성)	느림	빠름
보상	블록당 보상 + 수수료	수수료

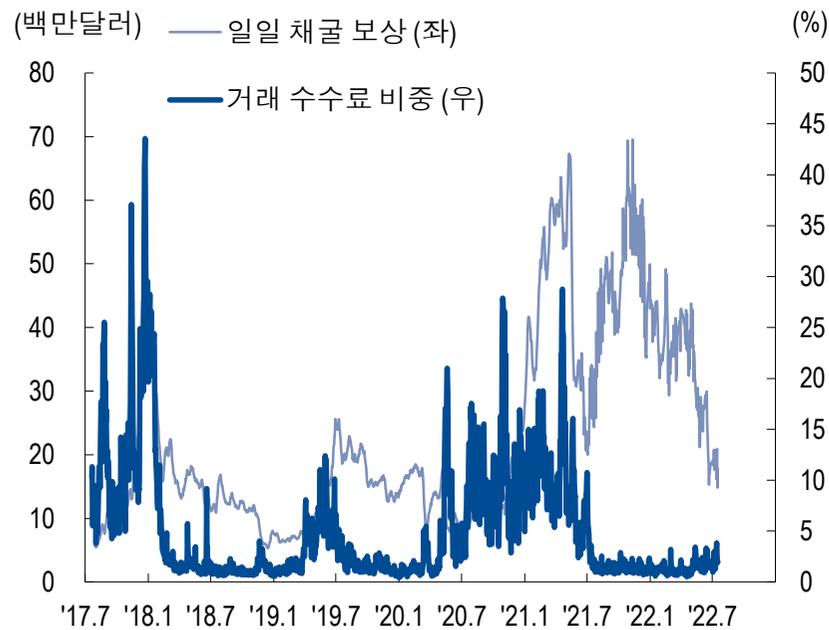
주: 지분증명도 탈중앙화가 높고 보안이 우수하다는 의견이 있지만 작업증명보다 역사가 짧고 보다 상세한 검증이 필요하다는 의견도 있음

자료: edChain, Qtum, NH투자증권 리서치본부

채굴에 대한 보상 개념으로 지급되는 비트코인

- 비트코인은 비트코인 네트워크를 의미하지만 비트코인을 세는 단위로도 쓰임. 비트코인의 단위 표시는 BTC로 하며, 가장 작은 단위 1SAT(satoshi)는 0.00000001BTC를 의미하고 현재 원화로 0.3원 수준
- 채굴에 성공해 블록을 생성할 경우, 블록당 일정 수준의 비트코인(현재 6.25 BTC)과 그 블록에 포함되는 거래 수수료(비트코인)를 보상으로 지급받게 됨

비트코인 보상: 블록당 보상 및 거래 수수료로 구성



주: 달러 환산 수치
 자료: Messari, NH투자증권 리서치본부

비트코인 단위 표시

단위명	단위 표시	크기
bitcoin	BTC	1 BTC
deci-bitcoin	dBTC	0.1 BTC
centi-bitcoin	cBTC	0.01 BTC
milli-bitcoin	mBTC	0.001 BTC
micro-bitcoin	μBTC	0.000001 BTC
satoshi	SAT	0.00000001 BTC

자료: Wikipedia, NH투자증권 리서치본부

보상 없이도 블록체인 운영이 가능할까

- 탈중앙화된 블록체인이 작동하려면 다수의 주체가 자발적으로 블록체인 운영에 참여할 유인이 있어야 하며 이를 위해 채굴에 대한 보상을 제공하게 됨. 비트코인 네트워크는 퍼블릭 블록체인 네트워크로 분류됨
- 완전한 탈중앙화를 목표로 하지 않는 블록체인(기업형 블록체인 등)의 경우, 블록체인을 운영할 소수 주체들을 직접 선정해 절충적으로 운영할 수 있음

다양한 블록체인 예시

퍼블릭 블록체인 네트워크 (Public blockchain networks)

퍼블릭 블록체인은 누구든지 신청하여 참여할 수 있는 블록체인(예: 비트코인). 상당한 컴퓨팅 파워의 필요성, 트랜잭션에 대한 프라이버시의 부족 혹은 부재 그리고 보안 취약성 등을 문제점으로 들 수 있음

프라이빗 블록체인 네트워크 (Private blockchain networks)

퍼블릭 블록체인 네트워크와 유사한 프라이빗 블록체인 네트워크는 분산형 P2P 네트워크. 그러나 한 업체가 네트워크를 관리하고 참여가 허용되는 자를 통제하여 합의 프로토콜을 실행하고 공유 원장을 유지 보수

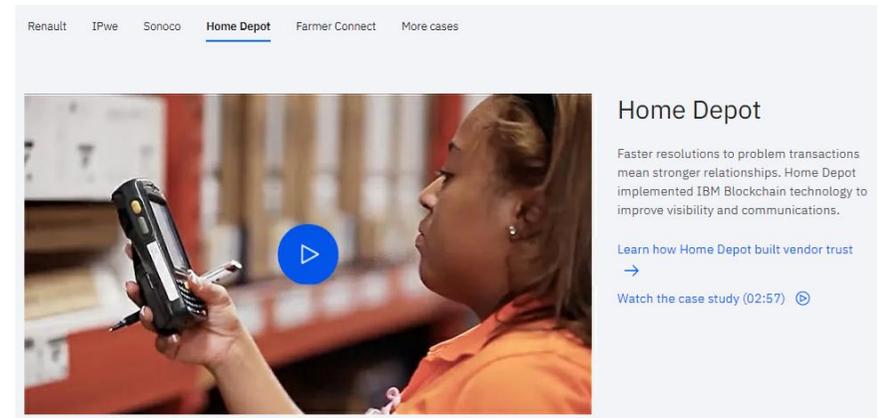
허가형 블록체인 네트워크 (Permissioned blockchain networks)

프라이빗 블록체인을 설정하는 기업들은 일반적으로 허가형 블록체인 네트워크를 설정. 퍼블릭 블록체인 네트워크 역시 허가형이 될 수 있음. 이는 네트워크 및 특정 트랜잭션에 참여할 수 있는 사용자를 제한

컨소시엄 블록체인 (Consortium blockchains)

여러 조직들이 블록체인을 유지보수 하는 책임을 공유할 수 있음. 이 사전 신청된 조직들은 트랜잭션을 제출 하거나 데이터에 액세스할 수 있는 사용자를 판별

기업형 블록체인 사례: 공급망 관리 등에 활용됨



자료: IBM, NH투자증권 리서치본부

자료: IBM, NH투자증권 리서치본부

비트코인의 Proof-of-Work 왕좌는 굳건

- 작업증명 자산 중 비트코인의 점유율 1위 지위는 굳건. 이더리움이 지분증명에 성공한다면 작업증명 자산으로서 비트코인의 희소성이 부각될 수 있을 것으로 기대. 작업증명 네트워크의 가치는 해시레이트의 크기와 상관관계가 높음
- 이더리움이 지분증명으로 전환하려는 이유는 작업증명의 전력 사용량 이슈와 확장성 개선을 위한 것. 작업증명 지지자들은 디지털 자산에서 핵심이 되는 탈중앙화에는 작업증명이 우월하며, 지분증명은 보다 상세한 검증이 필요하다고 주장

주요 작업증명 디지털 자산 목록

	가격 (달러)	시가총액 (십억달러)	해시 알고리즘	참고사항
비트코인	23,774	454.2	SHA-256	-
이더리움	1,699	207.3	Ethash	지분증명 전환 예정
도지코인	0.07	9.3	Scrypt	지분증명 전환 예정
이더리움클래식	40.80	5.5	Etchash	-
라이트코인	61.38	4.3	Scrypt	-
모네로	157.85	2.8	CryptoNight	-
비트코인캐시	148.50	2.8	SHA-256	-
비트코인SV	63.46	1.2	SHA-256	-

자료: Coinmarketcap, NH투자증권 리서치본부

왜 이더리움과 도지코인은 지분증명으로 전환하려고 할까?



자료: 각 재단, NH투자증권 리서치본부

디지털 자산별로 상이한 채굴 장비

- 채굴장비의 경우 디지털 자산의 해시 알고리즘에 따라 다름. 맞춤형 장비인 ASIC(Application Specific Integrated Circuit)이 가장 효율적이지만, 이더리움과 같이 해시 알고리즘에 의해 ASIC으로 채굴할 수 없는 디지털 자산도 있음
- 일반 PC에 쓰이는 CPU와 GPU로도 비트코인 채굴 가능. 하지만 채굴 경쟁이 점차 심화되어 비트코인을 CPU와 GPU로 채굴하는 것은 매우 비효율적(효율은 ASIC > GPU > CPU 순)

최신 비트코인 채굴 장비. 가격은 5,940달러



주: 가격은 2022.07.15 기준
자료: Bitmain, NH투자증권 리서치본부

작업증명 디지털 자산별 채굴장비

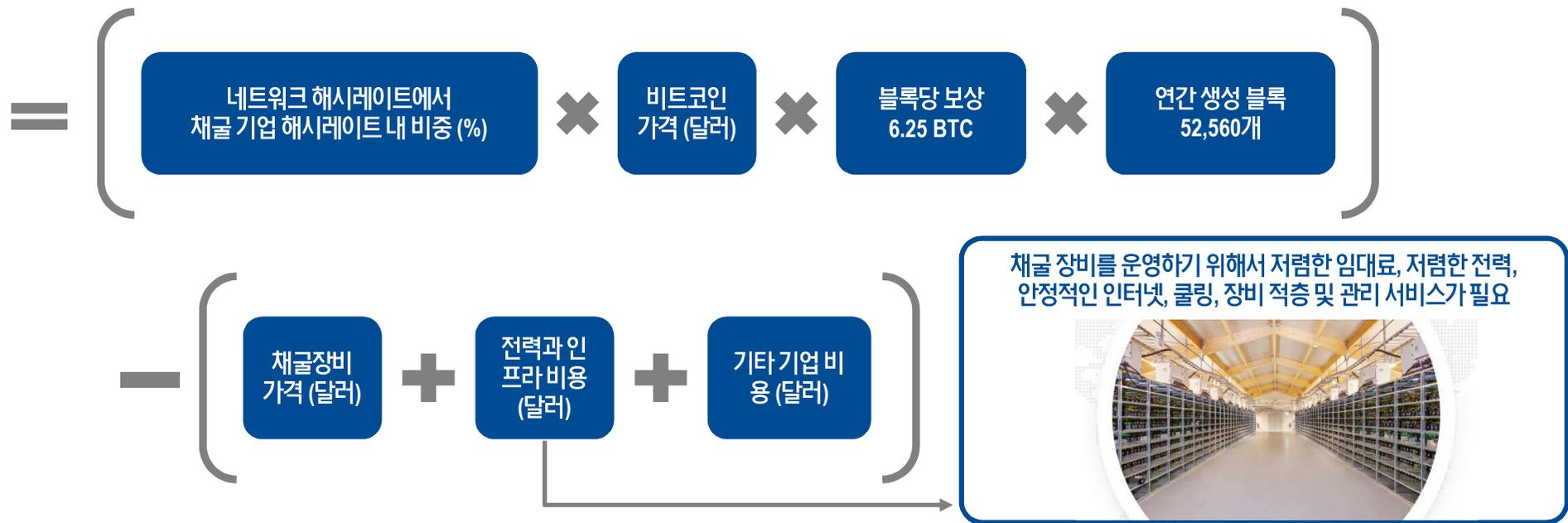
종목	해시 알고리즘	채굴 장비 예시	분류
비트코인	SHA-256	Bitmain Antminer S19 Pro	ASIC
이더리움	Ethash	Nvidia GeForce RTX 3090	GPU
도지코인	Scrypt	Bitmain Antminer L7	ASIC
라이트코인	Scrypt	Bitmain Antminer L7	ASIC

주: 이더리움과 도지코인은 지분증명으로 전환될 예정
자료: Bitmain, Nvidia, NH투자증권 리서치본부

비트코인 채굴 업체의 비즈니스 모델은? 저렴한 전기 찾기 싸움

- 채굴 업체들의 수익성은 비트코인 가격 등 외부 변수와 전력 비용 등 자체 변수에 의해 결정. 채굴 장비 등의 인프라를 직접 운영하는 경우 Vertically Integrated 모델, 채굴 호스팅 서비스를 이용하는 경우 Asset Light 모델이라 부름
- 채굴 업체가 수익성을 개선하기 위해 통제할 수 있는 핵심 비용은 전력. 원자재 채굴 장비들과 달리 비트코인 채굴 장비들은 이동이 용이하기 때문에 버려지는 전력이나 저렴한 전력을 찾기 위해서 발전 시설 근처로 이동하는 것이 가능. 원자재 채굴 장비와 달리 전력이 비싼 시간대에 채굴을 중단하고 저렴해지면 즉각 채굴을 재개하는 것도 가능

비트코인 채굴 업체의 연간 이익 계산방법



주: 채굴 장비 가격도 통상 비트코인 가격에 따라 변동
 자료: Marathon Digital Holdings, Compass Mining, NH투자증권 리서치본부

디지털 자산

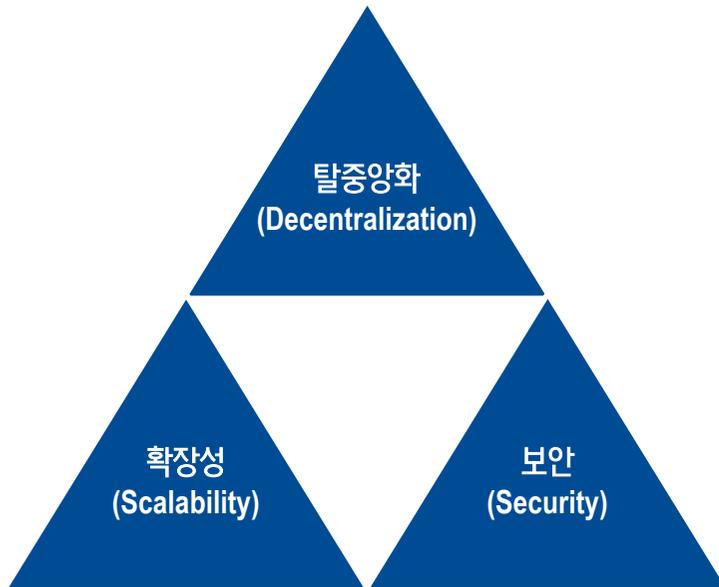
비트코인의 모든 것

- III. 블록체인 Trilemma로 본 비트코인의 특징

블록체인 자산들의 Trilemma

- 블록체인의 디지털 자산들은 탈중앙화, 확장성, 보안이라는 세 가지 특성 중 최소한 하나를 포기할 수밖에 없는 Trilemma를 가지고 있음. 각 디지털 자산별로 추구하는 비전에 따라 타협점이 정해짐
- 탈중앙화는 권력의 분산 정도, 확장성은 블록체인 네트워크가 처리하는 업무가 증가할 때 속도가 유지되는 정도, 보안은 블록체인 네트워크가 외부 공격으로부터 안전한 정도를 나타냄

블록체인 자산들의 Trilemma



자료: NH투자증권 리서치본부

디지털 자산별 상대 비교

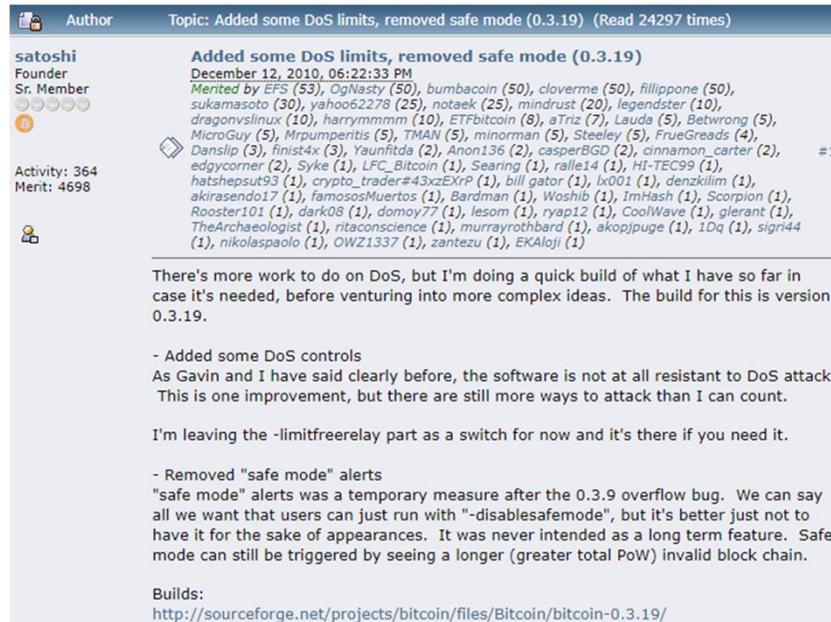
종목명	탈중앙화	확장성	보안
비트코인 (BTC)	상	하	상
이더리움 (ETH)	중	하	상
리플 (XRP)	하	상	중

주: 이더리움 지분증명 전환 이전 기준
 자료: NH투자증권 리서치본부

탈중앙화: 리더십과 보유 상황

- 비트코인 설립자는 표면상 자취를 감췄으며, 설립자가 전면에 나서서 프로젝트를 지휘하지 않는다는 점은 탈중앙화에 기여
- 소수의 계좌가 상당량의 비트코인을 보유하고 있기 때문에 보유 측면에서의 다변화는 다소 미흡. 나카모토 사토시는 약 100만 BTC를 보유했을 것으로 추정. 다만, 이는 개발자들이나 초기 지지자에 ‘할당’ 된 것이 아니라, 그들이 채굴을 일찍 시작한 것에 따른 보상 결과

사토시는 2010년 12월 마지막 이메일 이후 자취를 감춤



자료: bitcointalk.org, NH투자증권 리서치본부

비트코인의 보유자는 다변화되어있지 못함

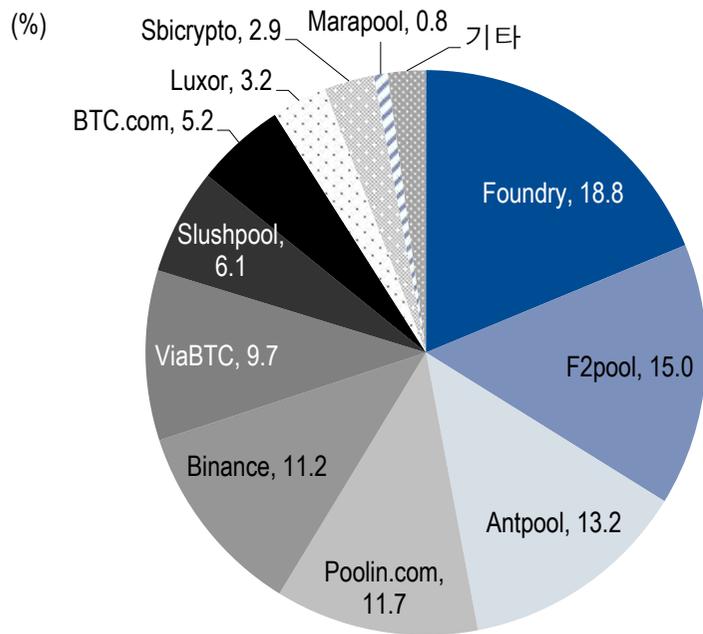
계좌 크기	계좌 백분위	계좌 수	보유 비트코인	비트코인 누적 비중
1,000 BTC 이상	상위 0.01%	2,183	7,941,565 BTC	41.60%
100~1,000 BTC	상위 0.04%	13,692	3,854,990 BTC	61.80%
10~100 BTC	상위 0.35%	133,356	4,300,095 BTC	84.32%
1~10 BTC	상위 2.07%	734,440	1,852,107 BTC	94.03%
0.1~1 BTC	상위 8.66%	2,821,205	873,889 BTC	98.61%
0.1 BTC 이하	-	6,775,190	266,205 BTC	100.00%

