

# 저에 대해서

## 개발자가 된 길

- 2017년 서울 비트코인 맷업 참여  
([meetup.com/seoulbitcoin](https://www.meetup.com/seoulbitcoin))

# 저에 대해서

## 개발자가 된 길

- 2017년 서울 비트코인 맷업 참여  
([meetup.com/seoulbitcoin](https://www.meetup.com/seoulbitcoin))
- 2019년 오픈소스 비트코인 기여 시작

# 저에 대해서

## 개발자가 된 길

- 2017년 서울 비트코인 맷업 참여  
([meetup.com/seoulbitcoin](https://www.meetup.com/seoulbitcoin))
- 2019년 오픈소스 비트코인 기여 시작
- 2020년 비트코인 개발 지원금 받기 시작



# 비트코인 노드에 대해서

노드의 역할, 개발 프로세스

# 비트코인의 특장점

꼭 지켜야만 하고 태협이  
불가한 특성

# **Trustlessness**

**무 신뢰성**

**무 신뢰성이란?**

나만 믿는 것

**“Of Bitcoin’s many properties, **trustlessness**, or the ability to use Bitcoin without trusting anything but the open-source software you run, is, by far, king”**

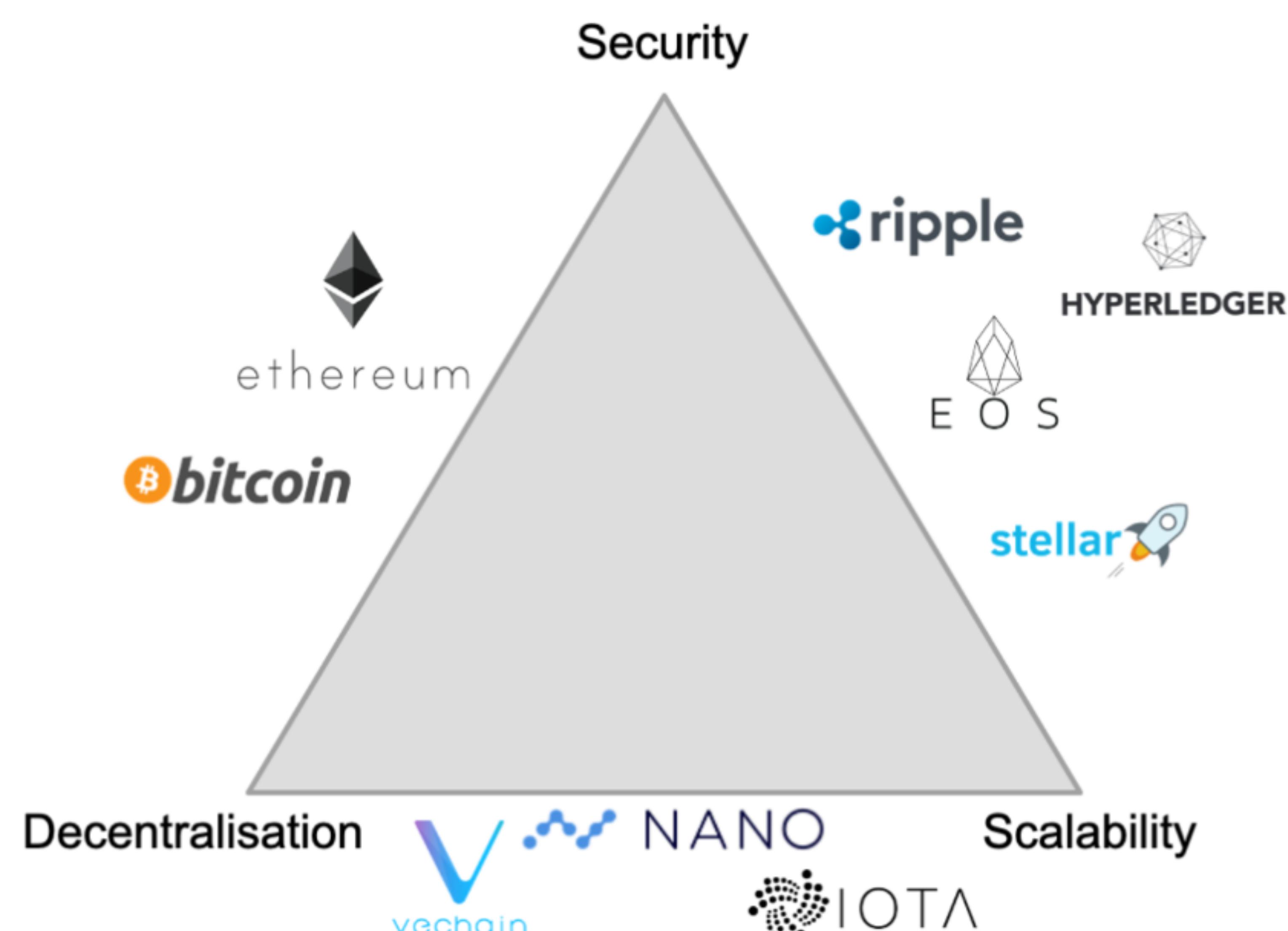
<https://bluematt.bitcoin.ninja/2017/02/28/bitcoin-trustlessness/>

“비트코인의 많은 속성들 중에서, **무 신뢰성**, 즉 스스로 운영하는 오픈소스 소프트웨어 외에는 아무것도 신뢰하지 않고 비트코인을 사용할 수 있는 속성이 최우선이다”

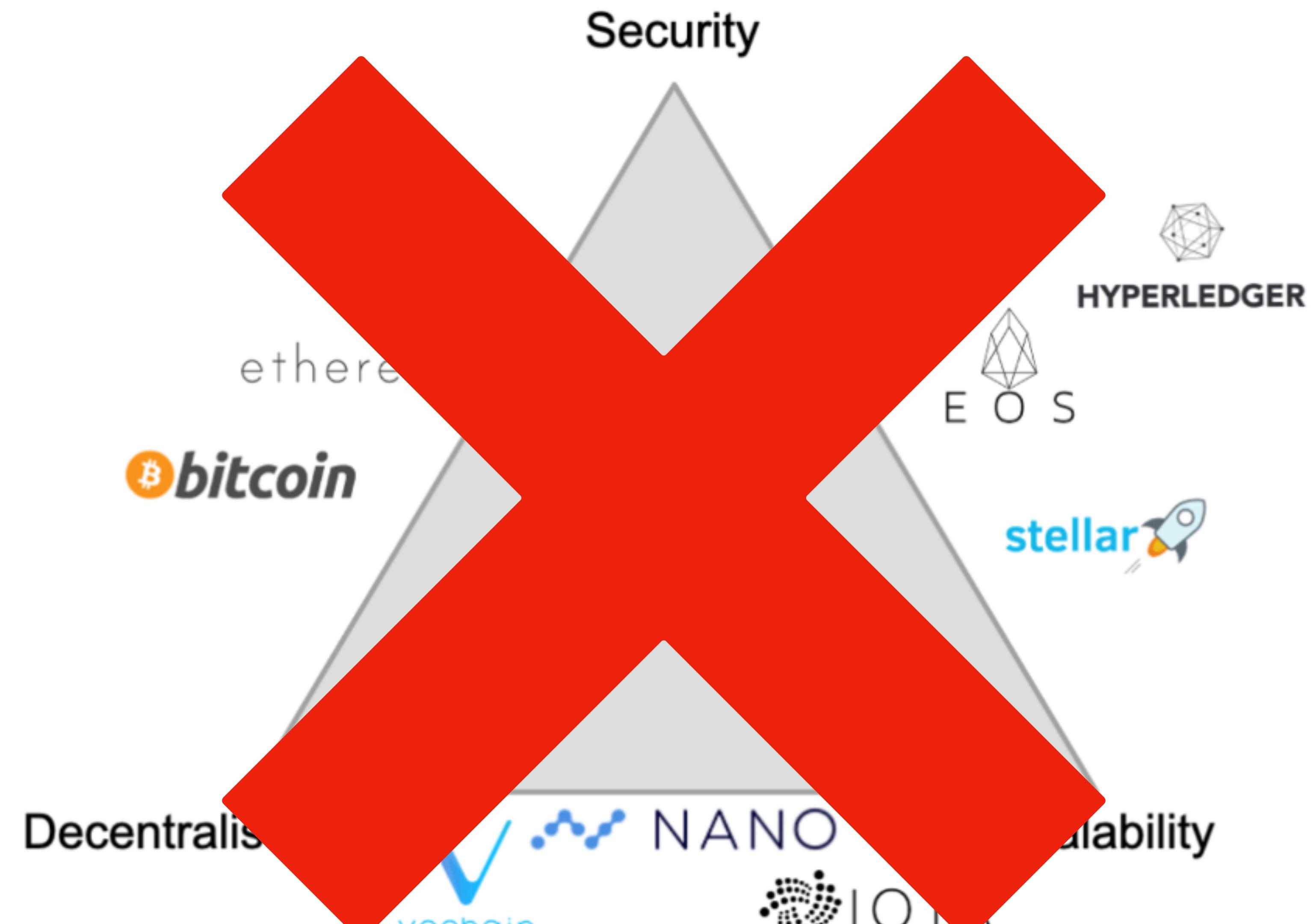
<https://bluematt.bitcoin.ninja/2017/02/28/bitcoin-trustlessness/>

