



# Bitcoin is Antifragile

What doesn't kill bitcoin only makes it stronger



**unchained**  
capital

# 21 Minute Crash Course

---

- **Bitcoin security function**
- **What is antifragility**
- **Social attacks**
- **Government attacks**
- **Hack attacks**
- **Volatility & Price Discovery**
- **Collective attack failure**



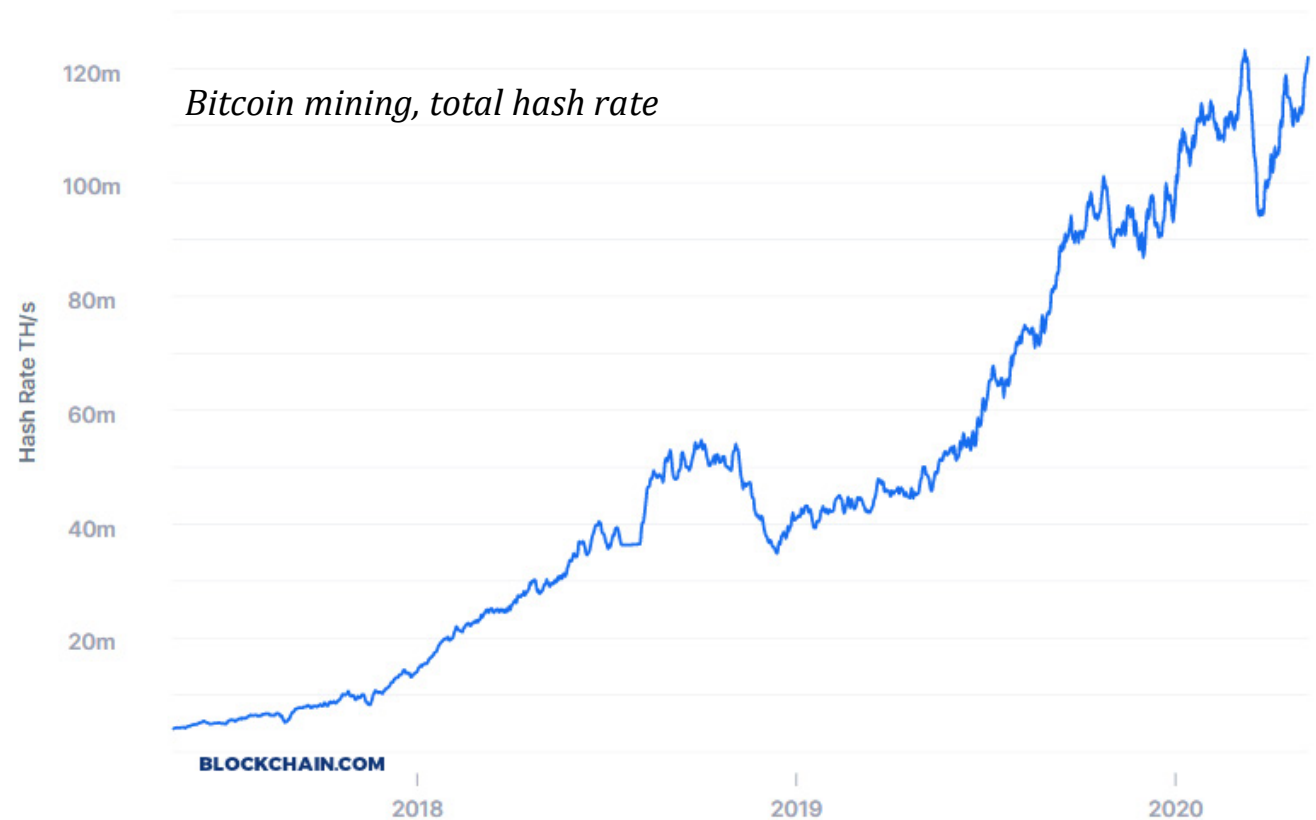
# Mining is the function most commonly associated with bitcoin's security function



Bitcoin miners validate transactions and blocks, construct blocks, and solve bitcoin's proof-of-work function, all as part of a process to write new history to the bitcoin ledger, effectively acting as bitcoin's final settlement engine.