주: 2022.07.11 기준
 자료: BitInfoCharts, NH투자증권 리서치본부

탈중앙화: 채굴의 탈중앙화

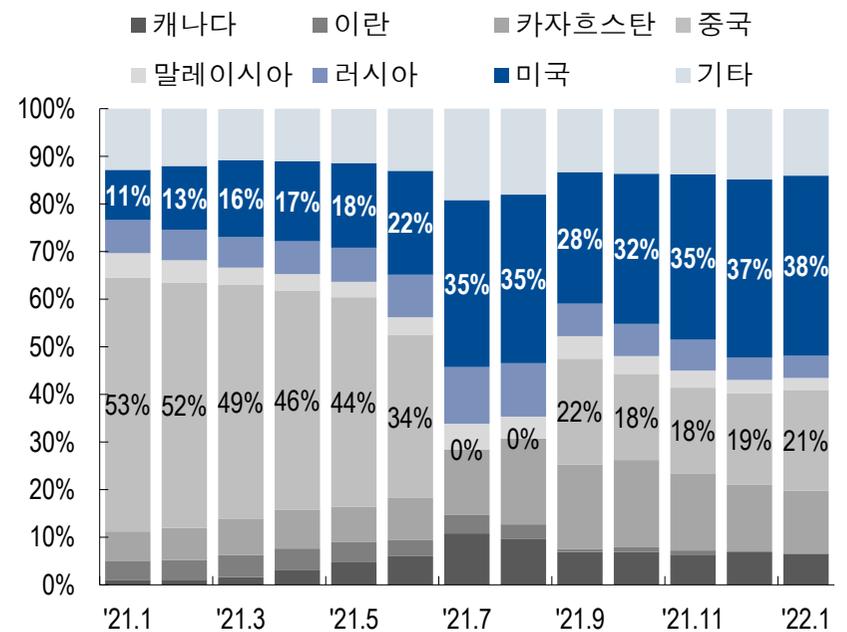
- 과거 중국의 해시레이트 비중이 높았으나, 2021년 중국 정부가 디지털 자산 채굴을 금지하면서 비중이 크게 축소. 이후 미국이 비트코인 채굴 주도권을 가져왔으며 텍사스 등 신재생에너지 발전량이 많고 제도가 우호적인 곳에서 채굴 활발
- 마이닝풀(mining pool, 연산력을 모아 채굴 확률을 높이는 채굴자의 모임) 기준으로 본다면 일부 지역/기관 비중이 높아 보이나 마이닝풀은 느슨한 연합체 개념으로 볼 수 있음

마이닝풀별 해시레이트 비중



주: 2022.05.15 기준
 자료: Marathon Digital Holdings, NH투자증권 리서치본부

국가별 해시레이트 비중

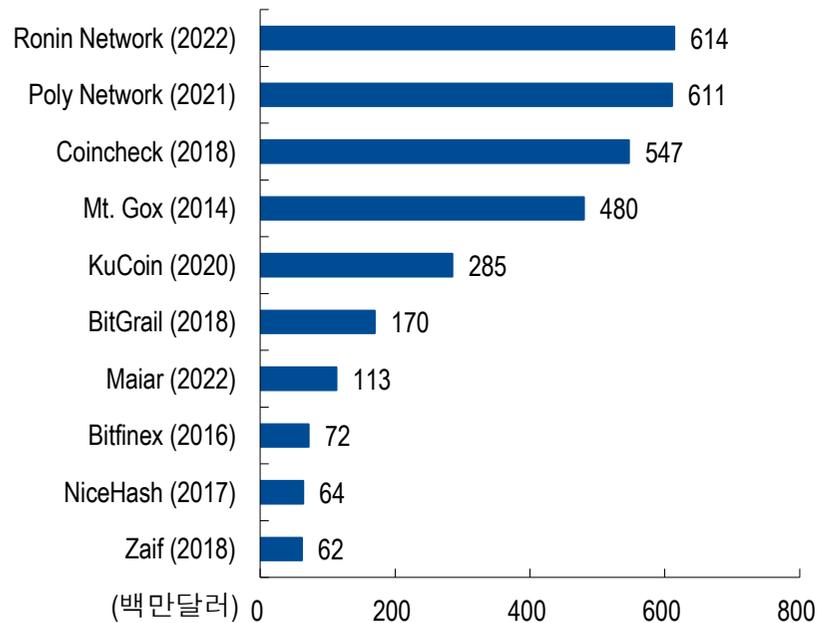


주: 2021년 6월 중국 정부는 디지털 자산 채굴 금지, 2021년 9월 디지털 자산 불법화
 자료: Cambridge Centre for Alternative Finance, NH투자증권 리서치본부

보안: 해킹에 대한 오해

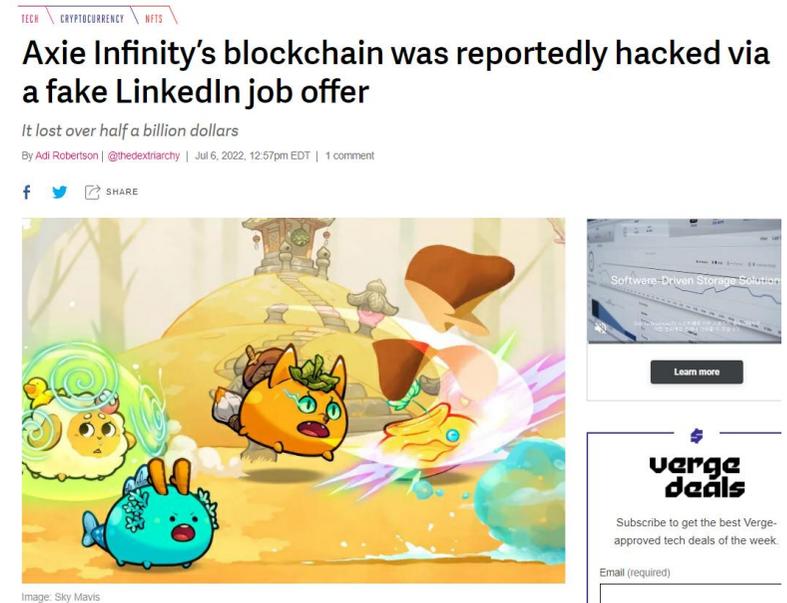
- 해킹 관련 뉴스가 많기 때문에 디지털 자산은 태생적으로 해킹에 취약하다는 인식이 있으나, 비트코인 네트워크는 해킹된 적 없으며 주요 네트워크의 해킹 사례는 드뭄. 블록체인 네트워크를 직접 해킹하는 것은 매우 어려움
- 최근 디스코드(SNS) 등을 통한 해킹이 성행하고 있음. 피싱(phishing)과 유사하며 상대의 실수를 노리는 경우가 대부분. 디지털 자산 최대 해킹 사건의 범인은 가짜 이직 제안을 통해 목표 대상에 심은 악성코드로 피해자의 개인 키를 빼돌린 후 이더리움과 USDC(스테이블코인)를 갈취

역대 해킹 금액 순위



주: 도난 발생 당시의 달러 표시 금액 기준
 자료: Tech Monitor, NH투자증권 리서치본부

엑시 인피니티 피싱 사건은 이직 제안을 가장한 피싱 사건이었음



자료: The Verge, NH투자증권 리서치본부

보안: '51% 공격' 에 필요한 비용은?

- 비트코인을 해킹하기 위해서는 전체 네트워크 해시레이트의 과반(51%)에 해당하는 해시레이트가 필요. 이에 필요한 비용은 비상식적으로 큼. 이더리움클래식과 비트코인SV처럼 해시레이트가 낮은 종목에 대한 공격이 성공한 사례는 있음
- 51% 공격이 성공한다면 이중지불(double-spending)이 가능. 예를 들면, ETC 공격자는 보유하고 있는 ETC를 거래소에 송금하고 ETC를 다른 자산 'XYZ' 로 바꾼 후 공격자 주소로 재송금. 이후 거래소에 ETC를 송금한 거래를 무효화. 그 결과 ETC와 'XYZ' 를 둘다 보유하게 됨

비트코인 해시레이트 증가 추이



주: EH/s(Exa Hash per second)는 초당 100경 해시를 의미
 자료: Messari, NH투자증권 리서치본부

51% 공격(51% attack)에 필요한 비용

	세부가정
전기 요금 가정	\$0.10 per kWh
사용 하드웨어 가정	제품명: Antminer S9 해시레이트: 14TH/s 사용 전력: 1375W
현재 비트코인 해시레이트	213 EH/s
필요 해시레이트	222 EH/s =현재 해시레이트 x (0.51/(1 - 0.51))
공격에 필요한 하드웨어비용	380억달러
공격에 필요한 전력비용	일 5,234만달러 (523,481,149 kWh per day)

주1: 하드웨어 대량 매입에도 하드웨어 가격이 일정하다는 가정. 기존 채굴자들이 대응하지 않는다는 가정
 주2: 2022.07.26 기준
 자료: GoBitcoin.io, NH투자증권 리서치본부

(참고) 양자 컴퓨터로 인한 보안 붕괴는 아직 먼 얘기

- 양자 컴퓨터로 인해 비트코인의 보안이 붕괴될 것이라는 우려도 간혹 있으나 현재로서는 불가능. 양자 컴퓨터 성능이 비약적으로 개선된다면 Shor 알고리즘을 이용해 비트코인 거래에서 개인키를 추출하는 것이 가능 (이럴 경우 디지털 자산뿐만 아니라 이메일, 은행 기록 모두 위험)
- 다만, 양자 컴퓨터 성능 개선에는 10~20년이 소요될 것으로 추정. 다른 영역과 마찬가지로 비트코인 네트워크도 양자 컴퓨터에 대응(Post Quantum Cryptography)할 시간은 충분한 것으로 보임

이론적으로 Shor 알고리즘을 통한 공격에는 취약

종목명	Shor 알고리즘 (개인키 해킹 공격)	Grover 알고리즘 (채굴 공격)
비트코인 (BTC)	취약	보통
이더리움 (ETH)	취약	보통
라이트코인 (LTC)	취약	보통
모네로 (XMR)	취약	안전
ZCash (ZEC)	취약	보통

자료: ScienceDirect, NH투자증권 리서치본부

비트코인의 25%가 취약하지만 어디까지나 이론에 불과

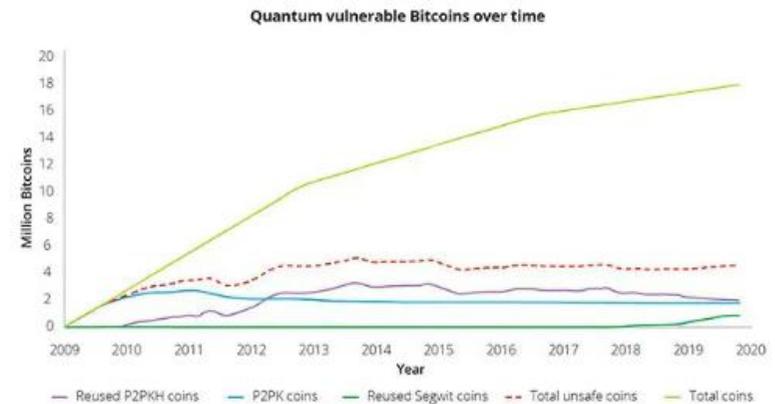


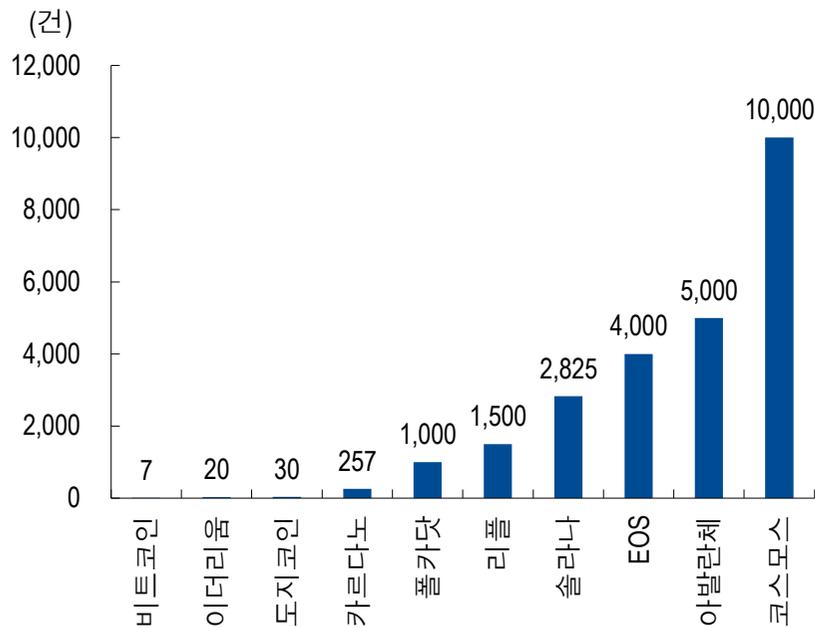
Figure 1: The distribution of Bitcoins that are stored in address that are vulnerable to quantum attacks. This graph shows that about 25% of all Bitcoins are vulnerable to a quantum attack and that there is an equal number of vulnerable p2pk and p2pkh coins. Note that reused Segwit coins are presented in the graph but are otherwise not mentioned in the article.

자료: Deloitte, NH투자증권 리서치본부

확장성: 가장 느린 블록체인 중 하나

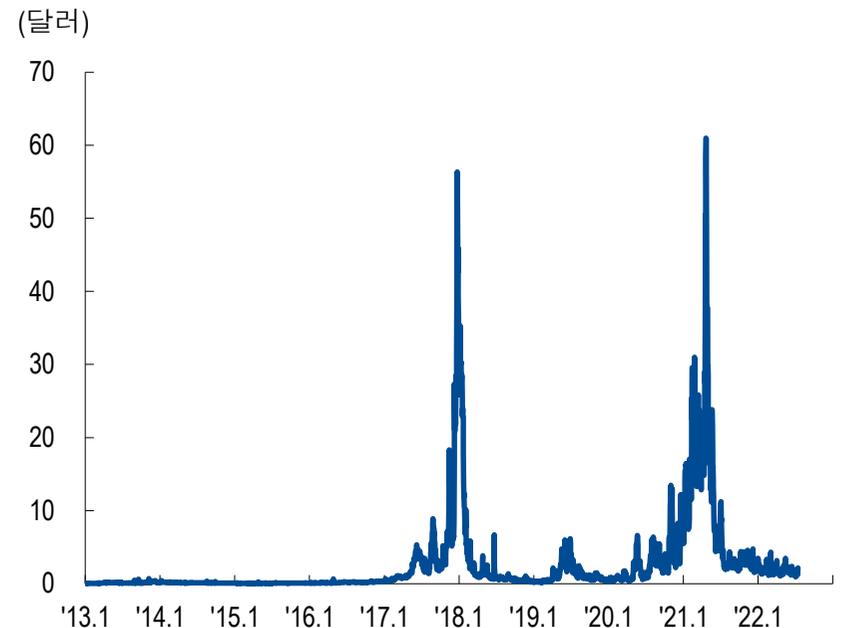
- 확장성은 TPS(transaction per second, 초당 거래 수)로 나타낼 수 있으며 네트워크가 정상 속도를 유지하면서 네트워크의 처리량이 얼마나 증가할 수 있는지를 의미. Visa와 Mastercard가 초당 2~3천건을, 페이팔이 초당 200~300건을 처리할 수 있음을 고려하면 비트코인 네트워크는 느린 편
- 또한 비트코인 거래가 증가하면 수수료를 더 지불하더라도 먼저 거래를 체결시키려는 수요가 발생해 거래 수수료가 급등할 수 있음. 거래 수수료 상승도 비트코인 사용을 저해할 수 있는 요인 중 하나

초당 거래 수: 비트코인은 가장 느린 축에 속함



주: 조사 기관마다 기준에 따라 차이 존재
 자료: Analytics Insight, NH투자증권 리서치본부

비트코인 거래 수수료: 2022년 평균은 2달러 이하

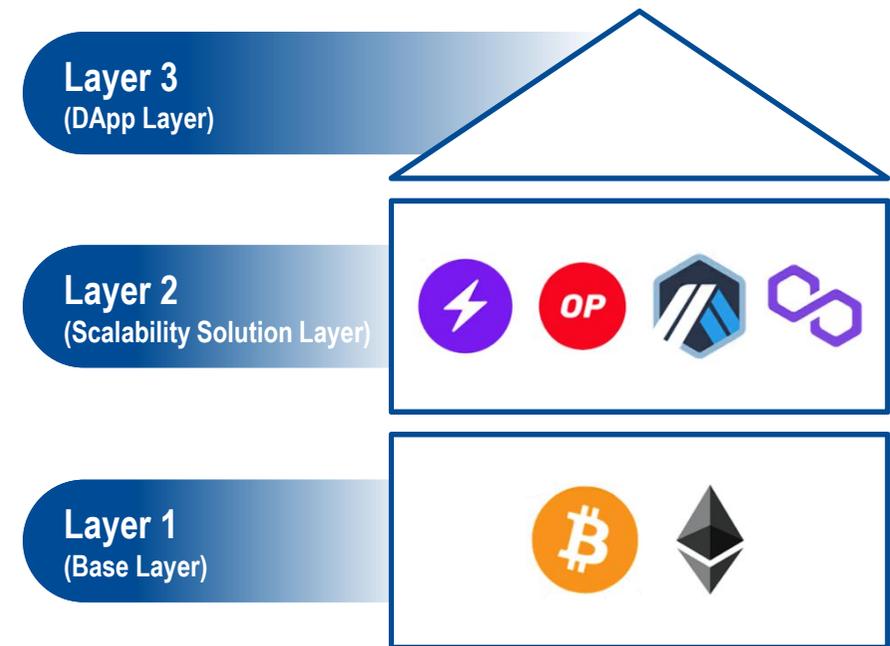


자료: Messari, NH투자증권 리서치본부

확장성: 비트코인의 속도 문제는 라이트닝 네트워크

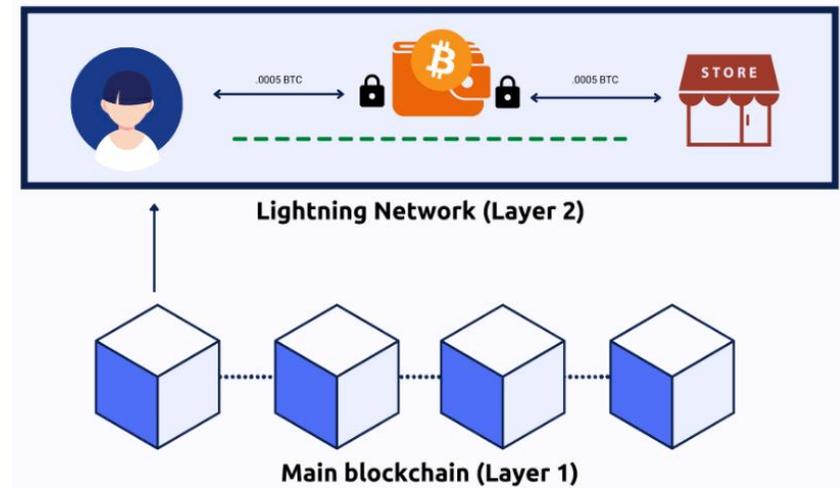
- 라이트닝 네트워크는 2018년에 베타 버전을 출시한 이후 비트코인의 확장성 문제를 해결하기 위해 노력 중. 비트코인은 초당 거래 수가 7회 이하로 매우 느리지만 라이트닝 네트워크를 사용하면 이론적으로 Visa와 Mastercard보다 빨라질 수 있음
- 오프체인(Offchain, 비트코인 블록체인을 거치지 않음)에서 채널을 열어 여러 거래들을 처리한 후 최종 결과만 비트코인 블록체인에 기록하기 때문에 속도 개선 가능. 비트코인 거래 중 소액결제들을 담당할 수 있을 것으로 기대