- 탈중앙성
- P2P
- 셀프 커스터디

**무신론성을 해치는 것들은  
반대된다**



이미지 출처: Quai Network



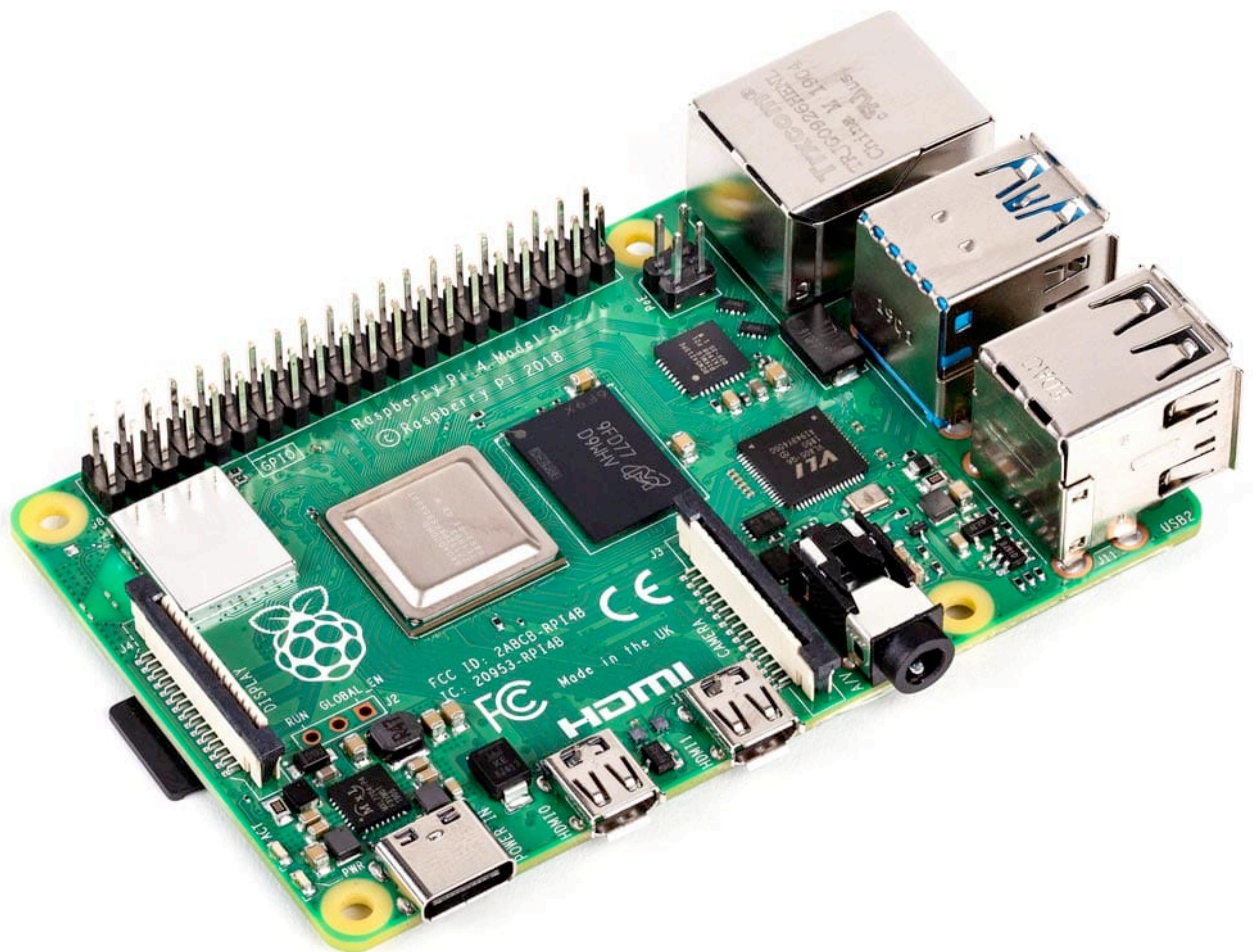
이미지 출처: Quai Network

**비트코인은 무 신뢰성 때문에 특별하다**

# 무신뢰로 비트코인 사용하기

# 노드를 사용

무 신뢰로 비트코인을 사용할 수 있는 유일한 방법





## node

미국식 [noʊd]  영국식 [nəʊd] 

명사

1 (나무줄기의) 마디

2 (뿌리·가지의) 옹이[혹]

3 (연결망의) 교점[접속점]

a network **node**  

통신망의 교점

영어사전 다른 뜻 1



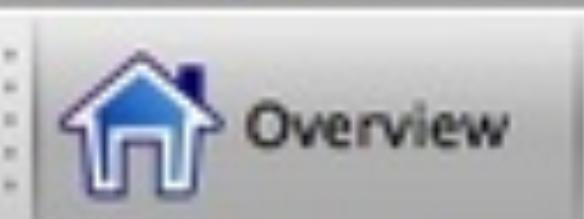
# 비트코인 노드란?

- 비트코인 네트워크에 참여하는 컴퓨터

# 비트코인 노드란?

- 비트코인 네트워크에 참여하는 컴퓨터
- 블록과 트랜잭션을 검증 및 전파

비트코인 지갑은 원래 비트코인  
노드였다



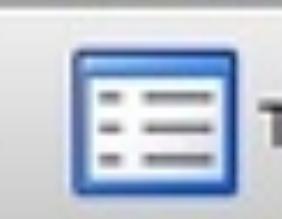
Overview



Send



Receive



Transactions

**Wallet (out of sync)**Available: **0.0002496 BTC**Pending: **0.00 BTC**Total: **0.0002496 BTC****Recent transactions (out of sync)**

10/12/13 10:28

+0.0001696 BTC

BitVisitor



10/12/13 03:47

+0.00008 BTC

BitVisitor

<https://www.bitcoin-en.com/install-bitcoin-qt-faster.html>**take days to sync**

Synchronizing with network...