As hash rate increases, it becomes more costly to solve bitcoin blocks and write history to the ledger; as a result, it also becomes more expensive (and practically impossible) to process invalid transactions.

Logically, if something is more expensive to attack, it is less likely to be attacked and fewer and fewer would even be capable or incentivized to attempt it.



# In reality, decentralization is bitcoin's real security model



At every layer of the network, bitcoin is becoming more decentralized over time.

As adoption increases, more people hold a smaller and smaller share of the network and value increases as a function of adoption (fixed supply + increased adoption = greater value).

As value increases, there are more resources available to further improve the network, including attracting more mining resources.

However, everything in bitcoin is ultimately dependent on decentralization and value, that is what secures the network; decentralization is what ensures there will only ever be 21 million bitcoin and adoption increases for that reason.

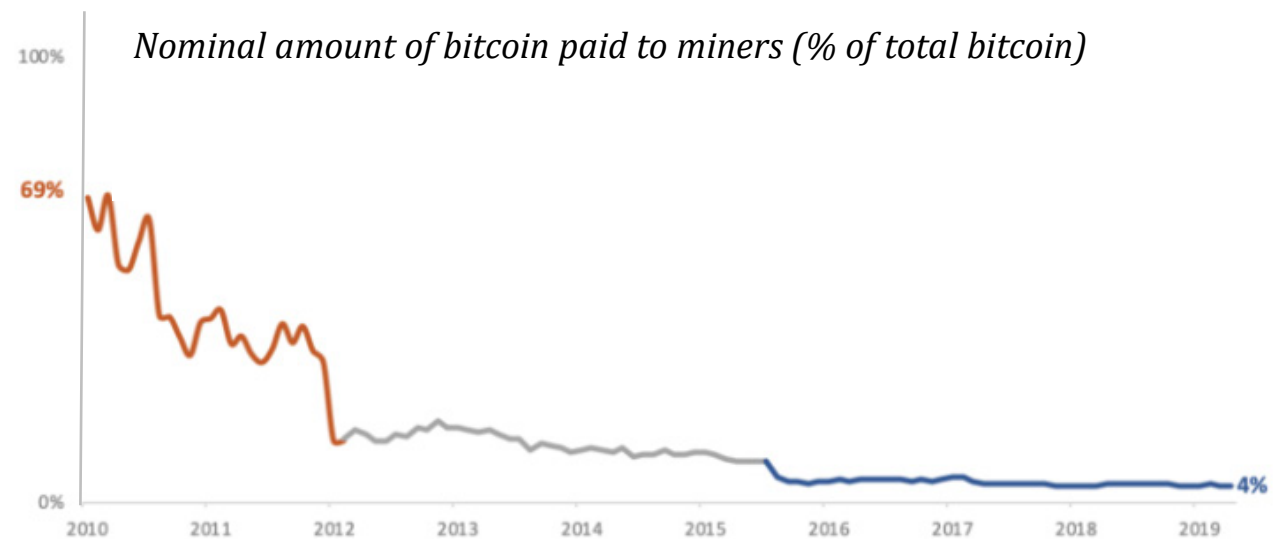
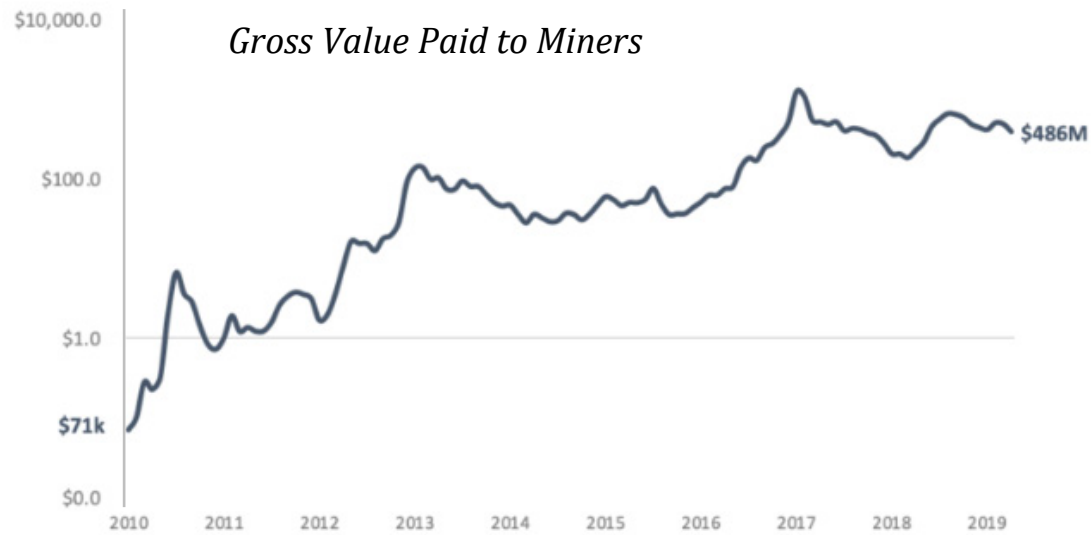