Layer 2란? 확장성 문제를 해결하기 위해 탄생



주: DApp은 Decentralized App의 줄임말
 자료: 각 재단 및 프로젝트, NH투자증권 리서치본부

라이트닝 네트워크는 오프체인에서 거래를 처리해 빠름



자료: Bitpay, NH투자증권 리서치본부

확장성: 라이트닝 네트워크로 소액결제에 비트코인을 사용할 수 있음

- 엘살바도르의 비트코인 법정화폐 지정, Twitter의 라이트닝 네트워크를 통한 후원 시스템 도입, Block(구 Square) Cash App의 라이트닝 네트워크 지원 등으로 라이트닝 네트워크 도입은 꾸준히 진행 중
- 중앙화나 보안 등의 문제점이 제기되고 있으나, 이를 개선하며 점차 많은 인구가 라이트닝 네트워크를 이용할 경우 소액결제 시 비트코인을 사용할 수 있는 인프라 구축 가능. 이는 비트코인 가치에도 긍정적으로 작용할 전망

라이트닝 네트워크 도입의 걸림돌

오프체인 작업에서의 중앙화에 대한 우려

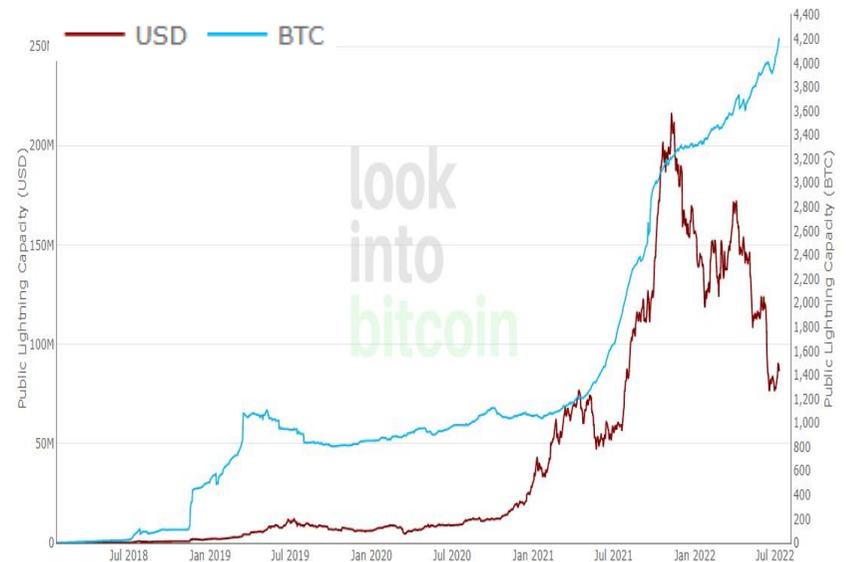
오프체인 채널 내에서 익명성이 증가함에 따라 규제 당국이 비우호적인 스탠스를 보일 가능성

속도를 위해 오프라인 작업 시 보안 수준이 저하될 수 있는 리스크

비트코인을 라이트닝 네트워크에 락업해야하는 추가적인 불편함

거래당사자들이 거래 끝까지 라이트닝 네트워크와의 연결을 유지하지 않을 경우 오류 발생할 가능성 확대

라이트닝 네트워크 용량 추이: BTC 기준으로는 꾸준히 상승



자료: NH투자증권 리서치본부

자료: Lookintobitcoin, NH투자증권 리서치본부

비트코인의 모든 것

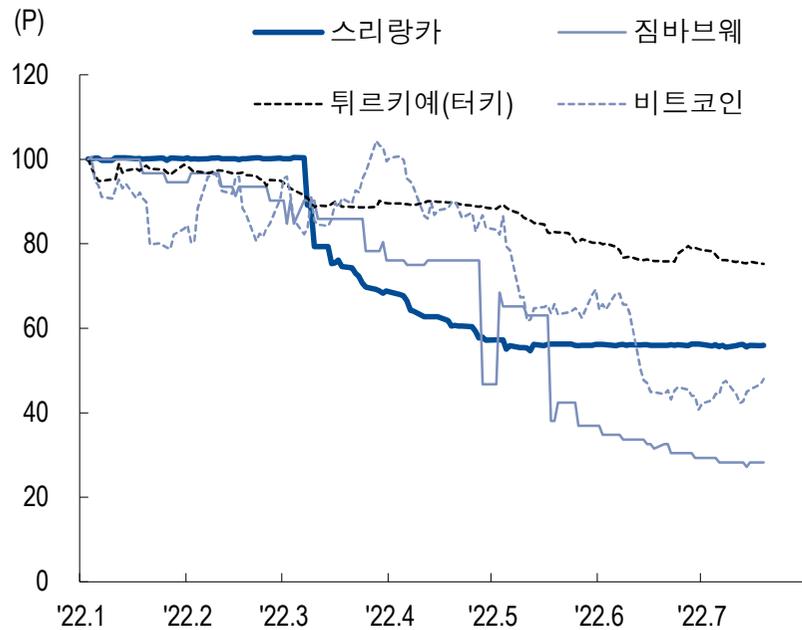
● IV. 비트코인을 둘러싼 쟁점들

- 1) 비트코인을 법정화폐로 도입하는 국가들 등장
- 2) 비트코인과 ESG, 과연 전력난과 기후위기의 공범일까
- 3) 비트코인 투자 접근법과 걸림돌
- 4) 비트코인 밸류에이션 난제

하이퍼인플레이션 통화와 비트코인

- 하이퍼인플레이션이 발생한 스리랑카, 짐바브웨, 튀르키예(터키)의 통화는 2022년 가치가 급락한 비트코인과 비교해보아도 변동성에 큰 차이가 없음. 통화정책의 실패는 신흥국 중심으로 발생하며 통화 가치를 안정적으로 유지하는 것이 쉽지 않음을 보여줌
- 세계 최초로 엘살바도르가 비트코인을 법정화폐로 채택했으며, 이에 대해 IMF는 단기적으로 비용과 리스크가 혜택보다 크기 때문에 추천하지 않는다고 밝힘

하이퍼인플레이션 발생 국가의 통화와 비트코인 비교



주: 2022.01.01 기준 100. 달러 표시 가격 추이
 자료: Bloomberg, NH투자증권 리서치본부

엘살바도르에 대한 IMF의 권고사항

Financial Stability: 은행과 기타 금융기관이 비트코인 가격 변동에 노출될 수 있음. 비트코인 익스포저를 헤지하거나 비트코인 예금을 막아야함. 결제가 Chivo(정부 e-지갑)에 집중되어있기 때문에 규제 및 감시 강화 필요

Financial Integrity: 익명성 때문에 불법자금, 테러 자금조달, 세금 회피 가능. 도난이나 사이버범죄가 금융시스템 안정 저해 가능. 비트코인 서비스 제공자(지갑 등)에 대한 국제 기준이 필요하며 보다 강하고 균일한 규제가 필요

Consumer Protection: 가격 변동성으로 가계나 기업이 부의 손실을 볼 수 있으며 사이버 범죄도 리스크. 이에 i) Chivo 등 지갑에 대한 법적 규제 강화해서 소비자 자금을 완전히 보호할 수 있도록 ii) 비트코인 거래와 보유에 대한 법적 제한을 둘 것 iii) 소비자 보호 프레임워크, 투명성 규제, 당국 개입, 비트코인 사용과 가격 변동에 의한 리스크에 대한 보다 분명한 정보 공개

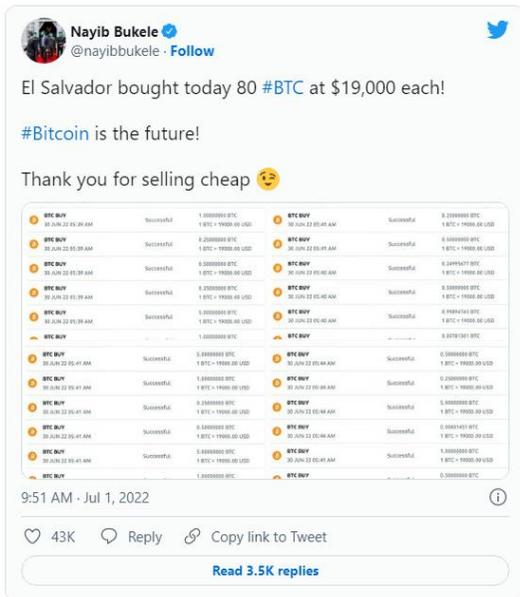
Contingent Fiscal Liabilities: 비트코인 도입은 신탁 펀드를 통해 전부 공공 재원으로 진행 중. 가격변동에도 펀드가 달러를 비트코인으로 교환해줄 수 있기 위해 기타 재원이나 차입을 통한 보충이 필요

자료: IMF, NH투자증권 리서치본부

비트코인을 법정화폐로 채택한 정부들: 자체 통화가 없다는 것이 공통점

- 엘살바도르는 2001년부터 미국 달러를 법정화폐로 사용했으며 사실상 자국 통화가 없었음. 2021년 6월 비트코인이 법정 화폐가 될 것이라고 발표했으며 같은해 9월부터 사용. 현재 약 2,301BTC(약 5,000만달러)를 보유하고 있음
- 2022년 4월 중앙아프리카공화국도 비트코인을 법정화폐로 채택. 중아공 정부가 기존에 사용하던 통화인 CFA(Cooperation financiere en Afrique centrale, 6개국 사용)는 유로에 특정 비율로 페그되어있음

엘살바도르 대통령, 정부가 비트코인을 매수했다고 트윗



자료: Twitter, NH투자증권 리서치본부

중앙아프리카공화국도 자체 통화가 없던 셈

1 Euro equals

655.66 Central African CFA franc

Jul 6, 1:26 AM UTC · Disclaimer

1 Euro Central African CFA

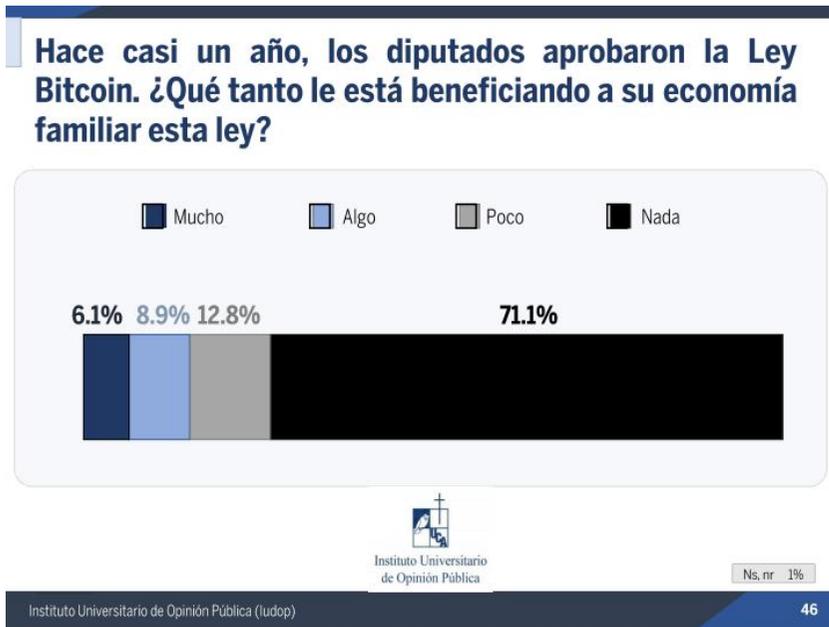


자료: Google, NH투자증권 리서치본부

엘살바도르의 비트코인 도입 현황

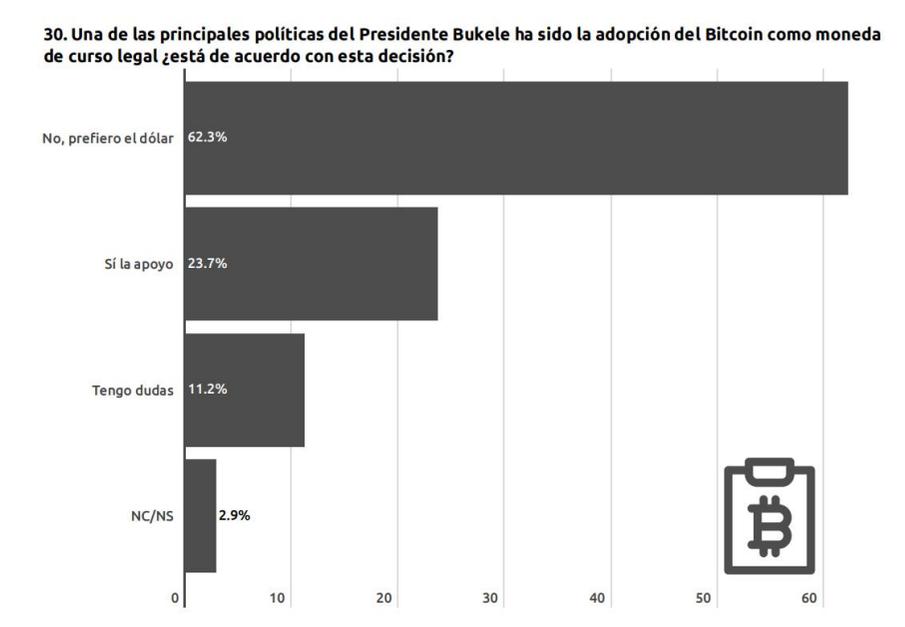
- 엘살바도르에서 비트코인을 법정화폐로 사용한지 1년이 되어가고 있으나 현지 보도에 의하면 사용 빈도가 높지 않은 것으로 파악됨. 국민 대상 설문조사 결과도 부정적
- 비트코인 법정화폐 지정이 가계에 도움이 되고 있는가: 전혀 71.1%, 조금 12.8%, 어느 정도 8.9%, 많이 6.1%
- 비트코인 도입 결정을 지지하는가: 달러가 낮다 62.3%, 지지한다 23.7%, 의문스럽다 11.2%

가계에 도움이 안된다는 의견이 71%



주1: 2022.05.14~2022.05.25 설문조사
 주2: 다만 비트코인이 하락 중이던 5월경에 실시된 설문조사임은 고려 필요
 자료: Instituto Universitario de Opinión Pública, NH투자증권 리서치본부

달러가 낮다는 의견이 62%



주1: 2022.05.11~2022.05.15 설문조사
 주2: 다만 비트코인이 하락 중이던 5월경에 실시된 설문조사임은 고려 필요
 자료: Universidad Francisco Gavidia, NH투자증권 리서치본부

법정화폐로 채택하는 국가가 추가로 등장할 가능성도 존재

- 비트코인은 은행 없이도 계좌적인 개인 주소 생성 가능. 엘살바도르는 국민 70% 이상이 은행서비스 접근성이 없으며 이는 비트코인 도입 근거. 또한 해외에서 자국으로 소득을 송금하는 규모가 연 60억달러에 달하며 비트코인 활용시 수수료 절감 가능
- 이미 자국 통화 없이 달러를 쓰고 있거나 통화정책 실패로 기존 통화가 유명무실해진 경우 비트코인이 대안으로 등장함. 추후에도 비트코인을 법정화폐로 채택하는 국가가 등장할 수 있으며 이는 비트코인 사용자 기반 확대의 주요 계기가 될 것으로 예상

‘비트코인을 법정화폐로 채택할 차기 국가는?’ 설문 결과

순위	국가명	화폐
1	파라과이	PYG
2	베네수엘라	VES
3	앙골라	XCD
4	우크라이나	UAH
5	미국	USD
6	러시아	RUB
7	짐바브웨	ZWB
8	브라질	BRL
9	파나마	PAB
10	UAE	AED
11	인도	INR
12	튀르키예	TRY
13	이란	IRR
14	베트남	VND

주: 누적 투표 순
 자료: Coinmarketcap 설문조사, NH투자증권 리서치본부

자국 화폐 없이 달러만 사용하는 국가들 다수

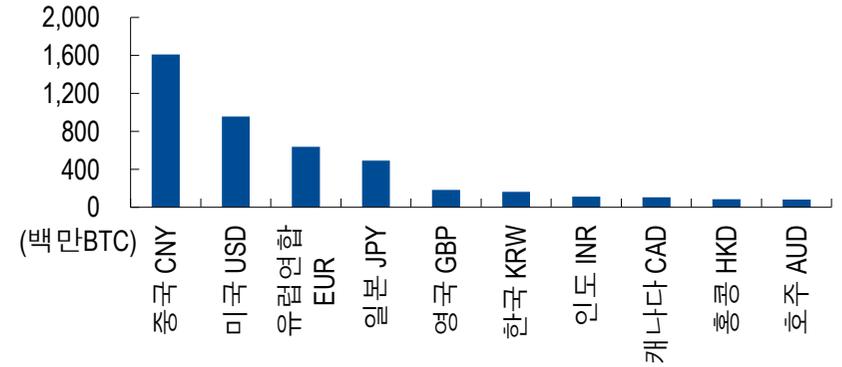
분류	국가명
자국 통화 없이 달러만 사용하는 나라	영국령 버진 아일랜드, 카리브 네덜란드, 마셜 아일랜드, 미크로네시아 연합, 팔라우, 튀르크 카이코스 제도
달러도 사용하는 나라	아르헨티나, 바하마, 바베이도스, 벨리즈, 버뮤다, 캄보디아, 코스타리카, 동티모르, 에콰도르, 엘살바도르, 아이티, 온두라스, 이라크, 레바논, 라이베리아, 파나마, 소말리아, 우루과이, 베네수엘라, 짐바브웨

자료: Wikipedia, NH투자증권 리서치본부

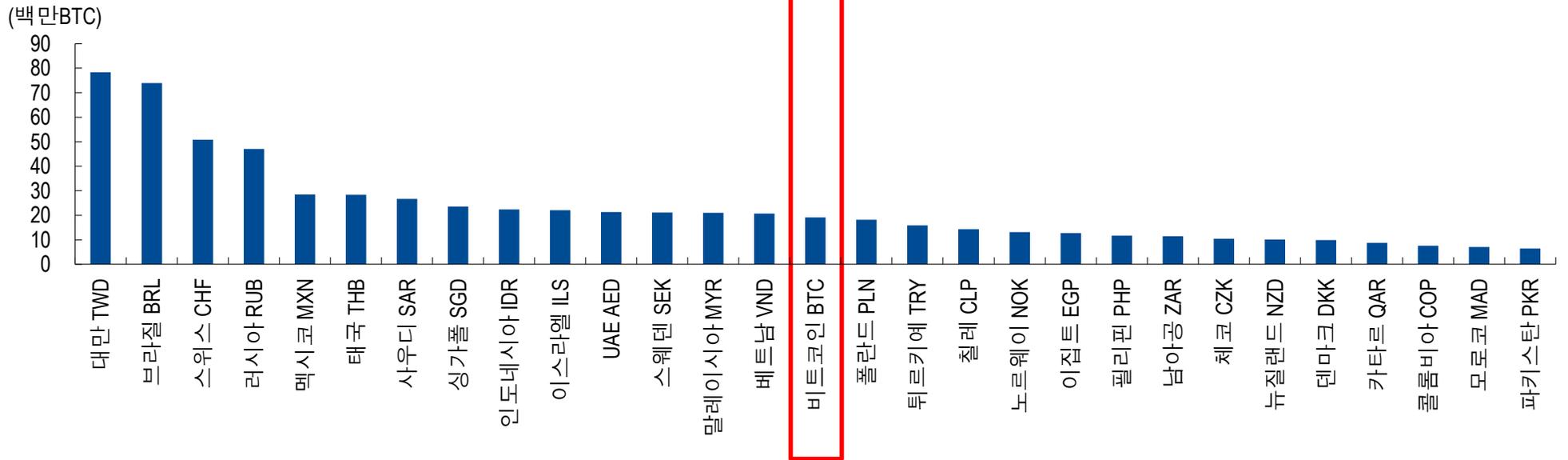
일반 통화 M2와 비교해본 비트코인 시가총액

- 일반 통화의 M2와 비트코인의 시가총액을 비교 시 이미 20위권. 사용자 기반이 증가한다면 순위 상승도 기대 가능

통화별 BTC 환산 시가총액 (1위~10위 비교)



통화별 BTC 환산 시가총액 (11위~40위 비교)



주1: 시가총액은 '통화량' x 'BTC 표시 환율'

주2: 2022.07.30 기준

자료: Coinmarketcap, NH투자증권 리서치본부

결제수단으로 받아들이고 있는 기업들 및 미국 주(州)들

- 금액이 크고 구매 빈도가 낮은 제품에 대해서 비트코인 결제 도입이 먼저 증가할 수 있음. 즉각 결제가 되지 않아도 소비자들이 느끼는 불편함이 크지 않기 때문
- 최근에는 고객 기반을 확대하거나 브랜드의 개성을 드러내기 위해 비트코인 등 디지털 자산 결제를 도입하는 기업들이 증가. 국가 내에서 지방 정부들이 자체적으로 비트코인 도입을 시도하는 경우도 많음

비트코인을 결제수단으로 쓰는 기업들 예시

Spend Crypto > Merchant Directory

Who accepts Bitcoin?