# How long should synchronizing your wallet for the first time take?

Asked 12 years ago

Modified 7 years, 6 months ago

Viewed 56k times



12

What is the normal synchronizing time for your wallet when you first start? I am using 4G on a wireless and it seems to be taking forever to count down the number of blocks left until it is properly synchronized.



synchronization



Share Improve this question Follow

edited Sep 20, 2013 at 12:10



Murch ♦

78.8k • 36 • 190 • 646

asked May 18, 2013 at 14:31



john

121 • 1 • 1 • 3



Author

Topic: Which bitcoin wallet is the best? (Read 25892 times)

**klintay (OP)**

Legendary



Activity: 1771

Merit: 1032



Value will be measured in sats



**Which bitcoin wallet is the best?**

February 18, 2014, 07:56:40 AM

---

I was wondering out of the four wallets listed on [www.bitcoin.org](http://www.bitcoin.org), which is the best?

1. Bitcoin-Qt
2. Multibit
3. Armory
4. Electrum

I personally have always used bitcoin-Qt but it is very safe as long as you encrypt and p  
one drawback is it takes forever to download the whole blockchain first time around. I h  
go you have a working wallet. No need to download blockchain or any of that.

Opinions?



---

Tips - bc1qwnmtf9k2d97q98ywwkv9lkpzfnzfa83gcg93tu

**“I personally have always used bitcoin-Qt... However one drawback is it takes forever to download the whole blockchain first time around.”**

**“klintay”**

“저는 개인적으로 항상 비트코인-Qt를 사용해왔습니다... 하지만 단점 중 하나는 처음에 전체 블록체인을 다운로드하는 데 시간이 정말 오래 걸린다는 점입니다.”

“klintay”

<https://bitcointalk.org/index.php?topic=472453.0>

# **블록 다운로드**

**처음 비트코인 지갑을 사용할때 하는 것**

## **1. 블록 다운로드**

# 블록 다운로드

처음 비트코인 지갑을 사용할때 하는 것

1. 블록 다운로드

2. 블록 PoW 검증

# **블록 다운로드**

**처음 비트코인 지갑을 사용할때 하는 것**

**1. 블록 다운로드**

**2. 블록 PoW 검증**

**3. 블록 트랜잭션 검증**

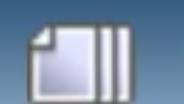
# 블록 다운로드

처음 비트코인 지갑을 사용할때 하는 것

1. 블록 다운로드
2. 블록 PoW 검증
3. 블록 트랜잭션 검증
4. 내 지갑에 비트코인이 왔는지 찾아보기

**속도**

사람들은 빠른것을 좋아한다



Author

Topic: [ANNOUNCE] Electrum - Lightweight Bitcoin Client (Read 274821 times)

**ThomasV** (OP)

Legendary



November 05, 2011, 08:44:57 AM

Last edit: January 05, 2013, 03:24:26 PM by ThomasV

*Merited by ABCbits (100), suchmoon (50), LoyceV (42), Husna QA (10), DireWolfM14 (4), o\_e\_l\_e\_o (4), HI-TEC (4)*

Activity: 1896

Merit: 1355

**ELECTRUM**

[updated october 2012]

Electrum is an easy to use Bitcoin client. It protects you from losing coins in a backup mistake or corruption. You can store your coins on paper or learn by heart. There is no waiting time when you start the client, because it does not download the blockchain.

Link: <http://electrum.org>**Features:**

- \* **Safe:** Your private keys are encrypted and stored locally.
- \* **Forgiving:** Your wallet can be recovered from a secret seed.
- \* **Instant on:** Your client does not download the blockchain, it uses a remote server.
- \* **No downtimes:** Several public servers are available, you can use any of them.
- \* **Ubiquitous:** You can run the same wallet on different computers, all instances remain synchronized.
- \* **Tested and audited:** Electrum is open source and was first released in November 2011.

---

[Electrum](#): the convenience of a web wallet, without the risks

<https://bitcointalk.org/index.php?topic=50936.0>

# **Electrum 지갑의 등장**

**첫 SPV의 구현**

- 2011-11-05일에 공개

# **Electrum 지갑의 등장**

## **첫 SPV의 구현**

- 2011-11-05일에 공개
- 블록체인을 다 받지 않아도 지갑을 사용할 수 있게 함

# **Electrum 지갑의 등장**

## **첫 SPV의 구현**

- 2011-11-05일에 공개
- 블록체인을 다 받지 않아도 지갑을 사용할 수 있게 함
- 처음으로 검증 없이 비트코인 지갑을 가질 수 있게 됨

# **Electrum 방식**

**처음 비트코인 지갑을 사용할때 하는 것**

## **1. 블록 헤더 다운받기**

# **Electrum 방식**

**처음 비트코인 지갑을 사용할때 하는 것**

- 1. 블록 헤더 다운받기**
- 2. 블록 PoW 검증**

# Electrum 방식

처음 비트코인 지갑을 사용할때 하는 것

1. 블록 헤더 다운받기
2. 블록 PoW 검증
3. 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기

# **Electrum 방식**

**처음 비트코인 지갑을 사용할때 하는 것**

- 1. 블록 헤더 다운받기**
- 2. 블록 PoW 검증**
- 3. 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기**
- 4. 서버에서 보낸 증명 검증**

**보안이 약해진다**

**Electrum 방식 지갑 사용시**

# Electrum 방식

처음 비트코인 지갑을 사용할때 하는 것

1. 블록 헤더 다운받기
2. 블록 PoW 검증
3. 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기
4. 서버에서 보낸 증명 검증

# Electrum 방식

처음 비트코인 지갑을 사용할때 하는 것

1. 블록 헤더 다운받기
2. 블록 PoW 검증
3. 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기
4. 서버에서 보낸 증명 검증

블록 헤더 다운받기

블록 PoW 검증

- 채굴자들을 신뢰하게 됨

## 블록 헤더 다운받기

## 블록 PoW 검증

- 채굴자들을 신뢰하게 됨
- 비트코인의 규칙이 틀려도 PoW만 맞으면 유효한 체인으로 인정 (블록 보상 추가로 받기 등)

## 블록 헤더 다운받기

## 블록 PoW 검증

- 채굴자들을 신뢰하게 됨
- 비트코인의 규칙이 틀려도 PoW만 맞으면 유효한 체인으로 인정 (블록 보상 추가로 받기 등)
- 비트코인 캐시같은 포크체인 블록도 유효하다고  
받음

**“In particular, it assumes that both branches of a fork are valid from the perspective of a SPV wallet, because they both follow the Bitcoin rules.”**

**“특히, SPV 지갑의 관점에서는 포크의 두 파생이 비트코인 규칙을 따르기 때문에 유효하다고 간주합니다.”**

내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기

- 프라이버시 약화

# 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기

- 프라이버시 약화
- 어느 비트코인 주소가 어디로 돈을 보냈는지 추적 가능

[Products](#)[Industries](#)[Services](#)[Insights](#)[Company](#)[Log in](#)[Request a demo](#)

# Blockchain intelligence for investigations, risk, and security

From reactive to proactive, monitor fraud, pursue illicit activity, and detect and deter threat actors.