# For example, value is what affords a larger mining budget in total, despite it representing a smaller share of the economy



Value is what pays for everything; adoption drives value; decentralization drives adoption and adoption decentralizes the network; It is circular and positively reinforcing. All of this to say that bitcoin's security model is far more dynamic than merely relying on miners. Miners are paid to do a job and nothing else; bitcoin is secure because more people increasingly value it but a principal reason why more and more people value bitcoin is because trust and reliability in the network is consistently reinforced by bitcoin's antifragile nature, which only exists because of decentralization.



# Antifragility is an idea popularized by Nassim Taleb; it describes systems or phenomena that gain strength from disorder



## Antifragile, Things that Gain from Disorder – Nassim Taleb

*“Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors and love adventure , risk, and uncertainty. Yet, in spite of the ubiquity of the phenomenon, there is no word for the exact opposite of fragile. Let us call it antifragile. Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better. This property is behind everything that has changed with time: evolution, culture, ideas, revolutions, political systems, technological innovation, cultural and economic success, corporate survival, good recipes (say, chicken soup or steak tartare with a drop of cognac), the rise of cities, cultures, legal systems, equatorial forests, bacterial resistance ... even our own existence as a species on this planet. And antifragility determines the boundary between what is living and organic (or complex), say, the human body, and what is inert, say, a physical object like the stapler on your desk.*

*The antifragile loves randomness and uncertainty, which also means— crucially—a love of errors, a certain class of errors.”*

# Bitcoin is the epitome of an antifragile system; it gains from volatility, error & disorder



- Bitcoin is an adaptive and evolving system; it is not static. No one controls the network and there are no leaders capable of forcing changes onto the network. Bitcoin is decentralized at every layer and as a result, it has shown to be immune to any type of attack.
- However, it is not just immune to attack or errors, bitcoin actually becomes stronger as external forces attempt to attack or coopt the network, as individuals within the network make errors and as a function of its volatility, which is often thought of as a negative.
- As bitcoin fends off attacks and as individuals learn from errors and react to its volatility, bitcoin becomes tangibly more reliable; its demonstration of resilience and immunity actually causes trust to be reinforced in the network which fuels increasing adoption, which then makes bitcoin more resistant to attack or individual errors. It is a self-reinforcing feedback loop.
- With every failed attempt to coopt or coerce the network, the bitcoin protocol hardens and confidence increases, which ultimately reinforces the reliability of its fixed 21 million supply, which is the function that drives all value.
- Every time bitcoin doesn't die, that very event propels bitcoin forward, and in a different state that previously existed.
- None of it would be possible if not for decentralization and the fact that bitcoin becomes more and more decentralized over time.

# Antifragility – The Segwit2x Civil War



- In 2017, large service providers and miners attempted to push a hard fork on the network (referred to as Segwit2x).
- Preemptively, an individual user activated Segwit via a softfork, with no block size increase, and the Segwit2x hard fork later failed miserably.
- The Segwit2x failure did only prove bitcoin to be resilient, it also educated many on censorship resistance; the failure of Segwit2X actually made the network stronger, by proving no one was in control.