250+ companies & stores that accept cryptocurrency

Find out where you can spend cryptocurrency from any wallet. Shop stores that accept Bitcoin online and in-person.

럭셔리

- GUCCI, FARFETCH, TAG HEUER, HUBLOT, BREITLING, BALENCIAGA

میم(Meme)

- AMC THEATRES, GameStop

자료: BitPay, 각 사, NH투자증권 리서치본부

미국 주(州) 중 비트코인으로 납세 가능한 경우 존재

주 이름	세부 내용
Utah	• 2023년부터 세금 및 정부 요금 등을 비트코인으로 지불 가능
Colorado	• 세금 및 정부 요금 납부를 가능하게 할 계획
Arizona, California	• 상원의원 차원에서 법정 통화로 만들기 위해 노력중
Kentucky	• 채굴자에 세제 혜택 제공 (50개 주에서 3위 채굴 지역)

자료: NPR, CNBC, NH투자증권 리서치본부

비트코인의 모든 것

● IV. 비트코인을 둘러싼 쟁점들

- 1) 비트코인을 법정화폐로 도입하는 국가들 등장
- 2) 비트코인과 ESG, 과연 전력난과 기후위기의 공범일까
- 3) 비트코인 투자 접근법과 걸림돌
- 4) 비트코인 밸류에이션 난제

비트코인의 작업증명은 많은 양의 전기를 사용한다는 비판에 직면

- 비트코인의 작업증명(Proof-of-Work)에는 많은 자원이 소모됨. 특히 전력 사용이 비판의 초점. 비트코인 채굴에 사용되는 전력량이 네덜란드의 소비 전력량보다 많다는 등의 사실은 비트코인 사용과 투자에 거부감을 느끼게 하는 요인
- 일부 정부가 작업증명에 대해 비판적인 스탠스를 보이고 있으나, 비트코인 커뮤니티는 비트코인 채굴이 전력난을 가중시키지 않으며 오히려 신재생에너지 발전을 촉진시킨다고 주장

미국 하원의원 23명이 미국 환경 당국에 보낸 공개 서한에 대한 Bitcoin Mining Council의 반박 서한

주장: 탄소배출이 많으며 환경 오염이 우려됨

반박: 비트코인 채굴은 탄소배출 등 오염물 배출이 없으며 전력을 사용할 뿐. 사용하는 전력도 지속가능발전 비중이 58.4%(자체 조사 기준)로 높음

주장: 비트코인 채굴로 인해 화석연료 발전소들이 재가동되는 중

반박: 이 또한 발전단계의 이슈이며, 일부 사례에 불과. 미국 중심 채굴기업들은 지속가능한 발전원을 사용하겠다고 밝히는 중

주장: 비트코인 거래 한 건마다 큰 전력이 사용됨

반박: 거래 처리에는 전력이 거의 들지 않으며 채굴에 거의 모든 전력을 사용

주장: 지분증명(Proof-of-Stake) 방식은 작업증명보다 에너지를 99.99% 덜 사용

반박: 지분증명은 채굴이 아니며 탈중앙화를 달성하는 것에 있어서 작업증명이 더 유리하다고 주장

주장: 채굴 장비의 수명은 평균 1.3년. 대량의 폐기물 발생

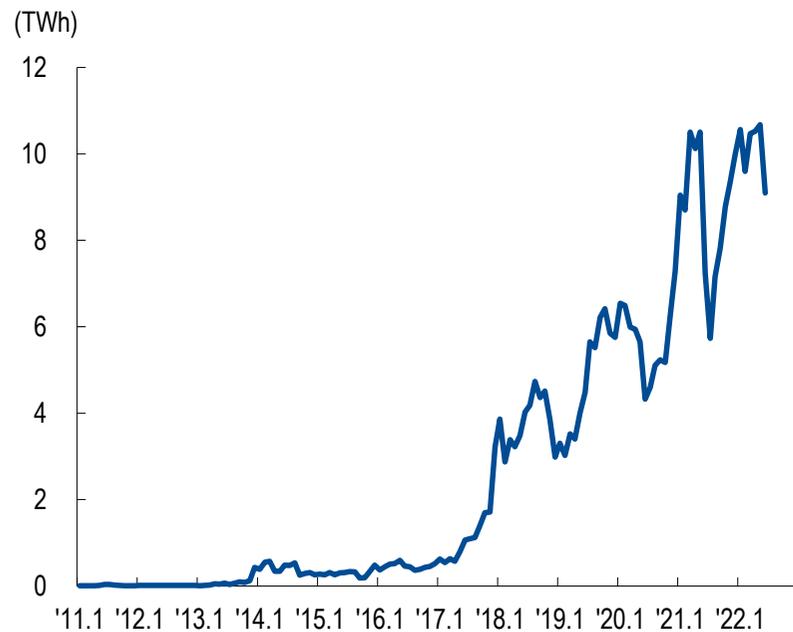
반박: 6년 이상 된 Bitmain S9 장비가 해시레이트의 40%를 차지. 더 오래된 채굴 장비도 전력만 저렴하다면 활용가능

자료: Bitcoin Mining Council, NH투자증권 리서치본부

소비 전력량이 많은 것은 사실

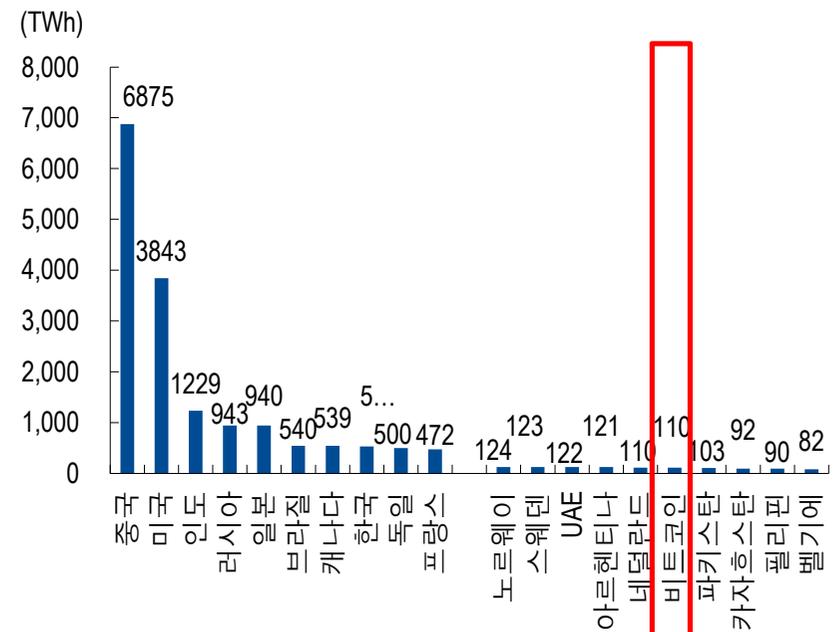
- 최근 비트코인 가격 하락으로 변동이 있지만 비트코인 채굴로 소비되는 전력량은 전 세계 소비 전력량의 약 0.4%에 달하며, 비트코인 채굴 소비 전력량은 빠르게 증가하는 추세
- 비트코인 채굴 소비 전력량은 전세계 30위권 전력 소비국의 소비 전력량과 유사한 수준이며, 일부 비공업국의 소비 전력량보다 더 많다는 사실이 사람들의 이목을 끌고 있음

비트코인 채굴의 소비 전력량 예상치 (월간)



자료: Cambridge Centre for Alternative Finance, NH투자증권 리서치본부

국가별 연간 소비 전력량: 비트코인은 약 30위권 수준

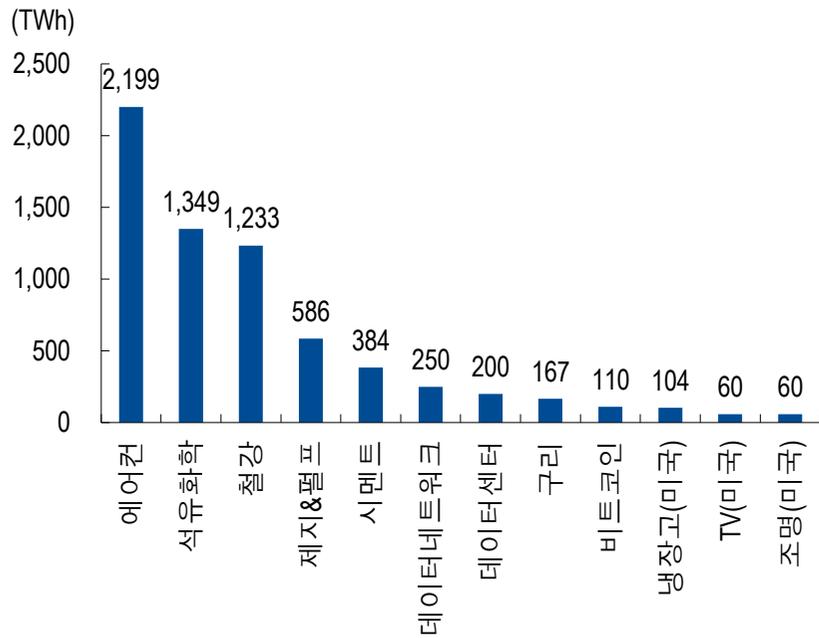


주: 국가별 소비 전력량은 2019년 기준. 비트코인 채굴 소비 전력량은 2022년 6월 기준 추정치
 자료: Cambridge Centre for Alternative Finance, NH투자증권 리서치본부

다른 산업이나 제품과 비교하면 많지 않다는 주장도 있음

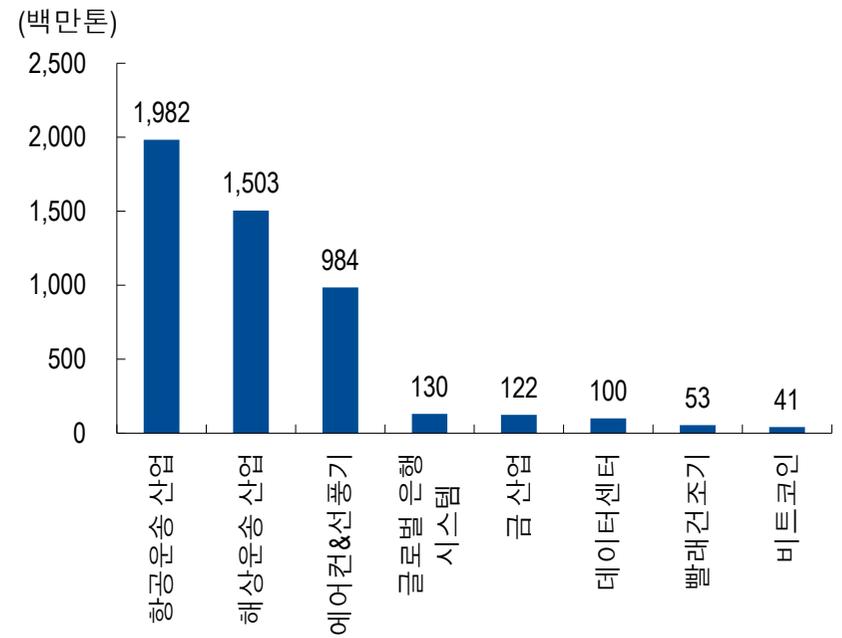
- 비트코인 채굴 소비 전력량은 아직 전 세계 에어컨 소비 전력량의 20분의 1에 불과하며 데이터센터 사용 전력의 절반 수준. 석유화학, 철강, 제지, 시멘트, 금 채굴과 비교해도 작은 수준. 크리스마스 당일 전 세계에서 조명에 소비되는 전력량보다 적다는 주장도 있음
- 탄소 배출량도 금 채굴이나 빨래건조기보다 작다는 통계 등을 근거로 타 산업 대비 크지 않다는 주장도 있음

소비 전력량 비교



자료: IEA, 미국 EIA, NH투자증권 리서치본부

탄소 배출량 비교

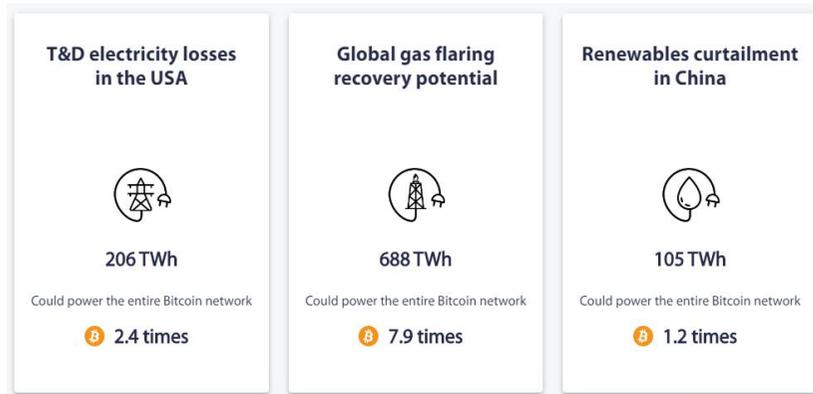


주: CoinShares 2022년 1월 자료 기준
 자료: CoinShares, NH투자증권 리서치본부

버려지는 전력을 좋아하는 비트코인 채굴자

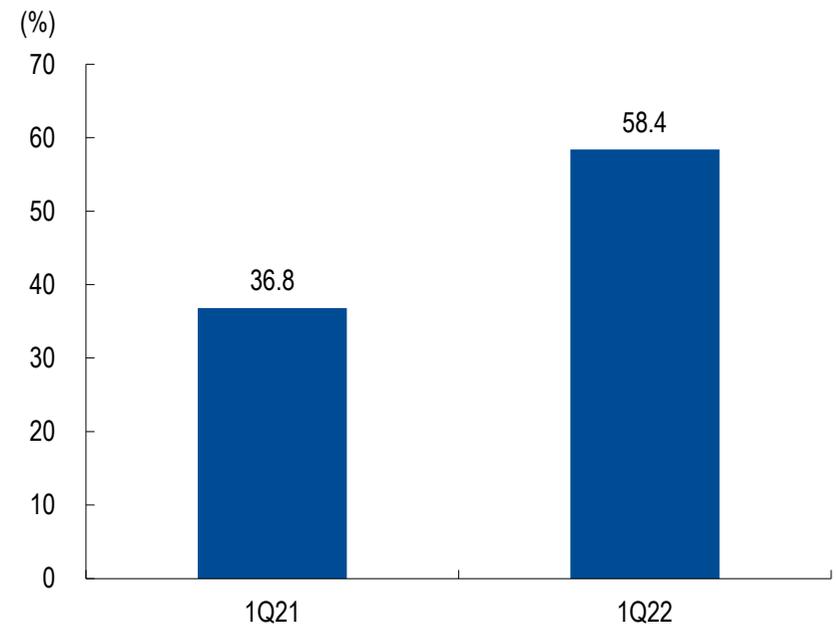
- 전력난을 가중시킨다는 주장이 있으나, 채굴 수익성의 핵심은 전력 비용 절감이기 때문에 전력이 비쌀 때는 전력 확보를 위해 경쟁하지 않음 (ex. 텍사스에 이상 기후가 발생하면 자발적으로 비트코인 채굴 중단) 송배전 손실을 없애기 위해 발전소 근처로 가거나, 파이프라인 부족으로 태워버리는 천연가스를 활용하거나, 수요가 낮은 시간대에 생산되는 신재생에너지를 이용하는 것을 선호
- 지속가능한 전력 사용 비율은 상승 추세이며 60%에 육박한다는 일각의 주장도 존재. 비율은 국가별로 상이하며 미국, 캐나다 등은 신재생에너지 활용 비율이 높다고 알려져 있음

비트코인 채굴자는 버려지는 전력을 좋아함



자료: Cambridge Centre for Alternative Finance, NH투자증권 리서치본부

지속가능한 전력(풍력, 태양광, 수력, 원자력) 사용 비율



자료: Bitcoin Mining Council 추정치, NH투자증권 리서치본부

신재생에너지 인프라 확대에 기여하는 비트코인 채굴 업체

- ESG 강화 트렌드에 맞춰 비트코인 채굴기업 중에도 신재생에너지 인프라 확대에 기여하고 있는 채굴업자 등장
- 예를 들어, 신재생에너지 인프라 사업자 입장에서 ‘풍력 발전소 근처로 채굴 설비를 이동해 밤 시간대에 잉여 풍력 발전량을 구매 해주고 낮 시간대 전력 부족 시 자동으로 전력 구매를 줄이는 비트코인 채굴자’ 는 사업성 개선에 기여하는 주체가 될 수 있음

착한 비트코인 채굴 업체는?