[Request a demo](#)

<https://www.chainalysis.com>

# 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기

- 프라이버시 약화
- 어느 비트코인 주소가 어디로 돈을 보냈는지 추적 가능
- $1 \text{ BTC} = 1 \text{ BTC}$  가 아니게 됨

# 케이스 스터디: 레딧 유저의 Coinbase 계정 정지사건

## 1 BTC = 1 BTC?

1. 유저가 Coinbase 거래소에서 비트코인을 구매

# 케이스 스터디: 레딧 유저의 Coinbase 계정 정지사건

## 1 BTC = 1 BTC?

1. 유저가 Coinbase 거래소에서 비트코인을 구매
2. 비트코인을 다른 사람에게 판매

# 케이스 스터디: 레딧 유저의 Coinbase 계정 정지사건

## 1 BTC = 1 BTC?

1. 유저가 Coinbase 거래소에서 비트코인을 구매
2. 비트코인을 다른 사람에게 판매
3. 그 사람이 비트코인을 마약구매에 사용

# 케이스 스터디: 레딧 유저의 Coinbase 계정 정지사건

## 1 BTC = 1 BTC?

1. 유저가 Coinbase 거래소에서 비트코인을 구매
2. 비트코인을 다른 사람에게 판매
3. 그 사람이 비트코인을 마약구매에 사용
4. Coinbase 거래소는 해당 유저의 계좌를 정지시킴

**마약 거래 1 BTC < 1 BTC**

## 서버에서 보낸 증명 검증

- 서버가 나는 비트코인이 있어도 없다고 할 수 있다

# 서버에서 보낸 증명 검증

- 서버가 나는 비트코인이 있어도 없다고 할 수 있다
- 실제로 비트코인을 가지고 있어도 내 지갑에서는 0으로 표기

**Electrum을 사용하면 보안이 떨어진다**

**Electrum보다  
못하다**

**현재 우리가 쓰는 대부분의 지갑**

# Electrum 방식

처음 비트코인 지갑을 사용할때 하는 것

1. 블록 헤더 다운받기
2. 블록 PoW 검증
3. 내 주소를 외부 서버에 보내서 비트코인이 왔는지 물어보기
4. 서버에서 보낸 증명 검증

# 현재 대부분 지갑들의 방식

처음 비트코인 지갑을 사용할때 하는 것

1. 내 주소를 외부 서버에 보내서 비트코인이 왔는지  
물어보기

**100% 신뢰**

**현재 대부분 지갑**

**일부 지갑들은 서버 지정 가능**



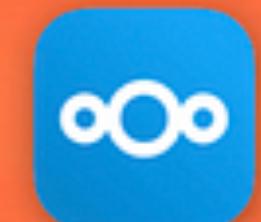
umbrel.local



# good morning, satoshi



Bitcoin Node



Nextcloud



Pi-hole



Lightning Node



Tailscale



Fulcrum



Synapse



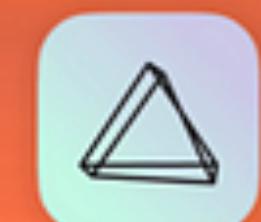
Home Assis...



Node-RED



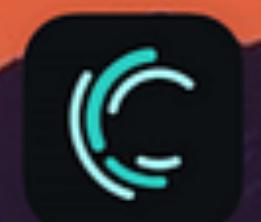
Syncthing



PhotoPrism



Urbit



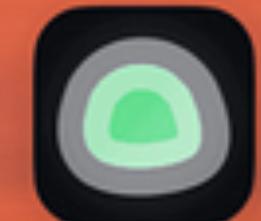
Elements



Snowflake



BTCPay



Uptime Kuma



Electrs



Core Light...



SimpleTorrent



Gitea



Vaultwarden



MANAGE APPS



무 신뢰성으로 비트코인을 사용하려면  
노드를 사용해야 한다

노드와 비트코인 네트워크

나를 위한 이유

노드를 사용하는 이유

- 보안과 프라이버시를 위해서

# 네트워크에 도움되는 이유

## 노드를 사용하는 이유

- 트랜잭션과 블록을 전파
- 비트코인 합의 규칙 강제

# 네트워크에 도움되는 이유

## 노드를 사용하는 이유

- 트랜잭션과 블록을 전파
- 비트코인 합의 규칙 강제

처음 블록을 받는 노드들에게  
도움 제공



• Running

# Bitcoin Node

Bitcoin Core 24.0.1

+ CONNECT

...

## Blockchain

Synchronized

0 %

32,852 of 790,316 blocks

## Network

Connections

10 Peers i

▼ -9%

Mempool

0 Bytes

Hashrate

10 MH/s

Blockchain Size

9 MB

↗ +8%

↗ +1%

## Latest Blocks



Block 32,772

1 transaction

13 years ago



Block 32,771

1 transaction

13 years ago



Block 32,770

1 transaction

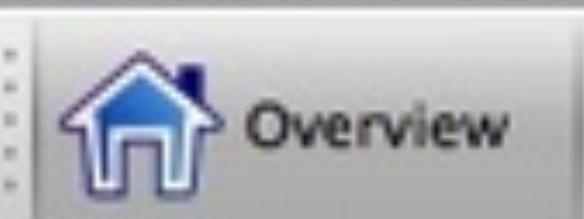
13 years ago



Block 32,769

1 transaction

13 years ago



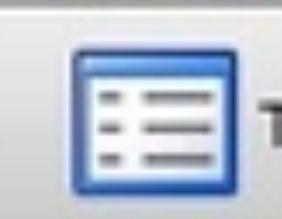
Overview



Send



Receive



Transactions

**Wallet (out of sync)**Available: **0.0002496 BTC**Pending: **0.00 BTC**Total: **0.0002496 BTC****Recent transactions (out of sync)**

10/12/13 10:28

+0.0001696 BTC

BitVisitor



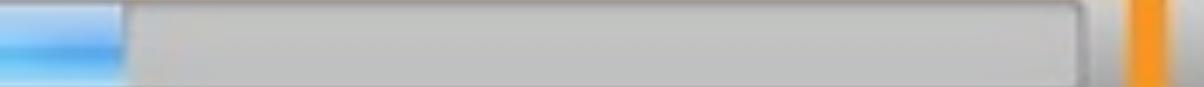
10/12/13 03:47

+0.00008 BTC

BitVisitor

<https://www.bitcoin-en.com/install-bitcoin-qt-faster.html>**take days to sync**

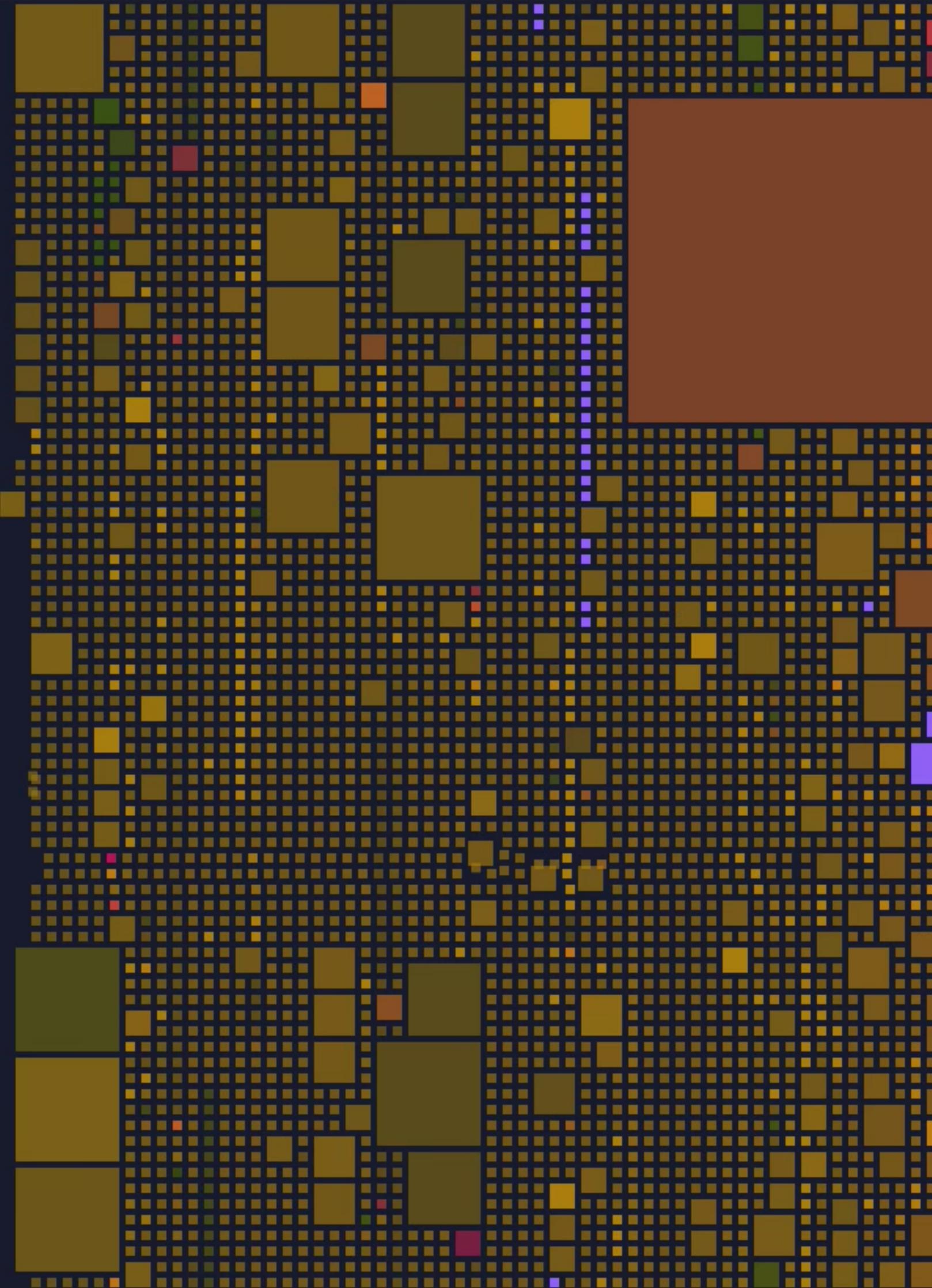
Synchronizing with network...