## Post-Segwit2x Fail

 **Ted Rogers** @tedmrogers

Replying to @tedmrogers and @CryptoOwl3


3/ Ironically, it was the loss of the Segwit2x debate that made me realize all this once and for all - large powerful industry threw everything at implement a seemingly innocuous change to BTC in order to relieve a (perceived) crisis. We lost, badly.

12:09 AM · Apr 24, 2018 · [Twitter for iPhone](#)

14 Retweets 58 Likes

3 14 58

 Tweet your reply

 **Ted Rogers** @tedmrogers · Apr 24, 2018

4/ the Segwit2x fail was the final victory for #bitcoin as digital gold. BTC is uncontrollable, ungovernable, and completely decentralized. Immutable. Agility & governance might help building a currency but its a liability for a store of value and for an immutable record of txs.

4 21 87

## Pre-Segwit2x Fail

 **Ted Rogers** @tedmrogers

Replying to @tedmrogers @AlyseKilleen and 7 others

To be clearer -we care deeply about censorship resistance. But does avg new user care more about that or Tx fees & speed? I think the latter

1:58 AM · Sep 7, 2017 · [Twitter for iPhone](#)

2 Likes

3 2

 Tweet your reply



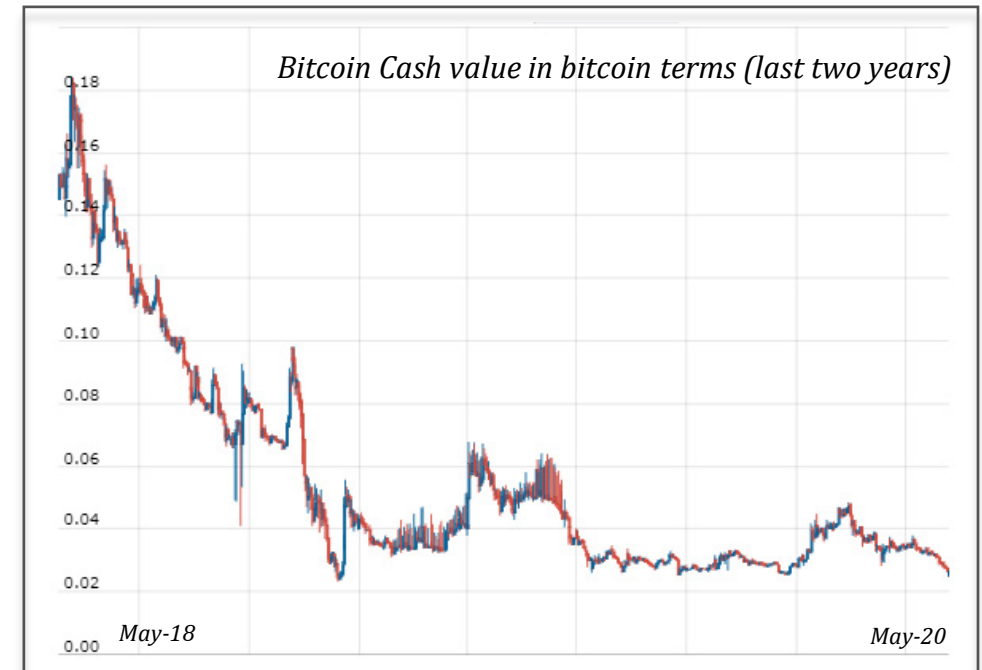
# Antifragility – The Bitcoin Cash Hard Fork



- Around the same time in 2017, a group organized by a large bitcoin miner and “Bitcoin Jesus” led a hard fork to increase the block size by 2x.
- It had many claiming and/or thinking “Bitcoin Cash” was the real bitcoin.
- The many failures of bitcoin cash have not only reinforced the strengths of bitcoin, it has educated users about consensus (what is / is not bitcoin) and demonstrated that there are no leaders in bitcoin, only strengthening confidence in the network.



“Bitcoin Jesus” fall from grace and inability to convince the consensus reinforced that no one was in control.