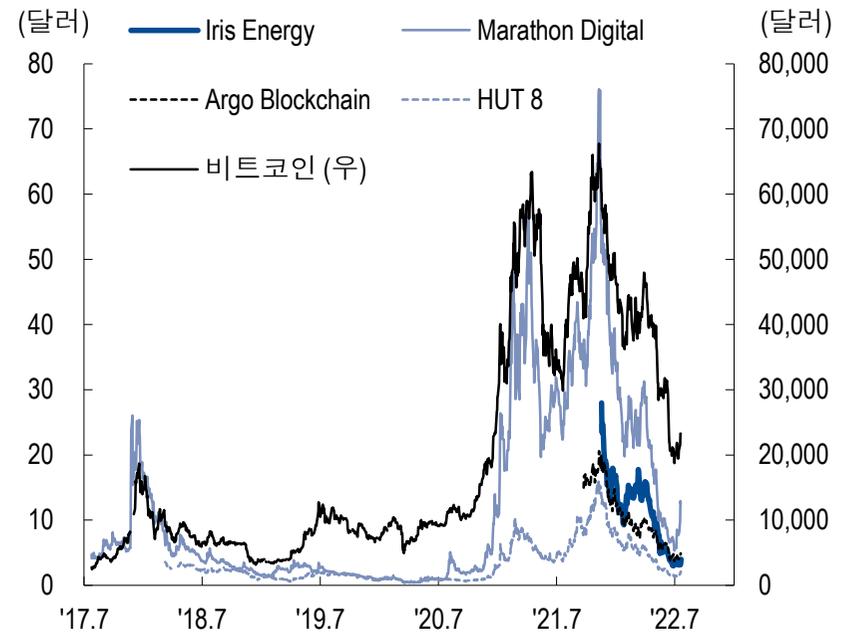
종목명	현황	목표
Iris Energy (NASDAQ: IREN)	신재생에너지 98% REC 구매 2%	신재생에너지 100%
Argo Blockchain (NASDAQ: ARBK)	퀘벡 수력 발전과 텍사스 풍력 발전 등 활용. 2020년과 2021년에 REC 구매로 인해 탄소중립을 넘어 탄소네거티브	현상 유지
Marathon Digital (NASDAQ: MARA)	현재 동사의 대부분의 채굴작업을 Compute North 텍사스 시설에서 호스팅. 해당 시설은 탄소중립 표방	2022년말까지 탄소중립
Hut 8 (NASDAQ: HUT)	-	2025년말까지 탄소중립

주1: 채굴 사업의 빠른 확장에 따라 변동이 있을 수 있음

주2: 티커는 나스닥 기준으로 정리

자료: Iris Energy, Argo Blockchain, Marathon Digital Holdings, Hut 8, NH투자증권 리서치본부

채굴 업체의 주가는 비트코인 가격보다 변동성이 더 큰 모습



주: 나스닥 상장 기준 가격

자료: Bloomberg, NH투자증권 리서치본부

자금 세탁 가능성 이슈: 비트코인은 추적이 용이한 자산

- 비트코인의 주 용도가 자금 세탁(money laundering)이며 이에 범죄자와 테러리스트를 돕는다는 오해가 많음. 비트코인은 거래 내역을 블록체인에서 누구나 바로 확인할 수 있기 때문에 자금 세탁이 어려움. 전통 금융범죄보다 빠른 추적이 가능한 면도 있음
- 미국 Colonial Pipeline에 대한 랜섬웨어 공격으로 갈취당한 비트코인을 FBI와 미 법무부가 빠르게 회수하는 등의 사례로 자금 세탁에 대한 오해가 풀리고 있음. 추적이 어려운 디지털 자산으로는 믹싱(mixing) 기법으로 자금 추적을 어렵게 만든 Tornado Cash 등이 있음

비트코인은 추적이 용이하며 자금 세탁에 불리함

Pipeline Investigation Upends Idea That Bitcoin Is Untraceable

The F.B.I.'s recovery of Bitcoins paid in the Colonial Pipeline ransomware attack showed cryptocurrencies are not as hard to track as it might seem.

자료: New York Times, NH투자증권 리서치본부

추적이 어려운 디지털 자산의 등장

Tornado Cash Classic

A fully decentralized protocol for private transactions on Ethereum.

[Launch App](#) [Alternative links >](#)

How Tornado Cash achieves privacy

Tornado Cash improves transaction privacy by breaking the on-chain link between source and destination addresses. It uses a smart contract that accepts ETH deposits that can be withdrawn by a different address. To preserve privacy a relay can be used to withdraw to an address with no ETH balance. Whenever ETH is withdrawn by the new address, there is no way to link the withdrawal to the deposit, ensuring complete privacy.

자료: Tornado Cash, NH투자증권 리서치본부

증권성 이슈: 비트코인은 증권이 아닐 가능성이 높음

- 비트코인은 미국에서 원자재로 인정받고 있으며 미국 CFTC(상품선물거래위원회)가 관리하고 있음. Ripple사에 대해 증권성 관련 소송을 진행하고 있는 미국 SEC(증권거래위원회) 위원장 Gary Gensler도 비트코인은 증권성이 없고 원자재라는 점을 인정
- 증권 여부를 판단할 때 미국에서 통상 ‘Howey Test’ 를 사용하는데 비트코인은 요건들을 충족하지 않음

비트코인은 CFTC 관할이며 SEC도 이를 인정

CFTC’s Jurisdiction

- In 2015, the CFTC found: “Bitcoin and other virtual currencies are encompassed in the [commodity] definition and properly defined as commodities.” See *In the Matter of: Coinflip, Inc., d/b/a Derivabit, and Francisco Riordan*, CFTC Docket No. 15-29.*
- In 2016, the CFTC took action against a bitcoin exchange that was offering futures in the U.S. without registering with the agency. *In the Matter of: BFXNA INC. d/b/a BITFINEX*, CFTC Docket No. 16-19.†
- In 2017, the CFTC proposed guidance regarding its jurisdiction over certain types of retail transactions involving virtual currency. It finalized this guidance in 2020. See “Retail Commodity Transactions Involving Certain Digital Assets,” 85 FR 37734 (June 24, 2020).
- In 2018, federal courts affirm the CFTC’s jurisdiction over digital assets in two cases, *CFTC v. McDonnell*, 287 F. Supp. 3d 213 (E.D.N.Y. 2018) and *CFTC v. My Big Coin Pay, Inc. et al.*, 334 F. Supp. 3d 492 (D. Mass. 2018).
- In 2019, CFTC Chairman Heath Tarbert expressed his view that ether is a commodity, as defined by the CEA.‡

* <https://www.cftc.gov/ido/groups/public/@enforcementactions/documents/legalpleading/enfcoinflproorder09172015.pdf>
 † <https://www.cftc.gov/ido/groups/public/@enforcementactions/documents/legalpleading/enf/bfxnaorder060216.pdf>
 ‡ See, e.g., CFTC Press Release 8051-19, available at <https://www.cftc.gov/PressRoom/PressReleases/8051-19>.



증권 여부를 가리는 Howey Test 요건들

요건	내용
자금의 투자	가상자산이 법정통화, 다른 가상자산 또는 다른 형태의 자산을 대가로 취득되는 경우로서, 자금조달이 이루어지는 대부분 가상자산 발행(ICO)이 동 요건을 충족
공동의 사업	SEC는 가상자산의 경우 구매자들과 발행인 및 구매자들 상호간에 연계가 있는 경우가 다수이므로 통상 공동의 사업(common enterprise) 요건이 충족된다고 판단
타인의 노력으로 수익이 창출될 것이라는 합리적 기대	가상자산의 증권 해당 여부 판단에 있어 가장 쟁점이 되는 사항으로 다음과 같이 구분하여 검토 가능 a) 운영주체에 대한 신뢰/의존 b) 수익에 관한 합리적 기대 c) 기타 고려사항

자료: 미국 CFTC, NH투자증권 리서치본부

자료: 금융감독원, NH투자증권 리서치본부

비트코인의 모든 것

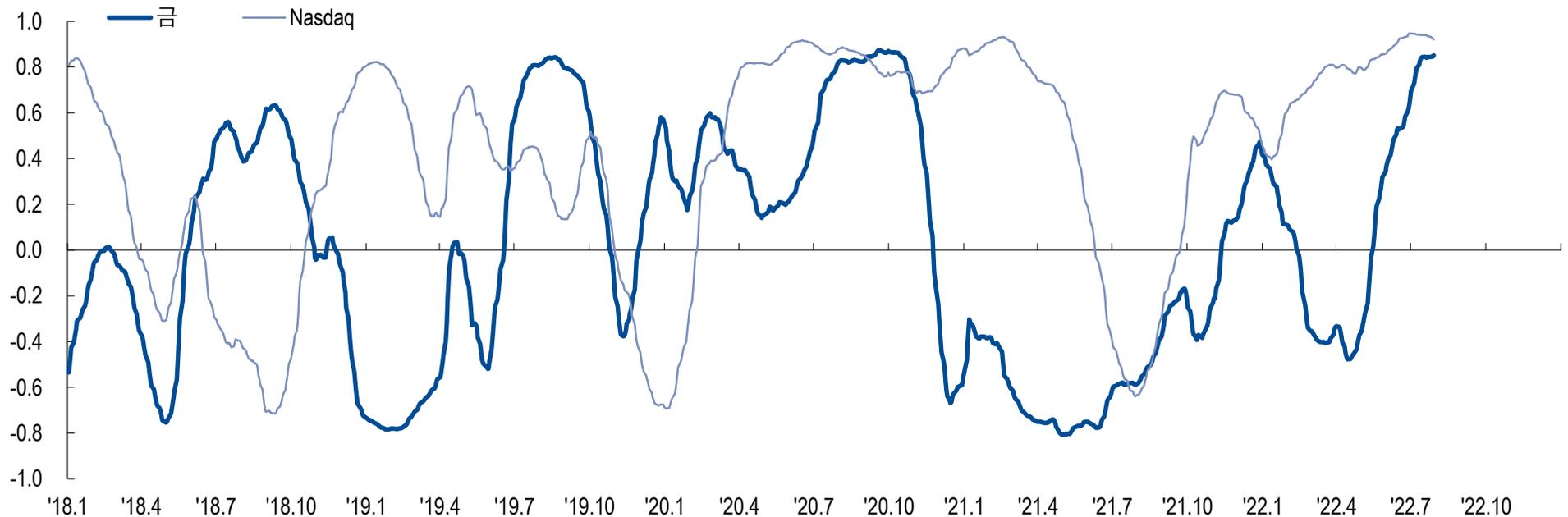
• IV. 비트코인을 둘러싼 쟁점들

- 1) 비트코인을 법정화폐로 도입하는 국가들 등장
- 2) 비트코인과 ESG, 과연 전력난과 기후위기의 공범일까
- 3) 비트코인 투자 접근법과 걸림돌
- 4) 비트코인 밸류에이션 난제

(1) 자산 포트폴리오 차원에서 바라보기

- 비트코인 가격은 현재 나스닥 지수와 높은 상관관계를 보이고 있으며, 금과의 상관관계도 동시에 높아진 점은 흥미로움. 디지털 금이라는 별명이 유효한 구간
- 경쟁 자산군과의 상관관계가 높아진 상황에서 포트폴리오 내 비트코인 편입을 서두를 필요는 없는 시점

다른 자산군과의 상관관계: 나스닥 지수와 높은 상관관계가 높아진 상황

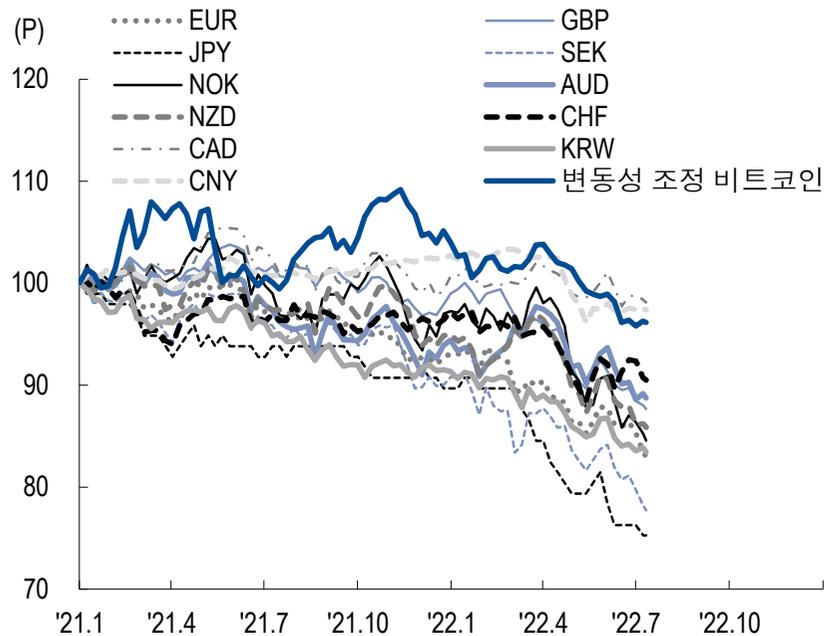


주: 나스닥 기준 100거래일 이동평균
 자료: Bloomberg, NH투자증권 리서치본부

(2) 환 포트폴리오 차원에서 바라보기

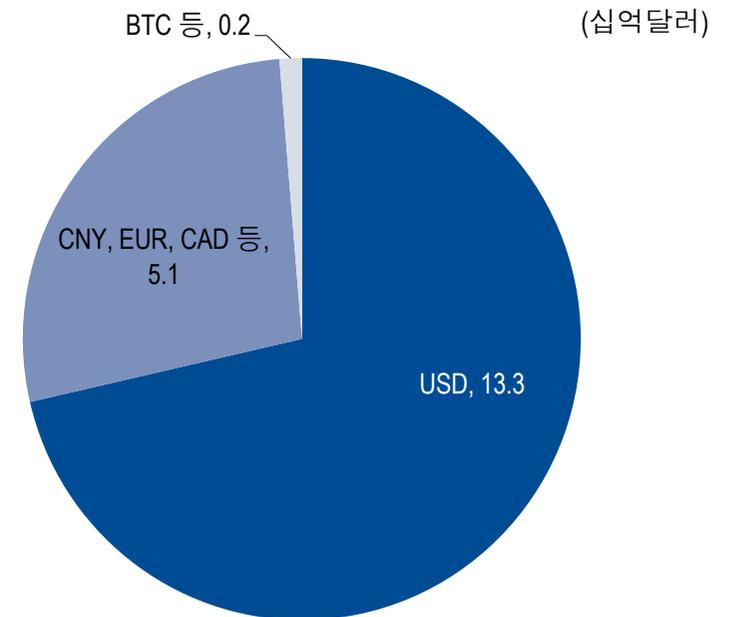
- 화폐가치 하락을 헤지하기 위해 비트코인을 환 포트폴리오에 추가하는 전략도 쟁점이 될 수 있음. 다만 최근 추이로 보면 비트코인은 화폐가치 하락에 따른 손실을 방어하지 못했으며, 변동성이 크기 때문에 일반 통화 대비 작은 비중으로 편입할 수밖에 없음
- Tesla와 같은 글로벌 대기업의 경우 비트코인을 작은 비중으로 편입 가능. 이미 다양한 외환으로 현금성 자산이 구성되어 있으며 비트코인의 규모는 일부에 불과. 2분기 말 기준으로 비트코인 등의 현금보유고(현금성 자산+디지털 자산) 내 비중 약 1.1%

주요 통화 및 비트코인의 가격 추이



주1: 달러 표시 가격. 2021.01.01 기준 100
 주2: 비트코인의 경우 변동성을 1/10로 조정
 자료: Bloomberg, NH투자증권 리서치본부

Tesla '현금성 자산 + 디지털 자산' 달러 기준 구성

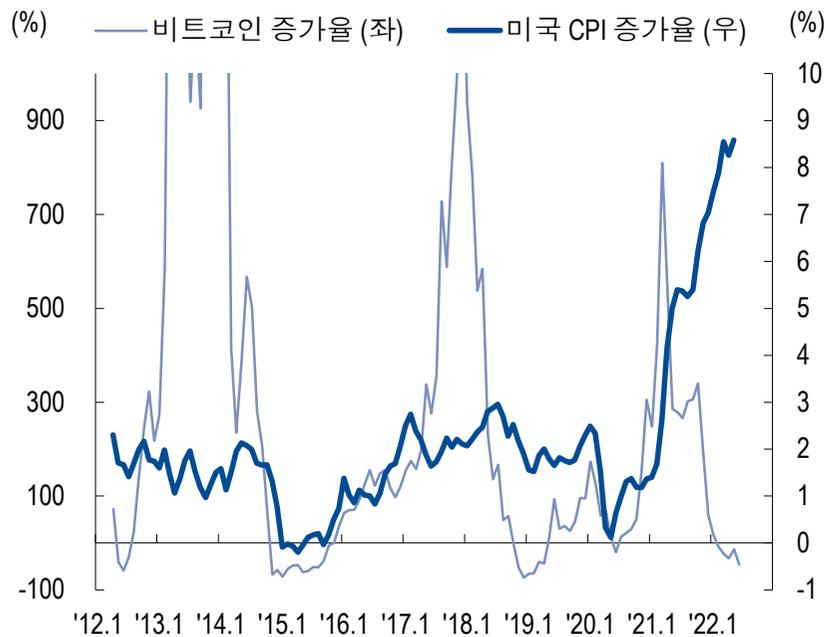


주: 2022년 6월 말 기준
 자료: Tesla, NH투자증권 리서치본부

(3) 인플레이션 헤지 차원에서 바라보기

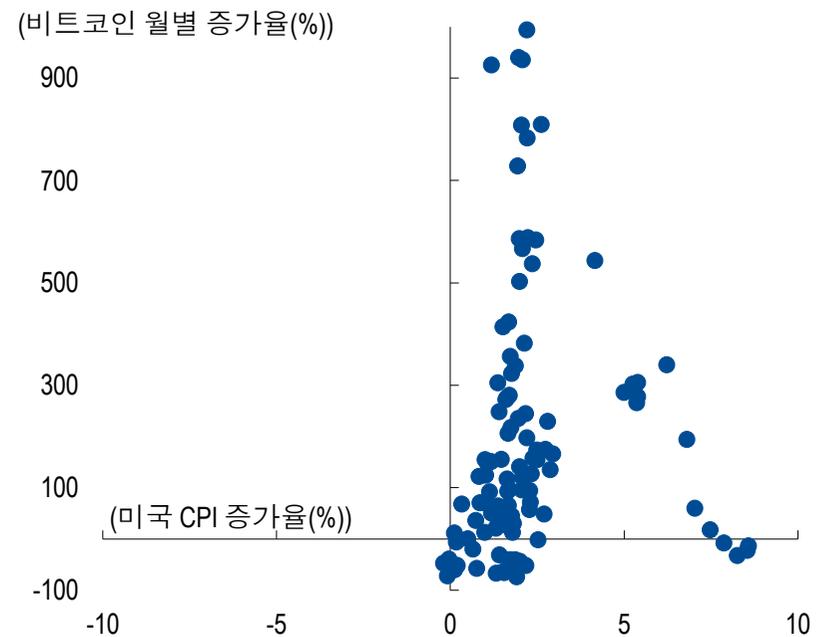
- 현재 단계에서 비트코인에 인플레이션 헤지 기능이 있는지는 불분명. 비트코인은 최근 물가 상승 국면에서 타격을 가장 심하게 입은 상품 중 하나. +0%와 +2% 사이의 물가 상승은 ‘저물가’로 인식되는 점을 고려하면 비트코인은 탄생 이후 첫 고물가 국면에서 좋지 않은 성적표를 보임
- ‘글로벌 교환수단이 되기 위한 성장 과정에 있는 자산’으로서의 정체성을 지니고 있는 바, 인플레이션 헤지 자산으로 분류되기에는 성장 자산의 성격이 강하다고 판단

미국 CPI와의 상관관계 약함



주: 월간 데이터 기준
 자료: Bloomberg, NH투자증권 리서치본부

2012년 이후 상관관계 분포도

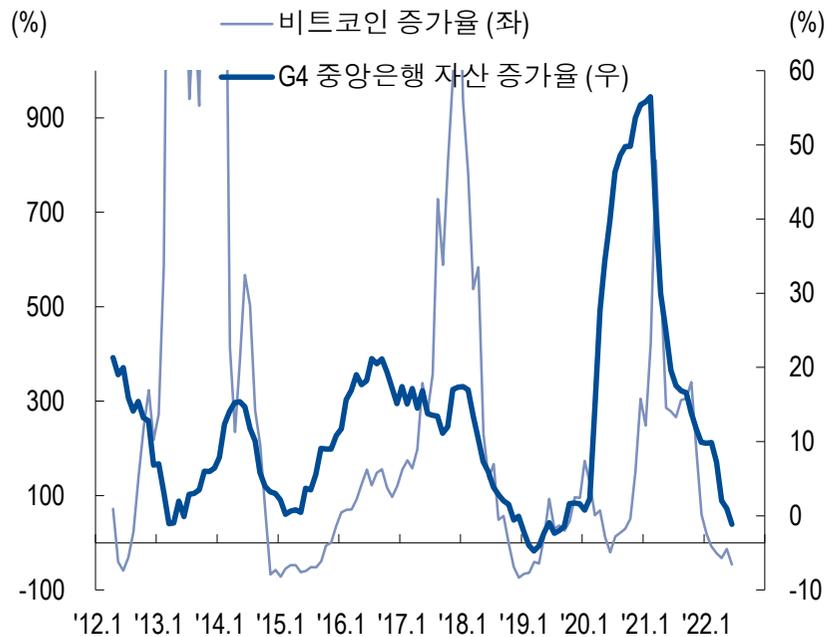


자료: Bloomberg, NH투자증권 리서치본부

(4) 주요 중앙은행 자산 증가율과의 관계는?