트랜잭션을 전파해 다른 노드들이  
수수료 계산을 가능하게 하기

# Mempool Goggles™ : All ↗

All   Consolidation   Coinjoin   Data



<https://mempool.space>

# 네트워크에 도움되는 이유

## 노드를 사용하는 이유

- 트랜잭션과 블록을 전파
- 비트코인 합의 규칙 강제

**검증을 통해 규칙에 부합하지 않는  
블록 거부**

# 규칙에 부합하지 않는 케이스들

## 블록 검증시

- PoW가 충분하지 않음

# 규칙에 부합하지 않는 케이스들

## 블록 검증시

- PoW가 충분하지 않음
- 트랜잭션의 서명이 유효하지 않거나 비트코인 양을 너무 많이 사용

# 규칙에 부합하지 않는 케이스들

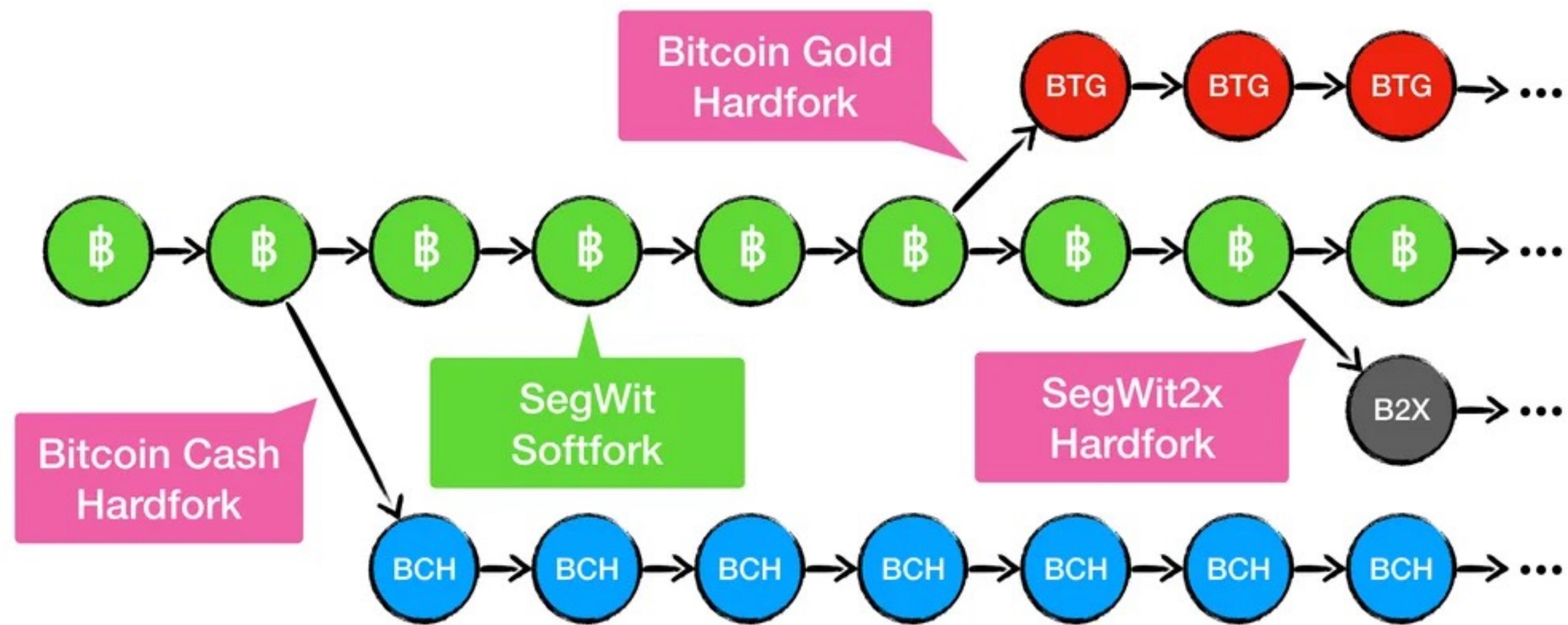
## 블록 검증시

- PoW가 충분하지 않음
- 트랜잭션의 서명이 유효하지 않거나 비트코인 양을 너무 많이 사용
- 동의하지 않는 네트워크 업그레이드 (합의 규칙 변화/ 하드포크) 후 새로운 블록들



**BitcoinCash**

# Bitcoin Forks 2017



[t.me/DivanCryptoInvestor](https://t.me/DivanCryptoInvestor)



• This article is more than 4 years old

# Australian man Craig Wright who says he created bitcoin takes £4bn claim to London high court

**Computer scientist demands 16 software developers give access to 111,000 bitcoins in case one defendant has called 'bogus'**



■ Australian computer scientist Craig Wright, who alleges he created bitcoin, has launched a London high court lawsuit demanding software developers allow him to retrieve bitcoin worth £4bn. It is his second lawsuit in three weeks. Photograph: BBC news

# Craig Wright 법정 공방

비트코인 개발자들은 비트코인을 신탁하고 있다

- 자신은 사토시 나카모토이고 사토시의 비트코인은 자신의 것이라고 주장

# Craig Wright 법정 공방

비트코인 개발자들은 비트코인을 신탁하고 있다

- 자신은 사토시 나카모토이고 사토시의 비트코인은 자신이 것이라고 주장
- 사토시의 비트코인을 관리하는 키를 잃어버렸다

# Craig Wright 법정 공방

비트코인 개발자들은 비트코인을 신탁하고 있다

- 자신은 사토시 나카모토이고 사토시의 비트코인은 자신의 것이라고 주장
- 사토시의 비트코인을 관리하는 키를 잃어버렸다
- 개발자들은 비트코인 신탁자이며 자신이 되찾을 수 있도록 비트코인 노드에 백도어를 만들어야 한다라고 주장

**소프트웨어에 해당 백도어를 넣는 것은  
가능하다**

비트코인 노드들을 강제 업데이트 시키는 것은 불가능하다

# Man convicted for repeatedly lying about inventing Bitcoin

20 December 2024

Share  Save 

**Joe Tidy**

Cyber correspondent, BBC World Service • [@joetidy](#)



Getty Images

Craig Wright attending the London High Court in February 2024

<https://www.bbc.com/news/articles/c74x0j47gz8o>

**비트코인 노드를 돌리는 것은 중요하다**



비트코인 노드를 사용하는 것이 더  
중요하다

# 왜 비트코인 노드를 사용해야 하는가

## Economic nodes (경제적인 노드들)

- 노드를 돌리기만 하면 트랜잭션과 블록 전파에만 도움이 된다

# 왜 비트코인 노드를 사용해야 하는가

## Economic nodes (경제적인 노드들)

- 노드를 돌리기만 하면 트랜잭션과 블록 전파에만 도움이 된다
- 합의 규칙을 검증하고 이 검증을 토대로 경제적인 활동이 있어야 한다

내 노드로 내 트랜잭션을 검증할때 비트  
코인 합의 규칙을 강제한다

업비트가 내 트랜잭션을 거부한다면?