## List of 44 Bitcoin fork tokens since Bitcoin Cash

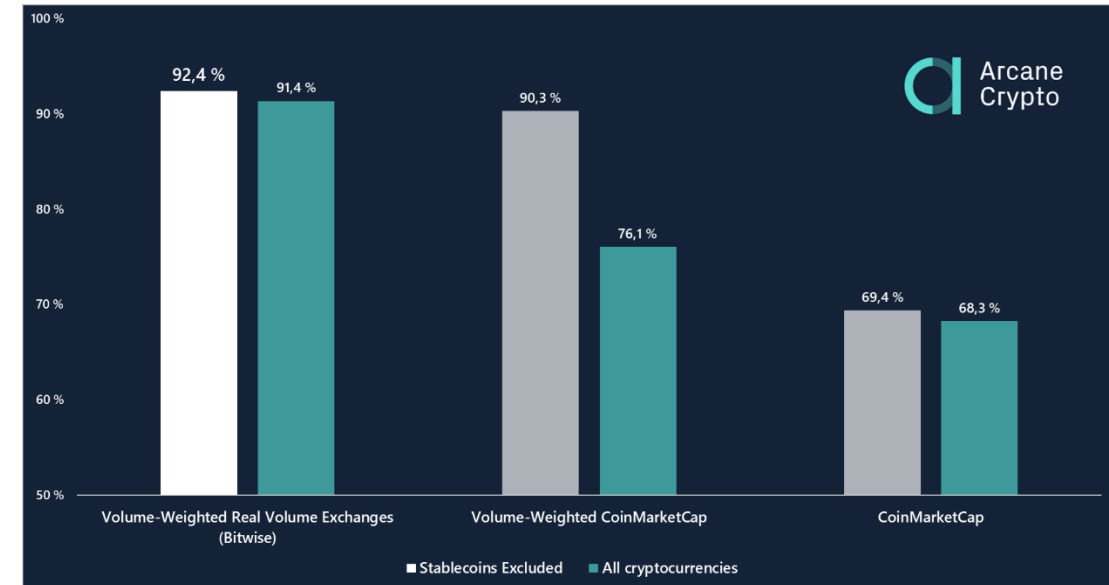
BitMEX Research 21 May 2018

**Abstract:** Although in 2018 Bitcoin may have somewhat moved on beyond this issue, in this sixth piece on consensus forks and chainsplits, we provide a list of 44 tokens which seem to have forked away from Bitcoin since the Bitcoin Cash split.

# Antifragility – Altcoin Season, Bitcoin Cannot Be Copied



- Ever since bitcoin was launched, there have been thousands of cryptocurrencies that have been launched, often attempting to improve on some perceived flaw in bitcoin; either it is too slow; it cannot support sufficient transaction throughput; it is not turing complete (too rigid / not sufficiently dynamic), etc. the list goes on.
- To be certain, in aggregate, these “copies” are attacks on bitcoin; they are attempting to improve on and replace bitcoin’s dominance. And, the existence of these thousands of cryptocurrencies is often then used to claim that bitcoin can just be copied, so therefore it is not actually scarce.
- Despite thousands of attempts, bitcoin dominance remains at 70-90% of value; one currency = 70-90% and thousands = 10-30%; whichever metric one looks at, the market is sending a clear signal: there is something different about bitcoin.
- For those actually paying attention, the existence of these competing cryptocurrencies and their poor performance relative to bitcoin, individually and collectively, reinforce that none of them are bitcoin and with each failed attempt to “flippen” bitcoin, confidence in bitcoin grows which fuels more adoption.
- *“When you strike at a king, you must kill him.” – Ralph Waldo Emerson*



Insight. News

Bitcoin’s reported market dominance is approaching 70%, but in reality it is above 90%

An analysis by Arcane Research shows how the real market dominance of bitcoin is way higher than what is traditionally reported.

