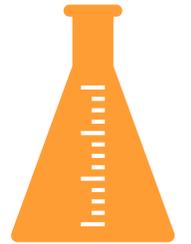


ANDREW M. BAILEY



BITCOIN ALCHEMY

RESISTANCE.MONEY

RESISTANCE.MONEY

▶ ABC

▶ @rettlerb

▶ @craigwarmke

▶ @resistancemoney

▶ Our Programme:

▶ Understand

▶ Evaluate

RESISTANCE MONEY
A BITCOIN RESEARCH COLLECTIVE

 = $\frac{V}{I}$

Twelve years ago, the Bitcoin network was launched by its pseudonymous creator. It promised a revolution in how money works. Here at last, some thought, was an inclusive digital system for storing and transferring value -- a system that was inflation-proof, censorship-resistant, and independent of any oligarchic banking cartel. Bitcoin has since spawned thousands of cryptocurrencies, and they command coverage in both popular media and technical research by computer scientists, economists, and lawyers.

The goal of this research collective is to apply the tools of philosophy, politics, and economics to understand and evaluate the cryptocurrency phenomenon in an integrated way. We favor specifics over generalities and focus on the case of the oldest, most valued, and most well-known cryptocurrency -- Bitcoin. We are:


[Andrew M. Bailey](#)
 Yale-NUS College


[Bradley Rettler](#)
 University of Wyoming


[Craig Warmke](#)
 Northern Illinois University

RESEARCH: PUBLISHED OR IN PROGRESS

- ▶ [Why Bitcoin Needs Philosophy](#) (CoinDesk)
- ▶ [What is Bitcoin?](#) (*Inquiry*)
- ▶ [Cryptocurrency: Philosophy, Politics, and Economics](#) (*Philosophy Compass*, commissioned)
- ▶ [Electronic Coins](#) (draft)
- ▶ [Bitcoin and Financial Injustice](#) [PDF] [archive]
- ▶ [Resistance Money](#) (book project)
- ▶ [A Pragmatic Case for Bitcoin](#)
- ▶ [Ethics for Bitcoin Research](#)

MEDIA

- ▶ [Bitcoin Doesn't Care About Your Politics: Why Bitcoin Has More Ideological Flexibility Than We Think](#) (podcast interview)
- ▶ [What is Bitcoin?](#) (podcast interview)
- ▶ [An Introduction to Bitcoin](#) (video)

WHY 'RESISTANCE MONEY'?

One theme in our research is that Bitcoin is a check against the authority and overreach of corporations, states, and anyone else who would serve as an intermediary between people and their money. Above all, it offers a way to elude and resist the interlocking and increasingly tight gears of institutions both private and public.

Last updated: 18 March 2021.

RESISTANCE.MONEY

▶ ABC

▶ @rettlerb

▶ @craigwarmke

▶ @resistancemoney

▶ Our Programme:

▶ Understand

▶ Evaluate

RESISTANCE MONEY
A BITCOIN RESEARCH COLLECTIVE

 = $\frac{V}{I}$

Twelve years ago, the Bitcoin network was launched by its pseudonymous creator. It promised a revolution in how money works. Here at last, some thought, was an inclusive digital system for storing and transferring value -- a system that was inflation-proof, censorship-resistant, and independent of any oligarchic banking cartel. Bitcoin has since spawned thousands of cryptocurrencies, and they command coverage in both popular media and technical research by computer scientists, economists, and lawyers.

The goal of this research collective is to apply the tools of philosophy, politics, and economics to understand and evaluate the cryptocurrency phenomenon in an integrated way. We favor specifics over generalities and focus on the case of the oldest, most valued, and most well-known cryptocurrency -- Bitcoin. We are:


[Andrew M. Bailey](#)
 Yale-NUS College


[Bradley Rettler](#)
 University of Wyoming


[Craig Warmke](#)
 Northern Illinois University

RESEARCH: PUBLISHED OR IN PROGRESS

- ▶ [Why Bitcoin Needs Philosophy](#) (CoinDesk)
- ▶ [What is Bitcoin?](#) (*Inquiry*)
- ▶ [Cryptocurrency: Philosophy, Politics, and Economics](#) (*Philosophy Compass*, commissioned)
- ▶ [Electronic Coins](#) (draft)
- ▶ [Bitcoin and Financial Injustice](#) [PDF] [archive]
- ▶ [Resistance Money](#) (book project)
- ▶ [A Pragmatic Case for Bitcoin](#)
- ▶ [Ethics for Bitcoin Research](#)

MEDIA

- ▶ [Bitcoin Doesn't Care About Your Politics: Why Bitcoin Has More Ideological Flexibility Than We Think](#) (podcast interview)
- ▶ [What is Bitcoin?](#) (podcast interview)
- ▶ [An Introduction to Bitcoin](#) (video)

WHY 'RESISTANCE MONEY'?