업비트가 비트코인 블록 사이즈를 늘리자고 하면?



내 경제활동으로 내 노드의 규칙을  
강제한다

거래소에 비트코인을 둔다면 내 경제활동은 거래소 노드의 규칙을 강제한다

**보안, 프라이버시, 그리고 합의  
규칙을 강제하기 위해서 노드를  
사용하자**

# 노드의 개발

*"The most important book about technology today,  
with implications that go far beyond programming."*  
—Guy Kawasaki

Revised & Expanded

# THE CATHEDRAL & THE BAZAAR

MUSINGS ON LINUX AND OPEN SOURCE  
BY AN ACCIDENTAL REVOLUTIONARY



ERIC S. RAYMOND

WITH A FOREWORD BY BOB YOUNG, CHAIRMAN & CEO OF RED HAT, INC.

# 비트코인 개발

여러 개발자들의 바자회

- 하나의 로드맵은 존재하지 않는다

# **비트코인 개발**

**여러 개발자들의 바자회**

- 하나의 로드맵은 존재하지 않는다
- 서로 다른 시선으로 비트코인을 개발을 바라본다

**상대의 무 신뢰성을 해치면 안된다**

**“We must consider not only our own ability to use Bitcoin, but consider how proposed changes might require others to trust third-parties more than they currently do.”**

**<https://bluematt.bitcoin.ninja/2017/02/28/bitcoin-trustlessness/>**

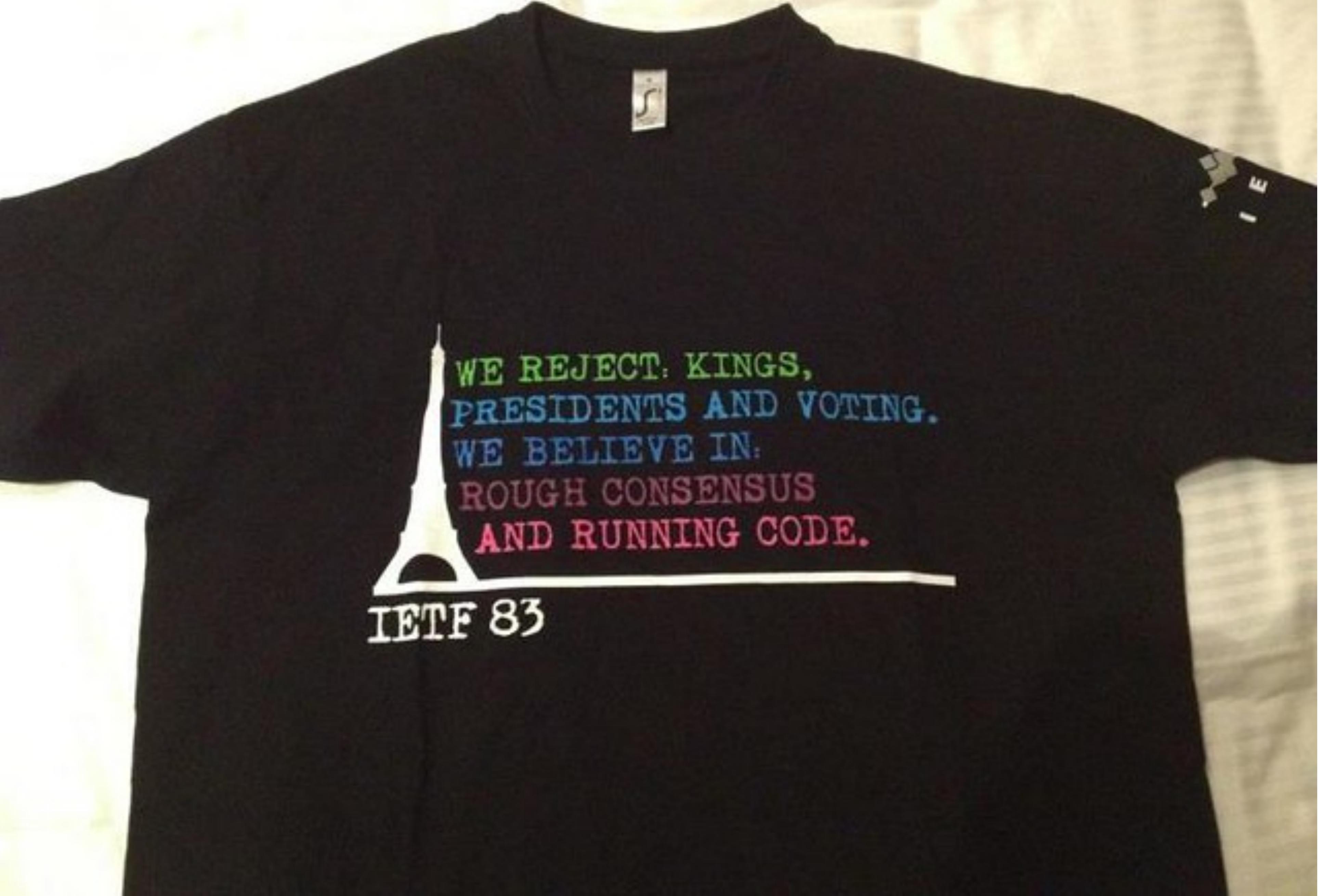
“우리는 비트코인을 사용하는 우리의 능력뿐만 아니라, 제안된 변경 사항이 다른 사람들이 현재보다 더 많은 신뢰를 제3자에게 요구하게 만들 수 있다는 점도 고려해야 합니다.”

<https://bluematt.bitcoin.ninja/2017/02/28/bitcoin-trustlessness/>

상대의 무 신뢰성을 해치지 않는 변화는  
반대할 근거가 없다

**해치는지 판단하는 프로세스?**

IETF의 Rough Consensus  
프로세스를 따른다



WE REJECT. KINGS,  
PRESIDENTS AND VOTING.  
WE BELIEVE IN.  
ROUGH CONSENSUS  
AND RUNNING CODE.

IETF 83

# Protocol Wars

文 A 3 languages ▾

Article Talk

Read Edit View history Tools ▾

From Wikipedia, the free encyclopedia



The **Protocol Wars** were a long-running debate in [computer science](#) that occurred from the 1970s to the 1990s, when engineers, organizations and nations became polarized over the issue of which [communication protocol](#) would result in the best and most robust [networks](#). This culminated in the **Internet–OSI Standards War** in the 1980s and early 1990s, which was ultimately "won" by the [Internet protocol suite](#) (TCP/IP) by the mid-1990s when it became the dominant protocol suite through rapid adoption of the [Internet](#).

**"We don't try to reach consensus in the IETF as an end in itself. We use consensus-building as a tool to get to the **best technical (and sometimes procedural) outcome** when we make decisions"**

<https://datatracker.ietf.org/doc/html/rfc7282#page-13>

“IETF에서는 합의를 그 자체가 목적이 아니라, **최고의 기술적 (때로는 절차적) 결정**을 내리기 위한 수단으로 활용합니다. 우리는 결정을 내릴 때 최선의 결과에 도달하기 위해 합의 형성 과정을 사용하는 것입니다.”