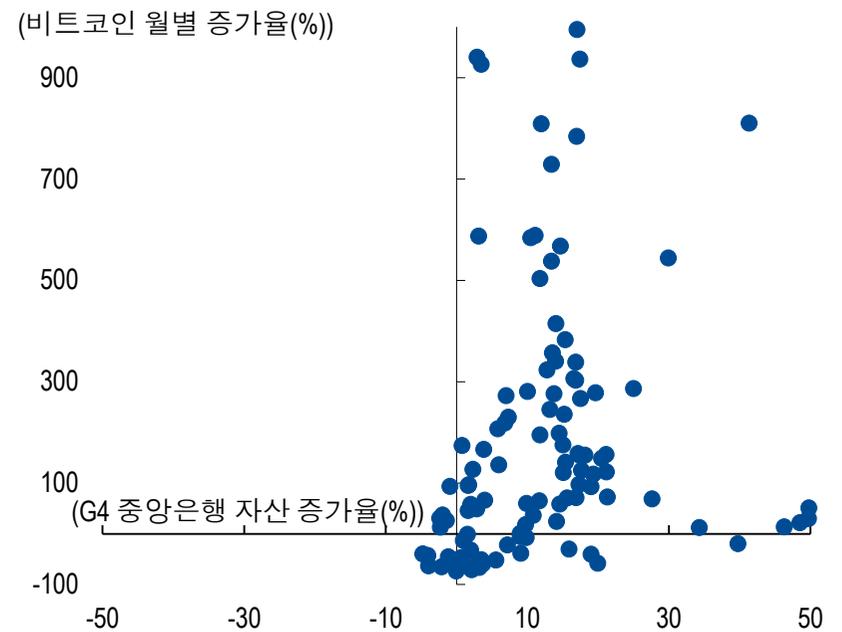
- 비트코인의 탄생 배경으로 회자되기도 하는 중앙은행의 과도한 자산 증가율을 살펴보면, 비트코인과의 상관관계가 조금 더 높은 것으로 파악됨. 이는 최근 비트코인 가격 하락을 설명하는 요인
- 앞서 나스닥 및 인플레이션과의 상관관계에서 살펴본대로 비트코인은 성장 자산으로서의 성격이 강하며, 중앙은행들의 자산 증가율 하락은 비트코인 가격에 특히 불리하게 작용

중앙은행 자산 증가율과는 상관관계 존재하는 것으로 보임



주: G4 중앙은행은 미국 Fed, 유럽연합 ECB, 영국 BOE, 일본 BOJ 지칭
 자료: Bloomberg, NH투자증권 리서치본부

2012년 이후 상관관계 분포도



주: G4 중앙은행은 미국 Fed, 유럽연합 ECB, 영국 BOE, 일본 BOJ 지칭
 자료: Bloomberg, NH투자증권 리서치본부

비트코인 관련 상품 출시 타임라인

- 비트코인 관련 상품은 대부분 ETF화되어 상장. 2017년 12월 비트코인 선물 출시 후 캐나다, 유럽 등 일부 시장에서는 비트코인 및 기타 디지털 자산에 대한 현물 ETF도 상장된 상태. 미국 SEC는 규제 당국 중에서 비트코인 현물 ETF에 대해 특히 조심스러운 스탠스를 유지하는 중
- 비트코인 현물 ETF가 미국 시장에서 출시될 경우 자금 유입 효과를 누릴 수 있을 것. 캐나다 현물 ETF 사례를 살펴봐도 비트코인 가격 등락에 따른 NAV 변화가 있으나 자금 유입에 기여한 점은 분명히 있음

비트코인 관련 주요 상품의 미국 출시 타임라인

일자	상품군	관련 기관/당국
2017.12	비트코인 선물	CBOE, CME, CFTC
2021.02	비트코인 현물 ETF (캐나다)	Ontario Securities Commission (캐나다)
2021.10	비트코인 선물 ETF (BITO)	SEC
2022.06	비트코인 선물 인버스 ETF (BITI)	SEC

자료: 언론보도, NH투자증권 리서치본부

주요 상품의 NAV 추이

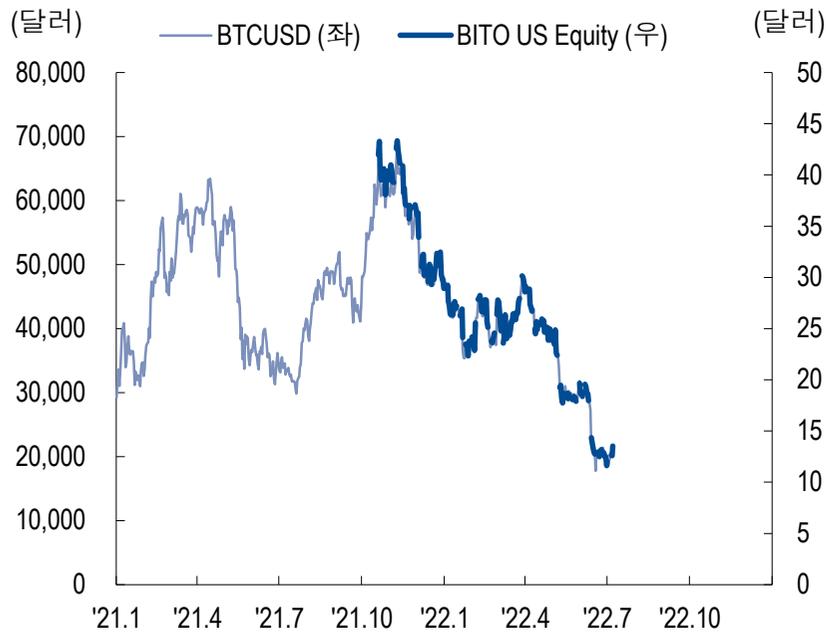


자료: Bloomberg, NH투자증권 리서치본부

선물 ETF가 이미 존재함에도 현물 ETF가 필요한 이유

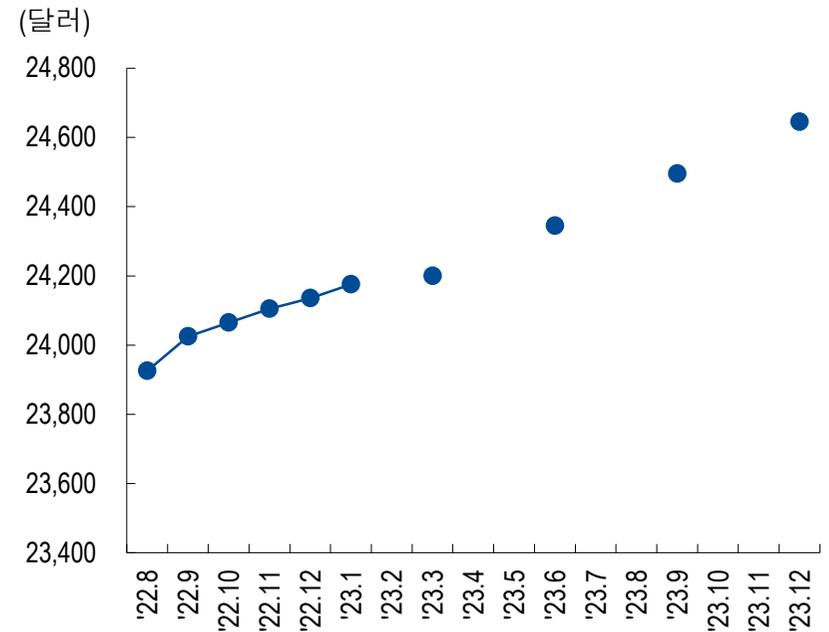
- 비트코인 선물은 비트코인 실물이 아니라 선물 계약에 대한 익스포저. 이는 투자자가 원하는 익스포저와 일치하지 않을 수 있음
- 결정적으로 비트코인 선물 ETF는 근월물을 원월물로 교체하는 것에 따른 롤링 비용이 있기 때문에 장기 투자자에게 부적합. 미국에서 출시된 BITO와 XBTF의 경우 비트코인 선물 지수를 비교적 정확히 추종하지만 액티브 ETF인 점도 유의

비트코인 선물 ETF 움직임은 대체로 비트코인 현물과 비슷



자료: Bloomberg, NH투자증권 리서치본부

비트코인 선물 커브



주: 2022.07.31 기준

자료: Bloomberg, NH투자증권 리서치본부

미국 이외 지역에는 이미 현물 ETF도 존재

- 캐나다와 유럽에는 이미 비트코인 현물 ETF가 상장되어 있으며, 캐나다에는 미국 내 비트코인 선물 ETF 출시 이전인 2021년 2월에 이미 비트코인 현물 ETF가 등장. 또한 비트코인 이외 이더리움 등의 자산에 대한 현물 ETF도 등장

캐나다와 유럽 등에는 이미 현물 ETF 존재

	BTCC	BCOIN
ETF명	Purpose Bitcoin ETF	Jacobi Bitcoin ETF
상장 거래소	Toronto Stock Exchange	Euronext Amsterdam
당국	Ontario Securities Commission	GFSC, AFM
현재가	4.72 CAD	-
AUM	8억1,800만CAD	-
보유 비트코인	26,729 BTC	-
보수비용	1.00%	1.50%
운용사	Purpose Investments	Jacobi Asset Management
출시	2021.02.23 (세계 최초)	2022.07 (유럽 최초)

자료: Purpose Investments, Jacobi Asset Management, NH투자증권 리서치본부

캐나다 등에는 이미 이더리움 현물 ETF도 존재



자료: Purpose Investments, NH투자증권 리서치본부

SEC가 비트코인 현물 ETF를 승인하지 않고 있는 이유

- SEC는 비트코인 시장의 사기와 조작 예방 조치가 미비하다는 판단하에 투자자 보호 차원에서 현물 ETF를 승인하지 않고 있음. 비트코인 시장의 변동성이나 비트코인의 가치에 대한 논쟁은 반대의 사유가 아니라고 밝힘
- SEC가 지금까지의 입장을 고수한다면 Grayscale이나 기타 운용사들이 현물 ETF 승인 조건을 충족하기 어려울 수 있음. ‘규제 받는 비트코인 현물 시장’이 존재해 비트코인 현물 ETF에 대한 시장 조작도 방지할 수 있다는 점(감시공유) 혹은 비트코인 시장이 태생적으로 시장 조작에 강하다는 점을 증명해야함

SEC가 제시한 거부 이유이자 승인 조건

As the Commission has explained, an exchange that lists bitcoin-based ETPs can meet its obligations under Exchange Act Section 6(b)(5) by demonstrating that the exchange has a comprehensive surveillance-sharing agreement with a regulated market of significant size related to the underlying or reference bitcoin assets.

→ ‘비트코인 현물에 대한 상당한 크기의 규제 시장과 감시공유에 대해 합의한다면 승인 가능 (하지만 ‘규제 받는 비트코인 현물 시장’이 없음)

if a listing exchange could establish that the underlying market inherently possesses a unique resistance to manipulation beyond the protections that are utilized by traditional commodity or securities markets, the listing market would not necessarily need to enter into a surveillance-sharing agreement with a regulated significant market.

→ 감시공유 합의가 필요 없으려면, 현재 비트코인 시장의 사기/조작에 대한 내생적인 방어력이 전통적인 원자재나 증권 시장에 적용되고 있는 보호조치보다 강해야함

자료: SEC, NH투자증권 리서치본부

비트코인에 대한 기타 논의는 판단에 영향이 없다고 밝힘

Comment letters also address, among other things, the general nature and uses of bitcoin and blockchain technology; the state of development of bitcoin as an investment asset; beneficial tax consequences of approval of a spot bitcoin ETP; the merits of an investment in bitcoin; the nature and state of the bitcoin mining network; the current failure, and potential promotion of, U.S. competitiveness in the global marketplace relating to bitcoin; suggestions for improving regulation of bitcoin and other digital assets markets and related market participants and criticisms of the current regulatory approach; increasing education relating to, and accessibility of, bitcoin; the merits of the Sponsor; and specific concerns relating to the Sponsor and its management of the Trust. Ultimately, however, additional discussion of these topics is unnecessary, as they do not bear on the basis for the Commission's decision to disapprove the proposal.

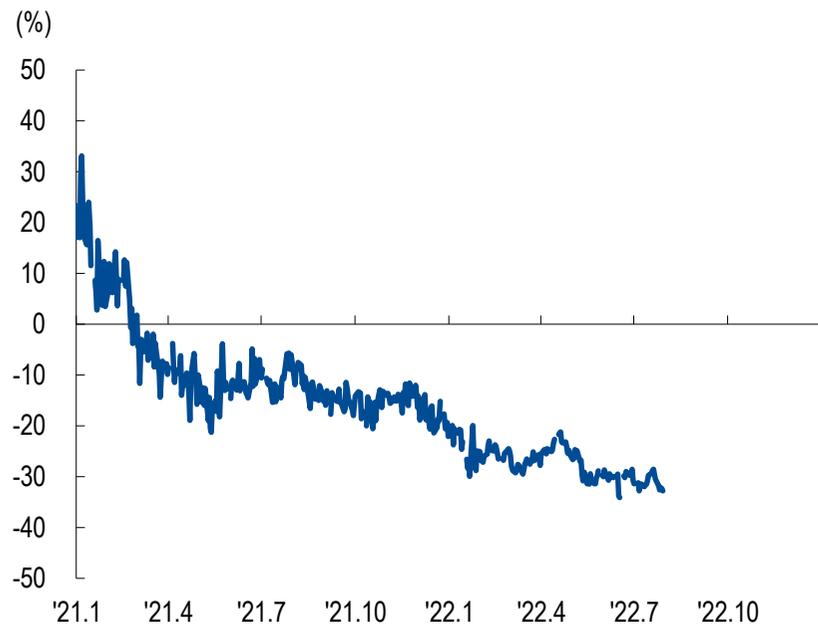
→ 비트코인, 블록체인 기술, 미국 암호화폐 시장 경쟁력 촉진 등 기타 논의는 SEC의 결정과 무관

자료: SEC, NH투자증권 리서치본부

비트코인 현물 ETF가 되고 싶은 GBTC

- Grayscale이 운영하는 GBTC(Grayscale Bitcoin Trust)는 closed-end(폐쇄형) 펀드이며 최대 규모의 비트코인 관련 펀드. 2021년 초까지만 해도 순자산가치(NAV)보다 할증된 가격으로 거래되었으나 할인폭이 순자산가치 대비 30%까지 점차 확대
- Grayscale은 디스카운트를 해소하기 위해 ETF 전환을 SEC에 요청했으나 거절당한 뒤 소송을 제기

GBTC의 NAV 대비 디스카운트/프리미엄 차트



자료: Bloomberg, NH투자증권 리서치본부

어떤 요인들이 디스카운트를 구성하고 있을까

현재로선 '환매' (redemption)가 안되는 중

디스카운트 해소 여부가 SEC의 결정에 달려있는바,
규제/법률 리스크 존재

SEC와의 소송이 길어질 수 있음

ETF로 전환되기까지 연 2%의 보수비용을 감당해야함

수익자들이 Grayscale 상대로 소송을 진행해 GBTC를 청산하고
비트코인을 배분받을 수도 있겠지만 Grayscale은 이를
막기 위해 ETF 전환에 힘쓸 것

자료: NH투자증권 리서치본부

전통 금융기관의 디지털 자산 시장 진출 현황

- 전통 금융기관의 영향력에 대한 논의가 디지털 자산 참가자들 사이에서 활발
- 현재까지 전통 금융기관들의 디지털 자산 시장 참여는 초기 단계이며, 바이사이드 기관의 투자 익스포저는 미미한 수준

디지털 자산 시장이 이야기하는 ‘기관(Institution)’ 은?



자료: 각 사, NH투자증권 리서치본부

진짜 기관들의 움직임은?