One theme in our research is that Bitcoin is a check against the authority and overreach of corporations, states, and anyone else who would serve as an intermediary between people and their money. Above all, it offers a way to elude and resist the interlocking and increasingly tight gears of institutions both private and public.

Last updated: 18 March 2021.

OVERVIEW

1. Genre and approach
2. The main question: how does bitcoin's market price relate to its protocol design and ultimate ambitions?
3. My answer: bootstrapping through speculation.
4. Consequence: one thing transmuted into another – alchemy. From speculative greed to cypherpunk technology, deployed at scale.

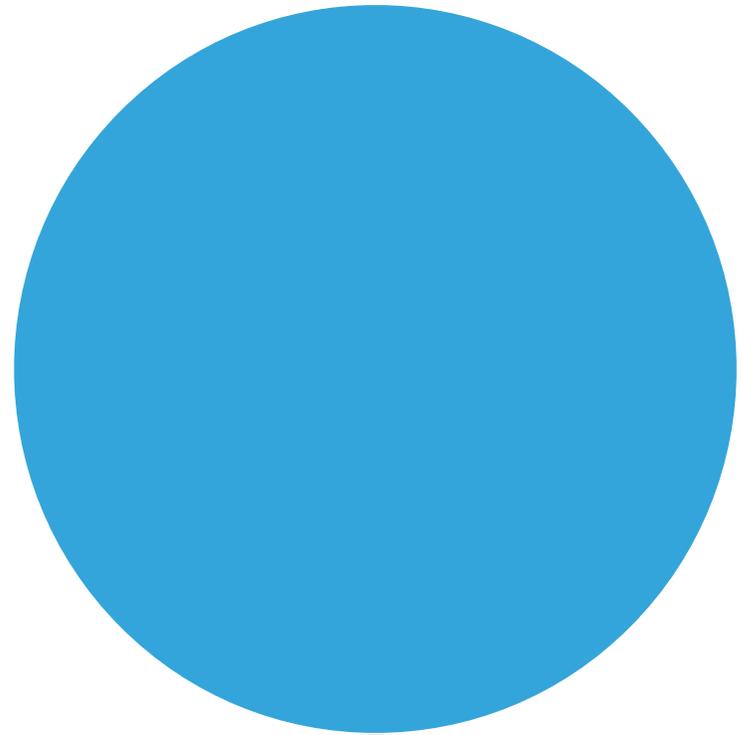
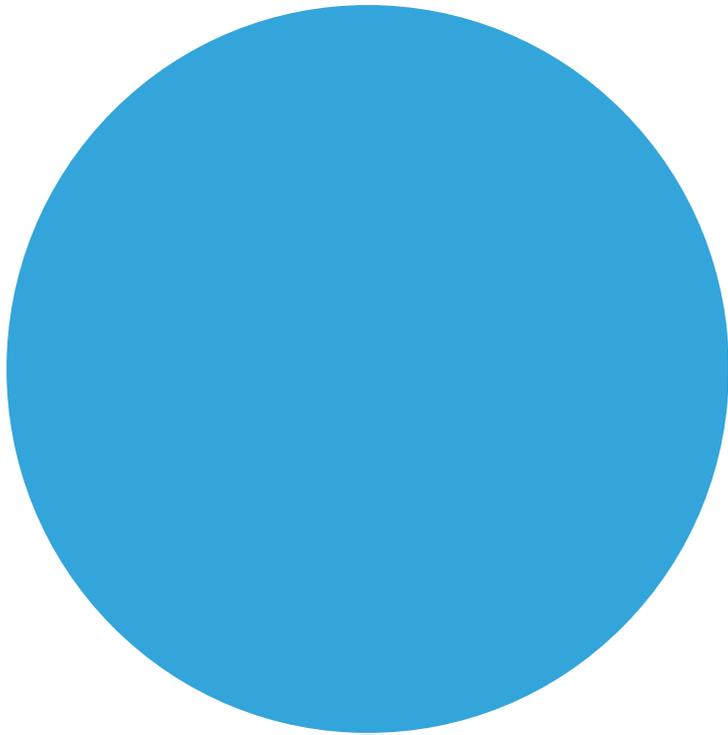
1.