<https://datatracker.ietf.org/doc/html/rfc7282#page-13>

# 대략적인 합의란?

IETF의 Rough consensus

- 최선의 기술적인 결과를 내기 위해서 사용

# 대략적인 합의란?

## IETF의 Rough consensus

- 최선의 기술적인 결과를 내기 위해서 사용
- 투표가 아니다

**100명이 찬성하고 5명이 반대**

**5명이 찬성하고 100명이 반대**

# 대략적인 합의란?

## IETF의 Rough consensus

- 최선의 기술적인 결과를 내기 위해서 사용
- 투표가 아니다
- 만장일치가 아니여도 된다

**어디서 이 프로세스가 진행되는가?**

비트코인 메일링 리스트 (mailing list)  
에서 진행된다

# 메일링 리스트란?

비트코인 개발이 이뤄지는 곳

- <https://groups.google.com/g/bitcoindev>

# 메일링 리스트란?

비트코인 개발이 이뤄지는 곳

- <https://groups.google.com/g/bitcoindev>
- 메일링 리스트에 가입하고  
[bitcoindev@googlegroups.com](mailto:bitcoindev@googlegroups.com) 으로 이메일을 보내면 전체에게 보내진다

# 메일링 리스트란?

## 비트코인 개발이 이뤄지는 곳

- <https://groups.google.com/g/bitcoindev>
- 메일링 리스트에 가입하고  
[bitcoindev@googlegroups.com](mailto:bitcoindev@googlegroups.com) 으로 이메일을 보내면 전체에게 보내진다
- 답장도 같은 이메일로 보내면 된다

# 메일링 리스트에 보내는 것

## 대화 주제

- 비트코인 프로토콜 관련 아이디어

# 메일링 리스트에 보내는 것

## 대화 주제

- 비트코인 프로토콜 관련 아이디어
- BIP

# 메일링 리스트에 보내는 것

## 대화 주제

- 비트코인 프로토콜 관련 아이디어
- BIP
- 새 소프트웨어 릴리즈 소식

메일링 리스트에 적절하지 않으면  
[delvingbitcoin.org](http://delvingbitcoin.org)에 올린다

# 메일링 리스트 이외의 사이트

## delvingbitcoin

- 메일링 리스트에는 적절하지 않고 원래 bitcointalk  
에 올리던 주제들 올림

# **메일링 리스트 이외의 사이트**

## **delvingbitcoin**

- 메일링 리스트에는 적절하지 않고 원래 bitcointalk  
에 올리던 주제들 올림
- 프로토콜등의 아이디어 토론

**개발의 절차는 어떠한가?**

없다

일반적인 절차는 있지만 정해진  
절차는 없다

강제성



# 일반적인 프로세스

## 비트코인 개발

- 문제 정의

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각
- 해결책 구현

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각
- 해결책 구현
- BIP 또는 스펙 작성

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각
- 해결책 구현
- BIP 또는 스펙 작성
- 배포

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각
- 해결책 구현

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각
- 해결책 구현
- 배포

# 일반적인 프로세스

## 비트코인 개발

- 문제 정의
- 해결책 생각
- 해결책 구현
- 배포
- BIP 작성

**개발은 IETF의 대략적인 합의를 따르  
고 메일링 리스트에서 토론한다**

OP Return 이슈

# 배경지식

## OP\_Return 이슈

합의규칙

Policy 규칙

# 합의규칙

- 블록에 적용

# Policy 규칙

- 블록에 아직 포함되지 않은 트랜잭션에 적용

## 합의규칙

- 바꾸려면 네트워크 전체의 합의가 필요

## Policy 규칙

- 네트워크 전체의 Policy 가 불필요

## 합의규칙

- 서로 규칙이 동일하지 않으면 다른 체인이 됨

## Policy 규칙

- 서로 규칙이 동일하지 않아도 무관

## 합의규칙

- 같은 체인이라면 동일한 블록들을 받아들임

## Policy 규칙

- 같은 체인이여도 다른 트랜잭션들을 받아들임

# 배경지식

## OP\_Return 이슈

- 기본 설정값으로 Policy 규칙이 정해져 있다

# 배경지식

## OP\_Return 이슈

- 기본 설정값으로 Policy 규칙이 정해져 있다
- 대부분의 유저들은 Policy 규칙을 바꾸지 않는다

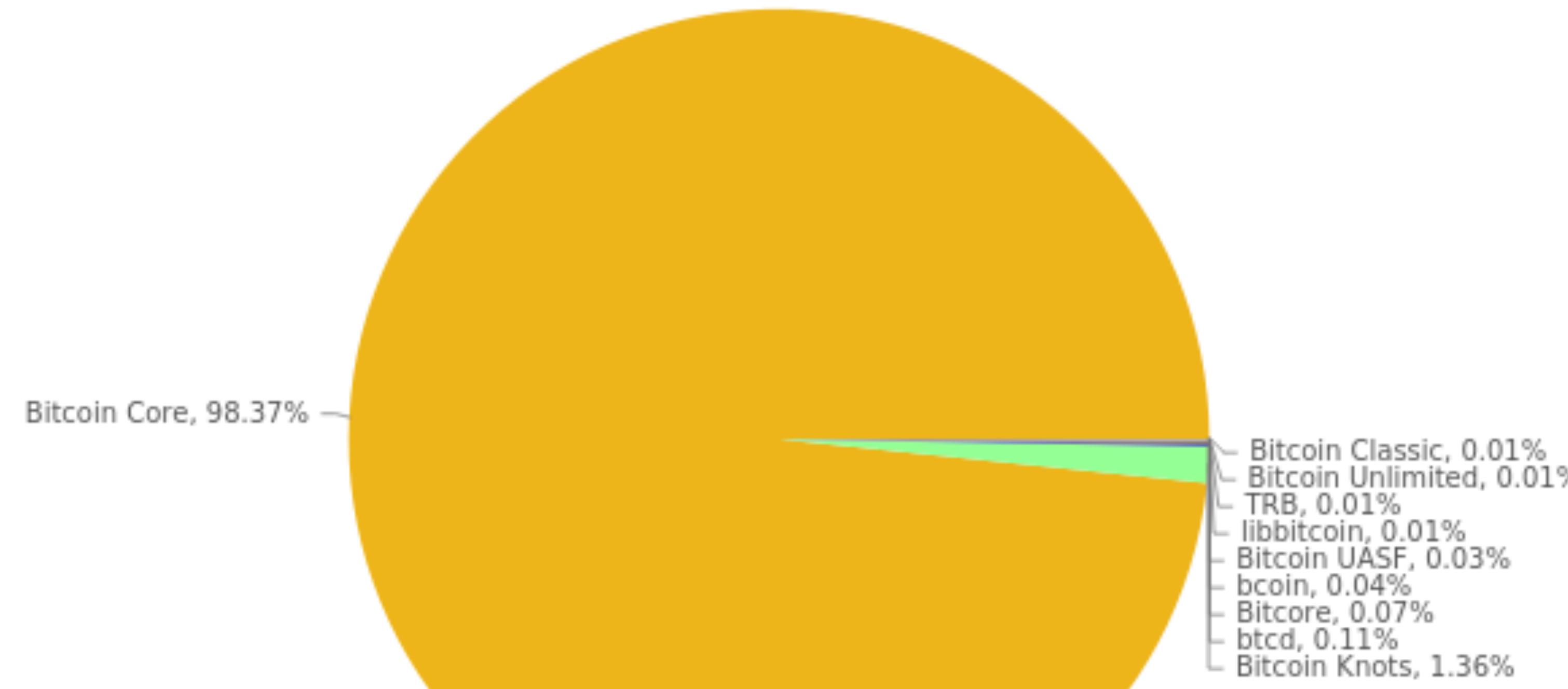
# 배경지식

## OP\_Return 이슈

- 기본 설정값으로 Policy 규칙이 정해져 있다
- 대부분의 유저들은 Policy 규칙을 바꾸지 않는다
- 대부분이 Policy 규칙을 바꾸지 않아서 기본 설정값으로 정해진 규칙을 어기는 트랜잭션은 대부분 노드들에게 전파되지 않는다