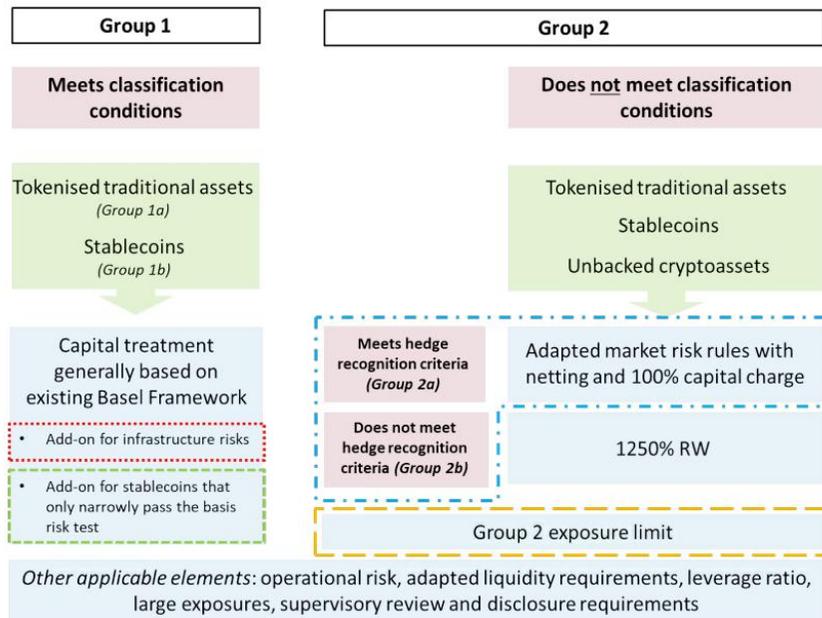
	주요 움직임
관련 ETF 출시	BlackRock
선물 및 옵션 거래 서비스	Goldman Sachs, Bank of America
비트코인 담보 달러 대출	Goldman Sachs
고객자산가 대상 상품 판매	Goldman Sachs, Morgan Stanley, JPMorgan, Wells Fargo 등
리서치 제공	다수의 금융사
크립토 인프라 기업 지분 투자	다수의 금융사
수탁 관련 사업	Fidelity, Citi, BBVA, DBS, Societe General, BNP 등
자문	Goldman Sachs(Celsius)
비트코인 401K 투자	Fidelity

자료: 언론 보도, NH투자증권 리서치본부

기존 산업과의 연결고리

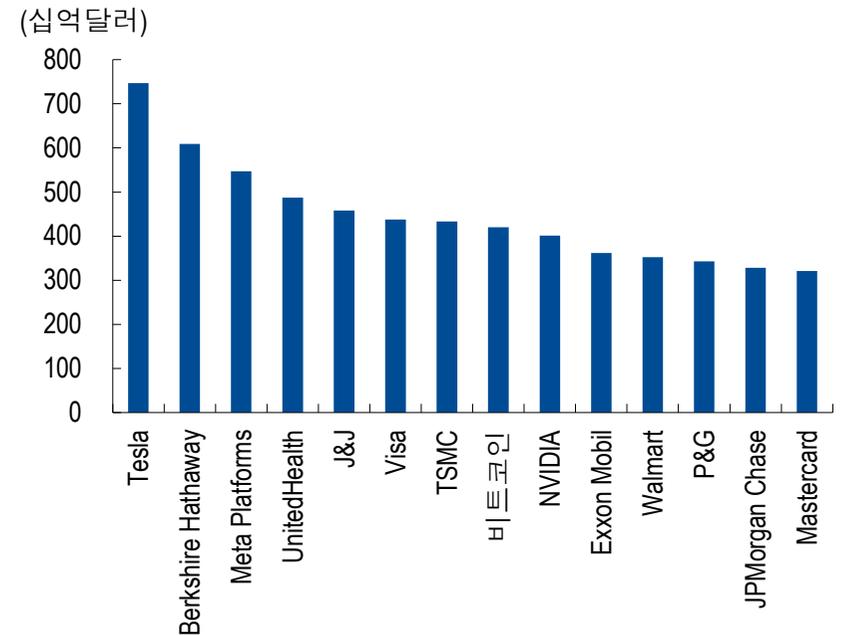
- 전통 금융기관 중에서도 특히 은행은 디지털 자산에 대해 보수적인 태도를 보이고 있음. BIS(국제결제은행)에 의하면 2020년 말 기준 평균적으로 디지털 자산은 은행 보유 RWA(위험가중자산)의 0.02% 미만이었음. BIS는 은행들의 디지털 자산 보유량에 Tier 1 자본의 1% 상한을 두어야한다고 제안하며 선제적으로 리스크 관리 권고
- 비트코인 시가총액은 디지털 자산 중에서는 가장 크지만 기타 자산군에 비해서는 작은 상황으로 비트코인 가격 등락이 실물 경기에 미치는 영향은 크지 않음

BIS의 디지털 자산 논의: 선제적으로 리스크 관리 중



자료: BIS, NH투자증권 리서치본부

주요 개별 종목과의 시가총액 비교: 아직 절대적 크기 작음



주: 2022.07.18 기준

자료: Coinmarketcap, NH투자증권 리서치본부

기관의 비트코인 도입을 위해서는 수탁(Custody) 인프라가 필요

- 비트코인의 수탁은 전통자산과 달리 기술적인 인프라가 필요하며 기관들의 진출을 저해하는 요소. 디지털 자산 수탁은 신뢰와 상당한 주의가 필요한 문제. 따라서 국내 은행들은 합작사를 통한 수탁 사업 진출에 적극적
- 거래소 계좌에 자금을 예치해두거나 ETF를 매수하는 것은 자산을 타인이 통제한다는 점에서 탈중앙화된 수탁 방식이 아니며 수탁을 맡긴 기업이 출금 제한 가능. 직접 수탁하는 경우에도 해킹의 위험이 있으며 개인 키를 잃어버린다면 디지털 자산을 복구할 방법이 없음

수탁에는 수탁 대행 방식과 직접 수탁 방식이 존재

	정의	예시
수탁 대행 (Custodial)	디지털 자산에 대한 익스포저는 있으나 직접 보관 및 관리를 하지 않는 것. 개인 키 등을 수탁 대행 주체가 보관. 탈중앙화 수준은 낮으나 수탁 관련된 번거로움 해결 가능	거래소, ETF, 수탁사
직접 수탁 (Non-custodial)	개인키 등을 직접 보관하며 관리. 개인키 등을 분실할 경우 디지털 자산을 영구적으로 분실하게 됨	개인 주소 (Not your keys, not your coins)

자료: Gemini, NH투자증권 리서치본부 정리

직접 수탁에는 크게 두 가지 방식 존재

	정의 및 예시	장단점
콜드 월렛 (Cold Wallet)	물리적인 분리된 기기에 개인 키 등을 보관 예시: 하드웨어 지갑 (USB 형태 등)	보안이 강력해, 코인 대량 보유 시 통상 대부분을 콜드 월렛에 보유. 자산 전송 시 콜드 월렛을 컴퓨터 등에 연결해 핫 월렛으로 이동해야해 번거로움
핫 월렛 (Hot Wallet)	인터넷에 상시 연결되어있는 지갑 예시: 웹기반, 모바일, 데스크톱 지갑	편리하지만, 보안이 상대적으로 약함

자료: Gemini, NH투자증권 리서치본부 정리

디지털 자산 회계 처리 방식

- 국제회계기준에 의하면 비트코인 등 디지털 자산은 대부분 무형자산으로 분류. 이에 가격이 취득원가보다 하락하면 손상차손으로 손실을 인식하지만 상승하는 경우에는 평가 이익으로 인식하지 않게 됨
- 현재 방식은 회계 불확실성이 크다는 의견이 있으며 한국회계기준원 등은 디지털 자산을 무형자산이 아닌 금융자산으로 봐야한다고 주장. 향후 회계 기준이 변화할 가능성이 있는 바 디지털 자산 기보유 기업들은 이에 주목할 필요 있음

현행 국제회계기준의 디지털 자산 회계 처리

계정	적용대상	회계처리	회계기준
재고자산	통상적인 영업활동 과정에서 판매를 위해 보유 중이거나 중개를 위해 매매하는 경우	공정가치로 가상자산을 평가하여 당기말에 평가 이익 및 평가 손실 반영	IFRS: IAS 2 K-IFRS: 제 1002호
무형자산	이 외의 목적으로 가상자산을 보유하는 경우	당기말 가상자산 가격이 취득원가보다 하락하면 손상차손으로 손실을 인식 당기말 가상자산 가격이 취득원가보다 상승하는 경우에는 평가 이익으로 인식하지 않음	IFRS: IAS 38 K-IFRS: 제 1038호

자료: 자본시장연구원, NH투자증권 리서치본부

비트코인 보유 기업의 회계 처리 현황

- 미국 상장사의 경우 비트코인을 ‘비한정 내용연수 무형자산(indefinite-lived intangible assets)’ 으로 분류. IFRS와 유사하게, 디지털 자산 가격 하락 시에는 손상 처리하지만 가격이 오를 경우에는 이를 반영하지 않으며 매도 시 차익을 반영
- 한국 기업들도 비트코인 등 디지털 자산을 무형자산으로 분류. 비트코인 보유 기업이 많아질수록 회계 불확실성을 해소하려는 움직임도 커질 것

미국 상장사는 ‘비한정 내용연수 무형자산’ 으로 분류

기업명	보유 디지털 자산	재무제표 표기
Microstrategy	비트코인	비유동자산에서 'Digital assets'
Tesla	비트코인, 도지코인	비유동자산에서 'Digital assets, net'
Block (구 Square)	비트코인	기타 비유동자산에서 'Other Non-Current Asset'
Marathon	비트코인	유동자산에서 'Digital currencies'

자료: 각 사 10-Q, NH투자증권 리서치본부

한국 비트코인 보유 기업

기업명	보유 디지털 자산	재무제표 표기
위메이드	KLAY, 비트코인, 이더리움, USDT 등	무형자산-암호화자산
엔엑스씨 (비상장)	비트코인 등	기타의 무형자산

자료: 전자공시시스템, NH투자증권 리서치본부

비트코인의 모든 것

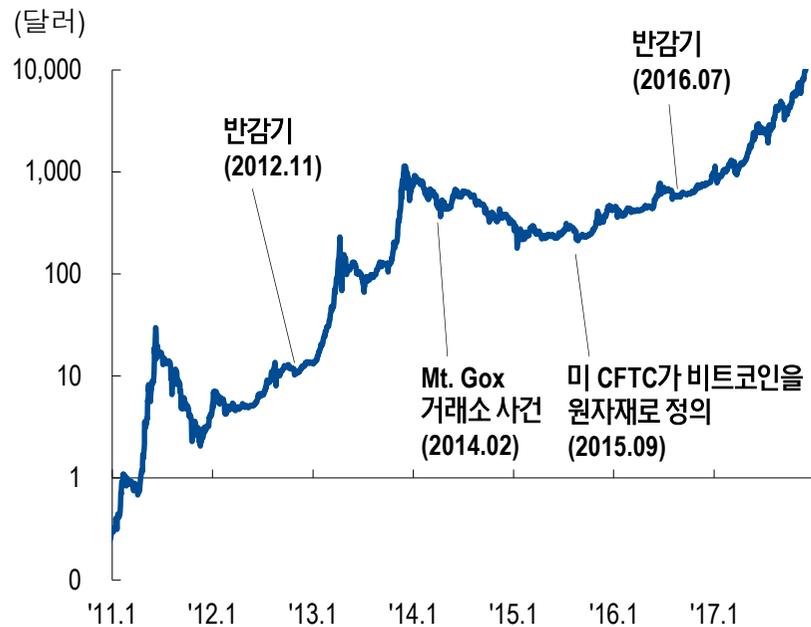
• IV. 비트코인을 둘러싼 쟁점들

- 1) 비트코인을 법정화폐로 도입하는 국가들 등장
- 2) 비트코인과 ESG, 과연 전력난과 기후위기의 공범일까
- 3) 비트코인 투자 접근법과 걸림돌
- 4) 비트코인 밸류에이션 난제

비트코인 가격 추이와 주요 이벤트

- 비트코인은 2010년 7월말 0.07달러 수준에서 거래됨. 이후 블록당 보상이 총 3번의 반감기를 거치며 유의미한 투자자산으로 발전해왔으며 가격 빠르게 상승. 다만, 2017년에 1만달러를 돌파한 이후 만 5년이 지났음에도 10만달러 도달에는 실패
- Mt. Gox 거래소가 출금을 정지한 사건이나 스테이블코인인 TerraUSD가 디페깅되며 발생한 일련의 사건들과 같이 투자심리를 극도로 저조하게 만드는 사건들도 다수 발생. 또한 각국 정부 규제나 제도권 편입 흐름 등도 중단기 가격 향방에 큰 영향

비트코인 가격 추이 (~2017년 말)



주: 로그 그래프
자료: Bloomberg, NH투자증권 리서치본부

비트코인 가격 추이 (2018년 초~현재)



자료: Bloomberg, NH투자증권 리서치본부

여러 차례 하락에도 회복력을 보여온 비트코인 가격

- 비트코인 가격은 수많은 하락에도 회복력을 보여오며 잠시의 유행이 아님을 증명해나가고 있음

비트코인 가격 등락의 역사

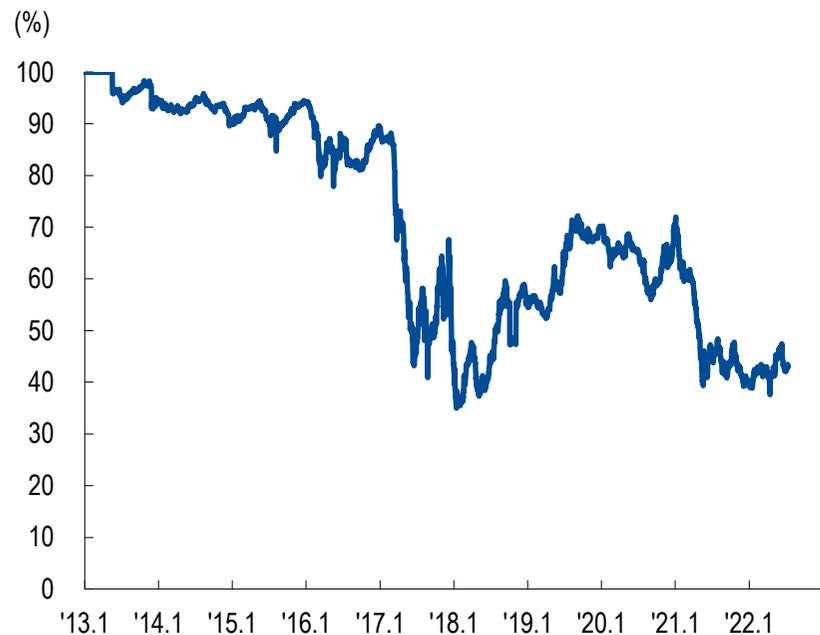
주요 비트코인 조정 (전고점에서 저점까지 기간)	조정 기간 일수	가격 고점	가격 저점	하락폭	다음 고점 시점	저점에서 새로운 고점 달성까지 소요 일수
2021.11.10 ~ 2022.06.18	216	\$69,000	\$17,745	-74%	?	?
2021.04.14 ~ 2021.06.22	69	\$64,899	\$28,800	-56%	09-Nov-21	209
2019.06.26 ~ 2020.03.13	261	\$13,868	\$3,858	-72%	03-Nov-20	496
2017.12.17 ~ 2018.12.16	364	\$19,783	\$3,204	-84%	16-Dec-20	1,095
2017.11.08 ~ 2017.11.12	4	\$7,879	\$5,507	-30%	16-Nov-17	8
2017.09.02 ~ 2017.09.15	13	\$5,014	\$2,951	-41%	10-Dec-17	99
2017.06.11 ~ 2017.07.16	35	\$3,025	\$1,837	-39%	06-Aug-17	56
2017.03.10 ~ 2017.03.24	14	\$1,326	\$892	-33%	27-Apr-17	48
2013.11.30 ~ 2015.01.14	410	\$1,166	\$170	-85%	23-Feb-17	1,181
2013.04.10 ~ 2013.07.07	88	\$266	\$63	-76%	11-Jul-13	92
2011.06.08 ~ 2011.11.17	162	\$32	\$1.99	-94%	28-Feb-13	631
2011.05.13 ~ 2011.05.21	8	\$8.45	\$5.58	-34%	25-May-11	12
2011.02.10 ~ 2011.04.04	53	\$1.10	\$0.56	-49%	17-Apr-11	66
2010.11.06 ~ 2010.11.10	4	\$0.50	\$0.14	-72%	31-Jan-11	86
2010.09.14 ~ 2010.10.08	24	\$0.17	\$0.01	-94%	24-Oct-10	40
가장 최근 하락 5번 평균	142			-57%		381
가장 최근 하락 5번 중간값	69			-56%		209

자료: Blockchain.com, NH투자증권 리서치본부

비트코인은 디지털 자산 시총 1위를 유지할 수 있을까

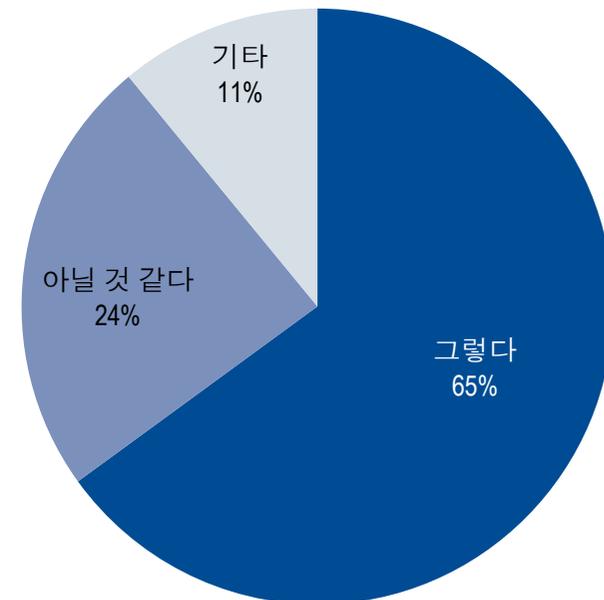
- 비트코인은 디지털 자산 시가총액 1위 자리를 내준 적이 없음. 다양한 자산들이 등장하며 전체 디지털 자산 시가총액에서 비중이 40%대로 하락했지만 여전히 시총 1위 자리는 굳건
- 시가총액 2위인 이더리움이 장기적으로 역전할 것이라는 의견도 많으나, 이더리움의 시가총액은 비트코인의 절반 수준으로 가까운 시일 내에 역전 현상이 발생하진 않을 것으로 보임

비트코인 점유율 추이: 현재 역사적 저점 수준



주: 비트코인 점유율(Bitcoin Dominance)이란? 전체 디지털 자산 시가총액에서 비트코인이 차지하는 비율
 자료: NH투자증권 리서치본부

비트코인이 10년 후에도 디지털 자산 시총 1위를 유지할까?