# Antifragility – Government Attacks Don't Kill Bitcoin (India)



- In 2018, India's central bank (the RBI) instituted a ban, preventing any banking institution from facilitating cryptocurrency trading (including bitcoin) or servicing any companies that did facilitate such activity.
- After initially and temporarily being upheld, the Supreme Court in India struck down the legality of the central banks actions inhibiting bitcoin trading.
- This entire episode not only creates precedent but it also demonstrated that the government of a nation with a billion people could take aggressive action to limit the spread of bitcoin, without it interrupting the bitcoin network to the least.
- Ultimately, each and every attempted jurisdictional ban of bitcoin will fail to kill, or even materially harm the network, and each time it not only provides great marketing for bitcoin by legitimizing it further, it also reinforces the idea that bitcoin lives beyond governments and government's cannot stop it.
- Again, a demonstration of such a fact actually causes bitcoin to gain strength, not merely that it is resilient.

Cryptocurrencies

## Cryptocurrency Virtually Outlawed in India as Top Court Backs Ban

By [Upmanyu Trivedi](#) and [Rahul Satija](#)

July 3, 2018, 4:10 AM CDT Updated on July 3, 2018, 5:55 AM CDT

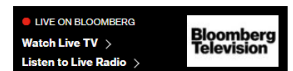
Technology

## Cryptocurrency Bourses Win India Case Against Central Bank Curbs

By [Upmanyu Trivedi](#)

March 3, 2020, 11:27 PM CST Updated on March 4, 2020, 1:41 AM CST

- ▶ RBI had barred banking services from using digital currencies
- ▶ Supreme court ruling on Wednesday struck down the RBI's curbs



# Antifragility – Government Attacks Don't Kill Bitcoin (China)



- Similarly, China has taken a number of measures to attempt to restrict bitcoin, from announcing measures to curb trading as well as desires to eliminate bitcoin mining.
- The standard headlines follow, and some attribution of bitcoin's price volatility is given to the news.
- India and China collectively have a population of 2.7 billion and bitcoin continues to thrive despite aggressive action; in many ways, it thrives because of the actions themselves. Not exclusively obviously, but the lack of any real ability to influence the bitcoin network, increases its strength.
- Not coincidentally, because the network is dynamic, it recognizes threats or risks and immunizes around them, in an entirely spontaneous order.

Markets

## Bitcoin Crashes Again After China Moves to Halt Exchange

Bloomberg News

September 14, 2017, 10:24 PM CDT

Updated on September 15, 2017, 3:55 AM CDT

- 
- ▶ Cryptocurrency has tumbled 28% this week amid crackdown
  - ▶ Exchange order follows ban on initial coin offerings
- 

CRYPTOCURRENCY

## China says it wants to eliminate bitcoin mining

PUBLISHED TUE, APR 9 2019 5:38 AM EDT

THE LEDGER • BITCOIN MINING

## Texas Bitcoin Mining Startup Gets \$50 Million From Peter Thiel to Steal China's Crypto Crown

BY JEFF JOHN ROBERTS

October 15, 2019 7:52 AM CDT



# Antifragility – Security Failures Drive Innovation (Mt. Gox)



- After already having been hacked in 2011, Mt. Gox which was one of the earliest operating bitcoin exchanges stopped all withdrawals in 2014, after a more material breach drained the majority of all bitcoin held by the exchange.
- In many immediate ways, this event was not only a black eye for bitcoin but it shook confidence in the network, despite the hack not being at the protocol level.
- Ultimately, the Mt. Gox hack that resulted in a loss of 650k in bitcoin (\$5.5 billion in today's terms but \$650 million then) materially increased the strength of the network.
- It fortified that accountability lies in the holders of bitcoin (all transactions are final so beware who you trust); new exchanges formed that utilize improved security practices and it spawned innovation in self-custody (not your keys, not your bitcoin).



OLUSEGUN OGUNDEJI

AUG 10, 2016

## Antonopoulos: Your Keys, Your Bitcoin. Not Your Keys, Not Your Bitcoin

Andreas Antonopoulos on diversifying risks after the Bitfinex hack.