### Bitcoin Nodes (2024-06-24)

coin.dance



Bitcoin Core

Bitcoin UASF

Bitcoin Knots

libbitcoin

btcd

TRB

Bitcore

Bitcoin Unlimited

bcoin

Bitcoin Classic

<https://coin.dance/nodes/share>

대부분 Bitcoin Core 노드들이여서 이  
기본 값이 전파되는 트랜잭션을 정한다

# 배경지식

## OP\_Return 이슈

- 채굴자들은 기본 설정값을 사용하지 않는다 (Ocean 포함)

# 배경지식

## OP\_Return 이슈

- 채굴자들은 기본 설정값을 사용하지 않는다 (Ocean 포함)
- 채굴자가 아니더라도 더 자유로운 Policy 규칙을 택 할 수 있다

# 배경지식

## OP\_Return 이슈

- 채굴자들은 기본 설정값을 사용하지 않는다 (Ocean 포함)
- 채굴자가 아니더라도 더 자유로운 Policy 규칙을 택할 수 있다
- 이 노드들을 통해서 전파가 될수도 있다



slipstream.mara.com



## Direct Bitcoin Transaction Submission Portal.

MARA  
**SLIPSTREAM**

For custom blocks please contact [slipstream@mara.com](mailto:slipstream@mara.com)

MARA.COM

 SUBMIT TX

 FAQ

 TERMS

### Transaction Hex

Enter Transaction Hex: 01000000000101...

Current Slipstream minimum fee rate



3 sats/vByte

MARA  
**SLIPSTREAM**

© 2025 MARA Holdings, Inc. All rights reserved.

# 배경지식

## OP\_Return 이슈

- 채굴자들이 자신의 노드에게 트랜잭션을 직접 보내는 서비스도 제공한다



# Tonal Bitcoin

Tonal Bitcoin is a representation of the Bitcoin system aimed toward people who prefer the Tonal number system.

## Contents [hide]

- 1 Number system
- 2 As an altcoin
- 3 Specification
- 4 Compatible Clients
- 5 Guessing TBC or BTC
  - 5.1 Python
- 6 Criticism
  - 6.1 Hexadecimal could be done without new fonts as characters
  - 6.2 Not relevant to Bitcoin

# 배경지식

## OP\_Return 이슈

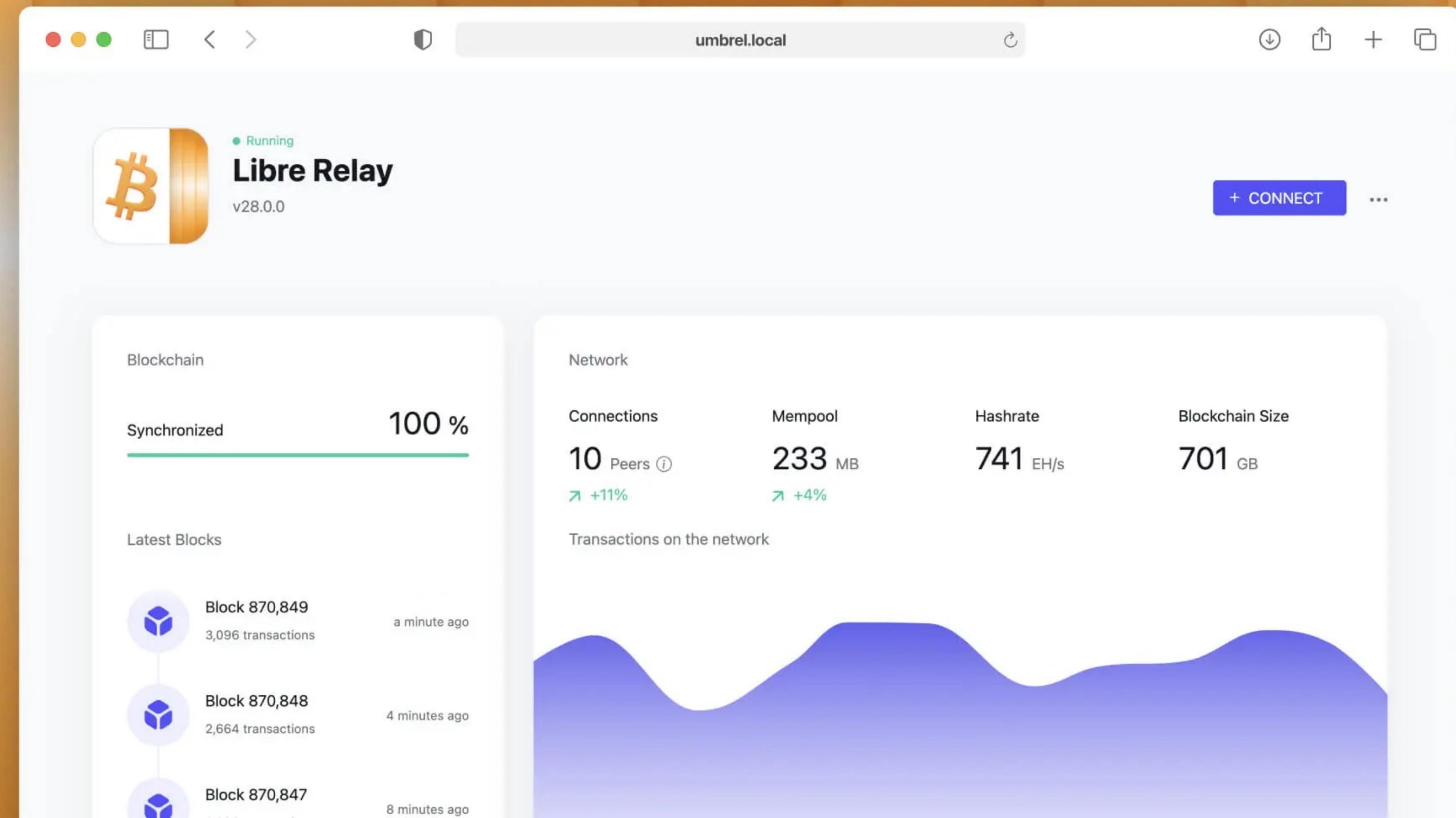
- Bitcoin Knots는 작년부터 더 제한적인 Policy규칙을 가졌다

# 배경지식

## OP\_Return 이슈

- Bitcoin Knots는 작년부터 더 제한적인 Policy규칙을 가졌다
- Ordinals 트랜잭션은 전파하지 않는다

# Run your own Bitcoin node. Powered by Libre Relay.



# 배경지식

## OP\_Return 이슈

- Bitcoin Libre Relay는 자유로운 Policy 규칙을 가졌다

# Remove arbitrary limits on OP\_Return (datacarrier) outputs

## #32359

< > Code ▾

[Jump to bottom](#)

 Closed

**peter todd** wants to merge 7 commits into `bitcoin:master` from `peter todd:2025-op-return` 

Conversation 238

Commits 7

Checks 19

Files changed 30



**peter todd** commented [3 weeks ago](#) • edited by fanquake ▾

Contributor ...

As per [recent bitcoindev mailing list discussion](#).

## 제한 찬성

- OP\_Return 제한이 넘어가는 트랜잭션은 Policy 규칙을 통해서 어느정도 제한을 할 수 있다

## 제한 반대

- OP\_Return 제한은 개인 멤풀을 장려한다

# Q&A