주: Twitter 상에서 2022.07.11에 5,828명 투표
 자료: Coinmarketcap 설문조사, NH투자증권 리서치본부

반감기는 21만번째 블록마다 발생

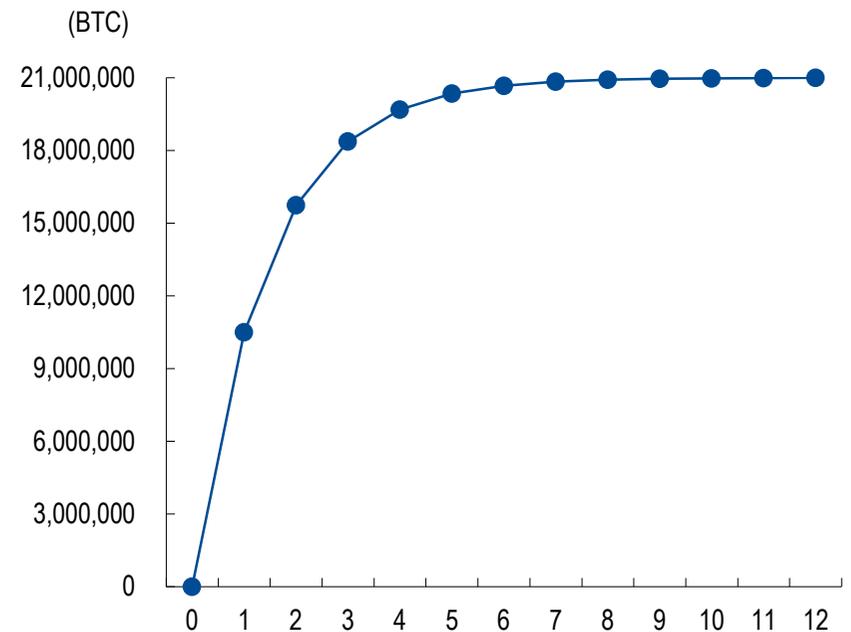
- 비트코인의 반감기 스케줄은 날짜가 고정되어있는 것이 아니라 21만번째 블록마다 발생. 비트코인이 처음 출시되었을때는 블록당 보상이 50BTC였으나 반감기를 세 번 거치며 현재는 6.25BTC(50BTC의 1/8)
- 2022년 4월 초까지 1,900만 BTC가 채굴되었으며 90% 이상이 채굴된 상태. 비트코인의 반감기는 30번 남았으며 그 이후에는 블록당 보상이 0 BTC가 됨

비트코인 반감기 스케줄

	블록당 보상 (BTC)	일일 총 보상 (BTC)	다음 반감기 전까지 채굴될 비트코인
2009.01.03~	50	~7,200	50%
2012.11.28~	25	~3,600	75%
2016.07.09~	12.5	~1,800	87.5%
2020.05.11~	6.25	~900	93.75%
2024~	3.125	~450	96.875%
2028~	1.5625	~225	98.4375%
2140	0	0	100%

자료: NH투자증권 리서치본부

채굴 총량 궤적: 이미 1,900만 BTC 이상 채굴됨



주: x축은 반감기 횟수
자료: NH투자증권 리서치본부

과거 반감기 이후 가격 상승

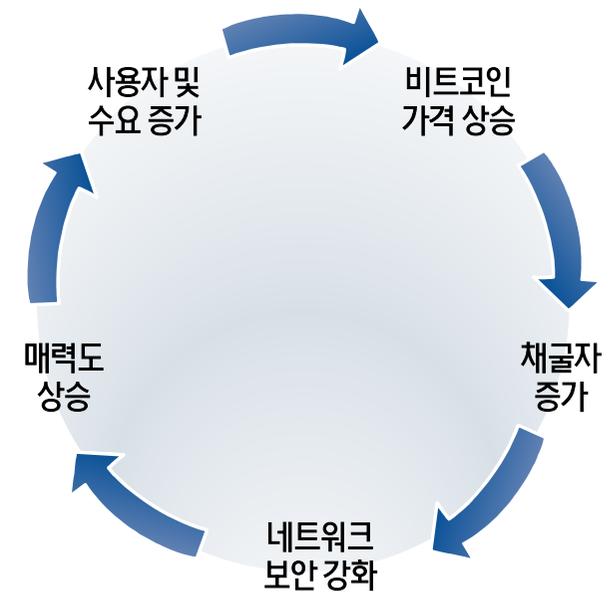
- 반감기 이후 비트코인은 상승폭을 보임. 비트코인의 신규 공급이 줄어들며 비트코인 가격이 상승한다는 논리. 지난 세 번의 반감기 사이클에서 비트코인은 최대 9,073%, 2,883%, 688% 상승
- 비트코인의 가격 상승은 채굴자와 사용자를 유입시켜 가격 상승의 선순환 발생 요인으로 작용 가능

반감기 사이클마다 가격은 얼마나 올랐을까?

반감기 시점	반감기 이후 단기 고점 일자 (소요 기간)	반감기 시점 가격	단기 고점 가격 (상승률)
2012.11.28	2013.12.02 (369일)	12.34달러	1,132.01달러 (9,073%)
2016.07.09	2017.12.16 (526일)	649.77달러	19,385.90달러 (2,883%)
2020.05.11	2021.11.08 (546일)	8,568.40달러	67,553.51달러 (688%)
2024년 상반기 (예상 시점)	-	-	-

자료: Messari, NH투자증권 리서치본부 정리

비트코인 선순환 고리

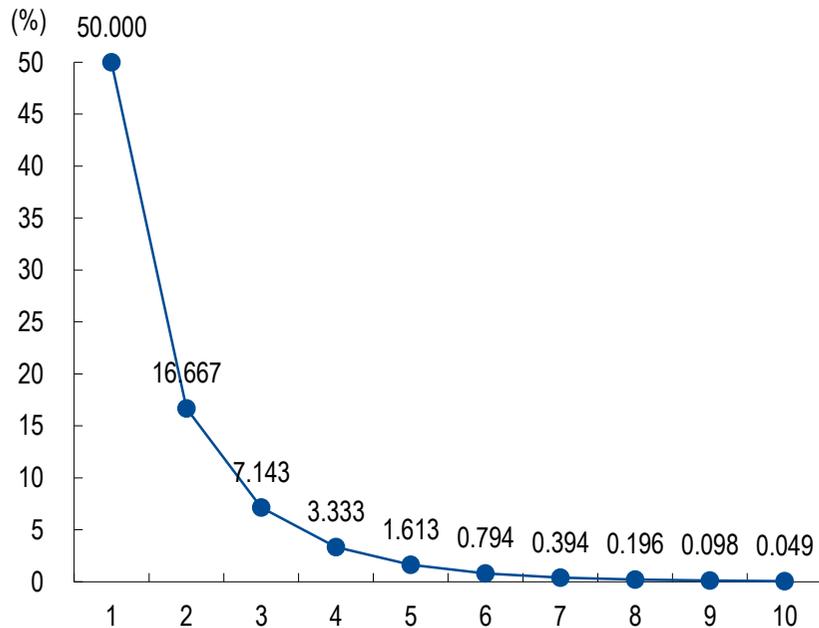


자료: NH투자증권 리서치본부

향후 반감기로 인해 가격이 상승할지는 확실하지 않음

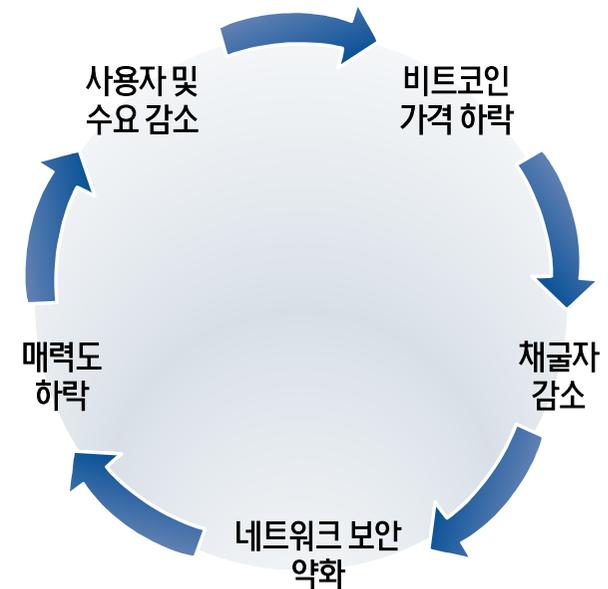
- 비트코인 초기에는 신규 비트코인 채굴로 인한 수급 부담이 상당했음. 채굴이 진행될수록 신규 비트코인이 기존 유통량에 미치는 영향은 감소하는 중. 반감기로 인한 우호적 수급에 미치는 영향력도 마찬가지로 감소할 수 있음
- 오히려 반감기로 인해 보상은 절반이 되는데 가격이 두 배가 되지 않는다면, 채굴자 입장에서는 채굴 유인 감소 효과가 나타날 수도. 반감기 이후 가격 상승은 확실하지 않음

‘금번 반감기 사이클 채굴 예정량 / 기존 채굴된 총량’ 비율



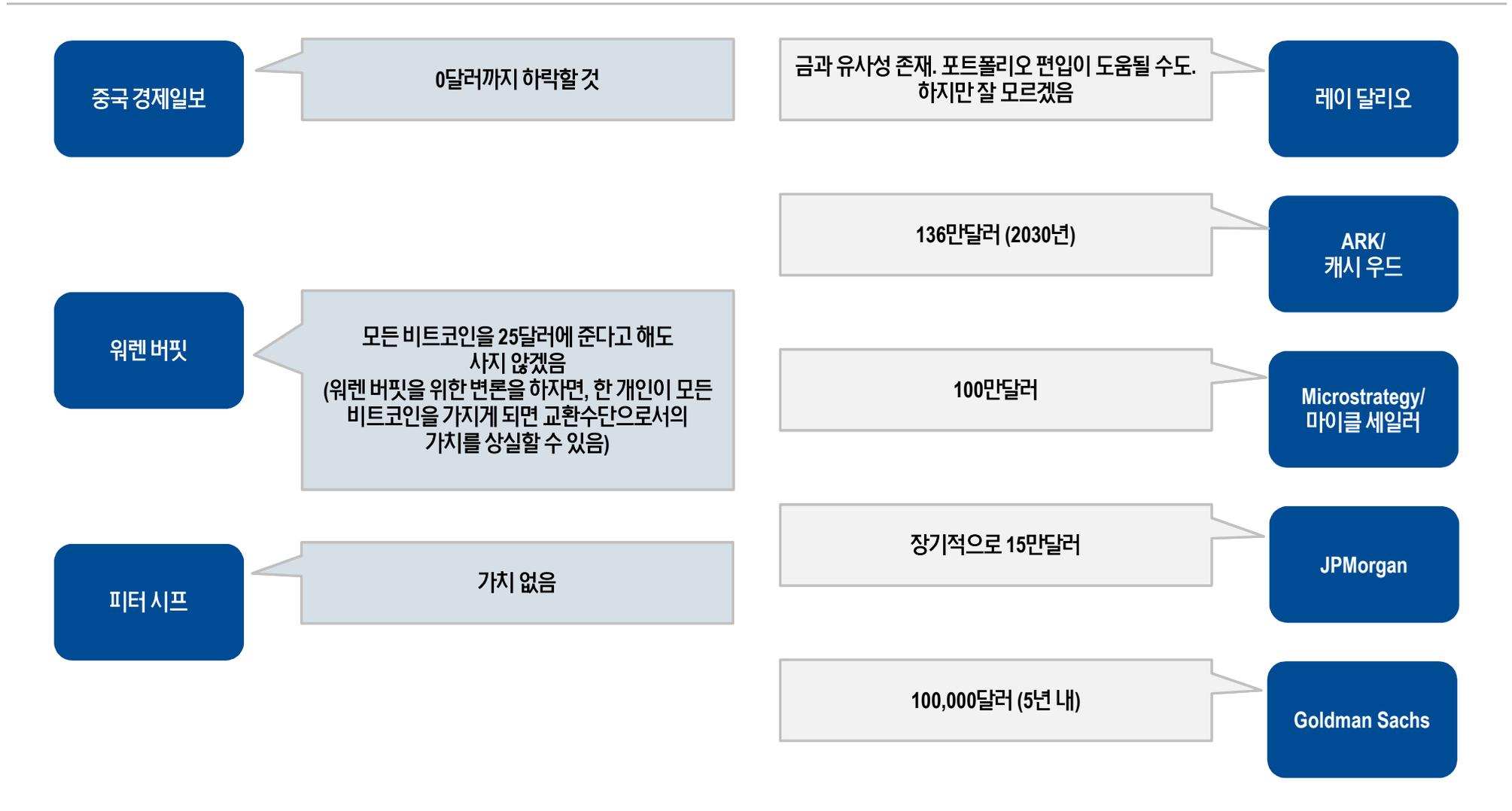
주: x축은 몇 번째 반감기 사이클인지
 자료: NH투자증권 리서치본부

비트코인 악순환 고리



자료: NH투자증권 리서치본부

주요 기관 및 인사들의 비트코인 가격 전망



대표적인 밸류에이션 방식과 그 문제점

- 비트코인 가격 추정에는 여러 방식이 활용되며 통일된 기준이 없음. 기술적 분석, 수급, 심리지표 등에 따른 추정을 제외하고, 널리 쓰이는 주요 밸류에이션 방식과 단점은 아래와 같음

기준	해결하는 경제 문제	네트워크 효과	유사자산(ex. 금) 비교	채굴 비용
설명	글로벌 송금 수수료를 얼마나 절감하는지. 혹은 관련 기업인 Visa, Mastercard 등의 시가총액과 비교	사용자 기반이 증가할수록 비트코인 네트워크의 가치도 증대	금 시가총액의 특정 비율(예 10%)에 해당하는 가치를 지닌다고 추정	비트코인 채굴에 들어가는 비용이 비트코인의 원가
단점	단순 송금 용도라면 더 효율적인 디지털 자산들 존재. 탈중앙화 등의 가치가 반영되지 않음	사용자 기반을 가격으로 환산하는 과정 필요	귀금속이자 외환보유고로도 쓰이는 금과 다른 면도 많음. 금 전체 시총과 비교해야 할지 귀금속 수요 등을 제외한 가치저장수단으로서의 금 시총에 비교해야 할지도 모호	시장가격이 언제나 상품의 원가 이상으로 형성되지는 않음. 보통 비트코인 가격을 채굴 비용이 역으로 추종

금과 비교한 비트코인의 가치

- 비트코인은 가치의 저장 수단으로서 금의 수요를 일정부분 대체할 수 있다는 주장이 수년간 지속되어 왔음
- 현재 비트코인 시가총액은 금 시가총액 대비 약 3.95%를 차지
- 금의 수요 중 투자수요는 약 42%로 이 중 절반 정도를 비트코인이 대체 시 비트코인 가격은 10만달러선까지 상승 가능하다는 주장이 있음

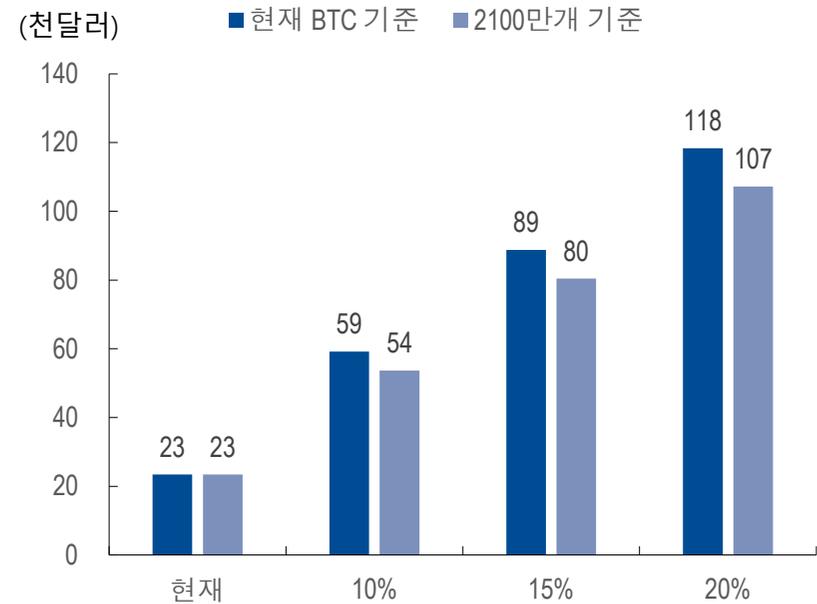
금의 수요 분포: 약 42%가 투자 수요(Investment)

Composition of average annual net demand*



주: 2020년까지 10년간 연평균 수요 분석
 자료: World Gold Council, NH투자증권 리서치본부

금 시가총액과 비교한 비트코인 가격 Simulation



자료: NH투자증권 리서치본부

비트코인 사용자 기반 확대 모니터링에는 ‘활성 주소’ 지표 활용이 적절

- 활성 주소(Active Address)란 당일 비트코인을 송금하거나 받은 기록이 있는 주소(개인 계좌 개념)를 뜻하며 DAU(Daily Active User) 지표와 유사. 이는 비트코인 사용자 기반의 확대를 나타내는 핵심 지표라는 판단
- 2017년까지 활성 주소 수가 가파르게 증가한 점이 비트코인 가격 상승을 이끌었으며 2021년 초까지 다시 증가한 바 있음. 다만, 전 고점을 유의미하게 넘지 못함. 추가적으로 법정화폐로 채택하는 국가들이 등장하거나 주요 기업들이 결제 수단으로 채택한다면 지표 개선 가능

활성 주소(Active Address) 추이: 비트코인 도입 핵심 지표



주: Active Address란 비트코인 주소로서 당일 비트코인을 송금하거나 받은 기록이 있는 주소. DAU 지표와 유사
자료: Messari, NH투자증권 리서치본부

거래 건수(Transaction) 추이: 사용자 기반 추이를 대체로 추종



자료: Messari, NH투자증권 리서치본부

네트워크 효과를 중심으로 본 밸류에이션 예시

- 비트코인을 플랫폼에 비유해 사용자 기반 증가가 네트워크 효과를 일으키며 가치 상승으로 이어진다고 가정. 비트코인의 사용자가 지속 증가할 것으로 예상된다면 활성 주소(AA)당 비트코인 가격(P)의 비율(P/AA)도 상승할 것
- 비트코인이 유의미한 상품으로 취급된 이후, 시장이 긍정적일때는 활성 주소의 0.017배 수준에서 가격이 형성되었으며 부정적일때는 0.05배 부여. 중단기적으로 활성 주소 수 가정 및 P/AA 비율 간의 매트릭스를 제시하면 하단 오른쪽 표와 같음

‘비트코인 가격/활성 주소’ (P/AA) 비율



주: Active Address란 비트코인 주소로서 당일 비트코인을 송금하거나 받은 기록이 있는 주소. DAU 지표와 유사
 자료: Messari, NH투자증권 리서치본부 계산

시나리오별 밸류에이션

(단위: 달러)		활성 주소 수 가정		
		100만개	200만개	400만개
‘비트코인 가격/ 활성 주소’ 비율 (P/AA)	부정적 (0.005)	5,000	10,000	20,000
	중간 (0.011)	11,000	22,000	44,000
	긍정적 (0.017)	17,000	34,000	68,000

자료: NH투자증권 리서치본부

장기적으로 자산 포트폴리오 편입 가능

비트코인	정의	‘P2P 전자 화폐’가 의도된 바. 디지털 금에 비유
	핵심 특징	탈중앙화, Proof-of-Work 합의
	쟁점들	화폐 여부, 기후위기 촉발 여부
투자자 관점에서 비트코인	투자 가능 방법	비트코인 현물, 비트코인 관련 ETF, (탄소중립) 채굴 기업 등
	투자 걸림돌	수탁, 회계, ESG 우려, 변동성, 부정적 인식
	네트워크 펀더멘털	활성 주소 수(Active Address), 거래건수(Transaction) (신흥국들의 법정화폐 채택이나 주요 기업들의 결제 지원으로 증가 가능)
	밸류에이션	다양한 방식이 있지만 장기 투자자들에게는 사용자 기반 확대가 중요

장기적으로 자산 포트폴리오 편입 가능

-
- 당사는 자료 작성일 현재 동 자료상에 언급된 기업들의 발행주식 등을 1% 이상 보유하고 있지 않습니다.
 - 당사는 동 자료를 기관투자가 또는 제3자에게 사전 제공한 사실이 없습니다.
 - 동 자료의 금융투자분석사와 배우자는 자료 작성일 현재 동 자료상에 언급된 기업들의 금융투자상품 및 권리를 보유하고 있지 않습니다.
 - 동 자료에 게시된 내용들은 본인의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 작성되었음을 확인합니다.
-