Cybersecurity

## Mt. Gox Chief Executive: Bitcoin Heist Wasn't Just Hacking

By [Joshua Brustein](#)

June 27, 2014, 12:59 PM CDT

Cybersecurity

## Mt. Gox Insider's Kraken Bitcoin Exchange to Open in Japan

Pavel Alpeyev

August 17, 2014, 7:23 PM CDT





# Antifragility – Security Failures Reinforce Censorship Resistance & Accountability (Binance)



- In 2019, one of the largest bitcoin exchanges (Binance) was hacked, resulting in the loss of \$40 million bitcoin.
- Not only did this reinforce that bitcoin holders are maximally accountable for how they store bitcoin and in whom they trust, it also similarly fueled the “not your keys, not your bitcoin” rally cry; everyone learns from the failures of others.
- Most importantly though, subsequent to the hack, Binance entertained the idea of negotiating a network re-org to get back the lost funds; it ultimately “decided” against it but this was really like “pre-canceling” because it was not possible.
- The fact that it was not possible for one of the largest exchanges to reverse an otherwise valid bitcoin transaction (even a hack) reinforced the network’s property of censorship resistance, strengthening the entire network.



**CZ Binance** ♦♦♦♦  
@cz\_binance

After speaking with various parties, including @JeremyRubin, @\_prestwich, @bcmakes, @hasufl, @JihanWu and others, we decided NOT to pursue the re-org approach. Considerations being:

12:29 AM · May 8, 2019 · [Twitter Web Client](#)

Cybersecurity

## Hackers Steal \$40 Million Worth of Bitcoin From Binance Exchange

By [Eric Lam](#)

May 7, 2019, 8:56 PM CDT Updated on May 8, 2019, 4:56 AM CDT

- ▶ Deposits and withdrawals suspended pending security review
- ▶ Binance says hackers may still control some user accounts



**Adam Back** @adam3us · May 8, 2019

A Bitcoin reorg is just not happening, and I doubt any Bitcoin industry, miners nor developers considered it either. Recall 2014 \$473mil, 2016 bitfinex hack \$72mil, 2019 binance \$40mil etc. [#NotHappening](#)

54

262

1.4K



## Here's why Binance can't erase the \$40M hack from Bitcoin's blockchain

7,000 BTC was stolen, you can't undo that

# Antifragility – Volatility & Price Discovery



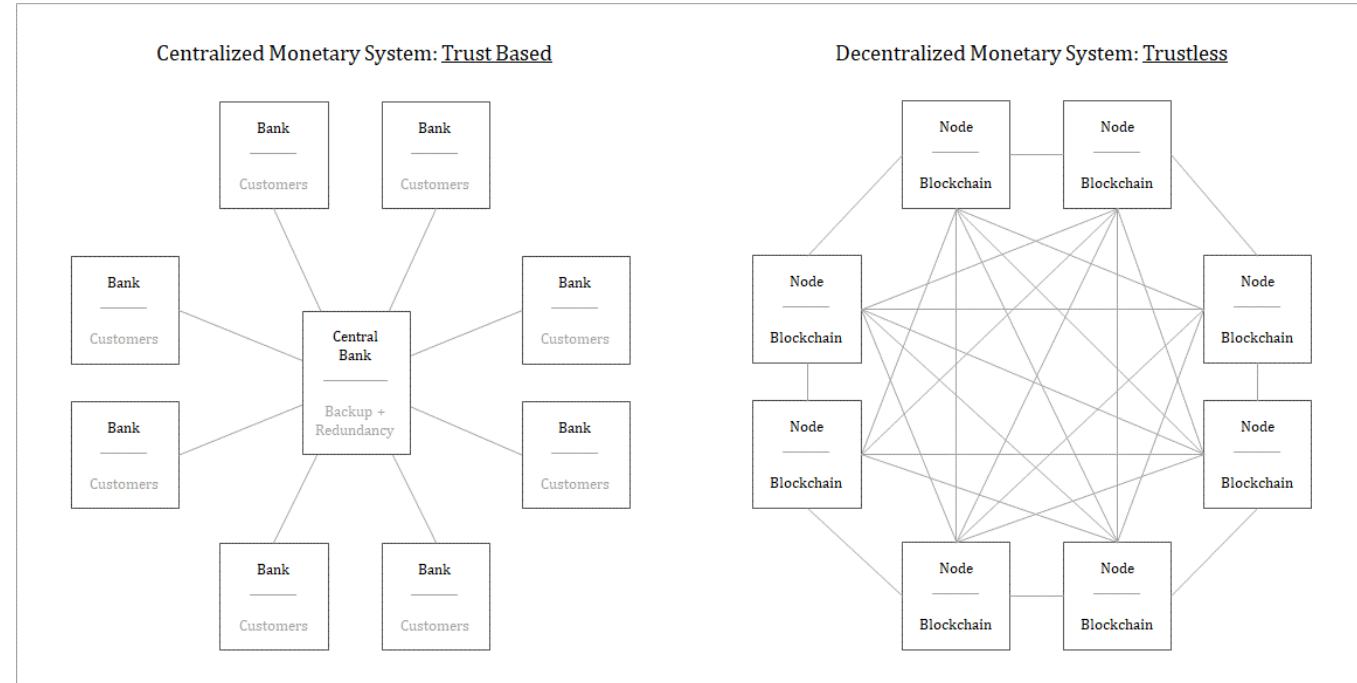
- Bitcoin volatility is often lamented as a critical flaw in its ascent to global reserve currency status; but really, volatility is a feature, not a bug.
- Volatility is price discovery and in bitcoin, it is unceasing and uninterrupted. There are no Fed market operations to rescue investors, nor are there circuit breakers.
- Everyone is maximally accountable and if caught off sides, no one is there to bail you out. Because there are no bailouts, the market is devoid of moral hazard.
- Not only is information communicated through price volatility, volatility is also how bitcoin gets distributed and becomes further decentralized. Every time a bitcoin is sold, someone else is buying. Consistently over time, the ownership of the network becomes more decentralized and this occurs most acutely in bouts of volatility.
- In very tangible ways, the volatility strengthens bitcoin by decentralizing it and reinforcing that on either side, tulips may die but bitcoin never does.



# What doesn't kill bitcoin, only makes it stronger.



- Bitcoin is not only decentralized at every layer but by its very nature, it becomes more decentralized over time.
- Decentralization and the censorship resistance that decentralization affords sits at the core of why bitcoin, as a system, is antifragile.
- No one controls the network and the level of redundancy ensures that no single attack vector or collective attack surface could successfully impede bitcoin's growth; instead, they fuel bitcoin.
- Bitcoin is a dynamic and adaptive system; security is forced out to the edge of the network, ensuring that each individual be responsible for themselves; failures result in network learnings, not death.
- There are no bailouts and it's a system devoid of moral hazard, which drives maximum accountability and long-term efficiency. Central banks manage currencies to mute short-term volatility, which creates the instability that leads to long-term volatility.
- Volatility in bitcoin (not just price) is native to its architecture and this volatility ultimately strengthens the resilience of the bitcoin network, driving long-term stability. Variation is information.



*"Some things benefit from shocks; they thrive and grow when exposed to volatility, randomness, disorder, and stressors[.]" – Nassim Taleb, Antifragile*

**In summary, Bitcoin is antifragile. It gains strength through disorder, error and volatility.**



*The central banking model trades short-term stability for long-term volatility; bitcoin trades short-term volatility for long-term stability; at the end of the day, a currency which is constantly exposed to error, disorder and volatility and gains strength by that very function. It is antifragile.*

## ***Have Questions?***

*Check out my Gradually, Then Suddenly Series,  
The Bitcoin Standard or read some Hayek*

***Need Help on Your Bitcoin  
Journey? Look us up.***

*Bitcoin Cannot Be Copied   Bitcoin is Common Sense   Bitcoin, Not Blockchain*

*Bitcoin is Not for Criminals   **Bitcoin Obsoletes**   Bitcoin is Not Too Slow*

*Bitcoin is Not a Pyramid Scheme   Bitcoin is Money   Bitcoin Does Not Waste Energy*

*Bitcoin Cannot Be Banned   **All Other Money**   Bitcoin is Not Too Volatile*

*Bitcoin is a Rally Cry   Bitcoin is Not Backed By Nothing   Bitcoin Fixes This*







## For More Information

Contact Parker Lewis ([parker@unchained-capital.com](mailto:parker@unchained-capital.com))

Unchained Capital  
201 E. 5th St., Suite 108  
Austin, TX 78701