GENRE AND APPROACH

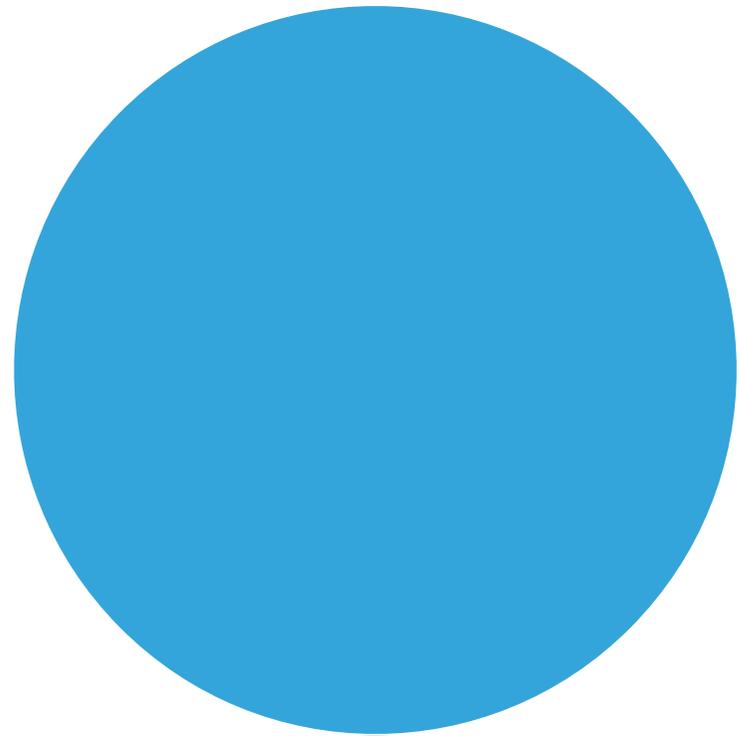
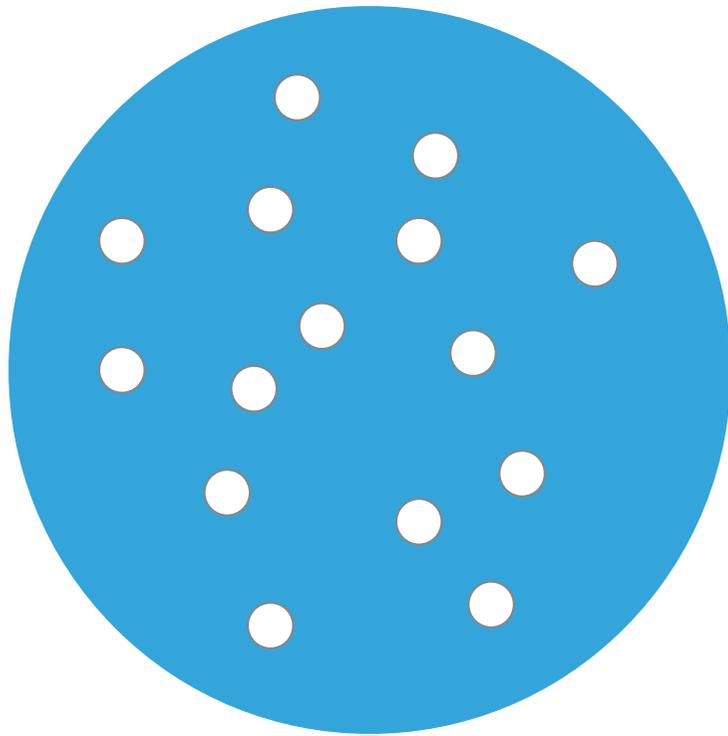
GENRE

- ▶ Bitcoin is a bundled phenomenon. It spans:
 - ▶ Cryptography
 - ▶ Computer science
 - ▶ Social and political theory
 - ▶ Economics
- ▶ Danger: epistemic trespassing [BALLANTYNE 2020](#)
- ▶ Danger: border-policing [DOTSON 2013](#)
- ▶ Strategy: intellectual arbitrage [BAILEY 2020](#)

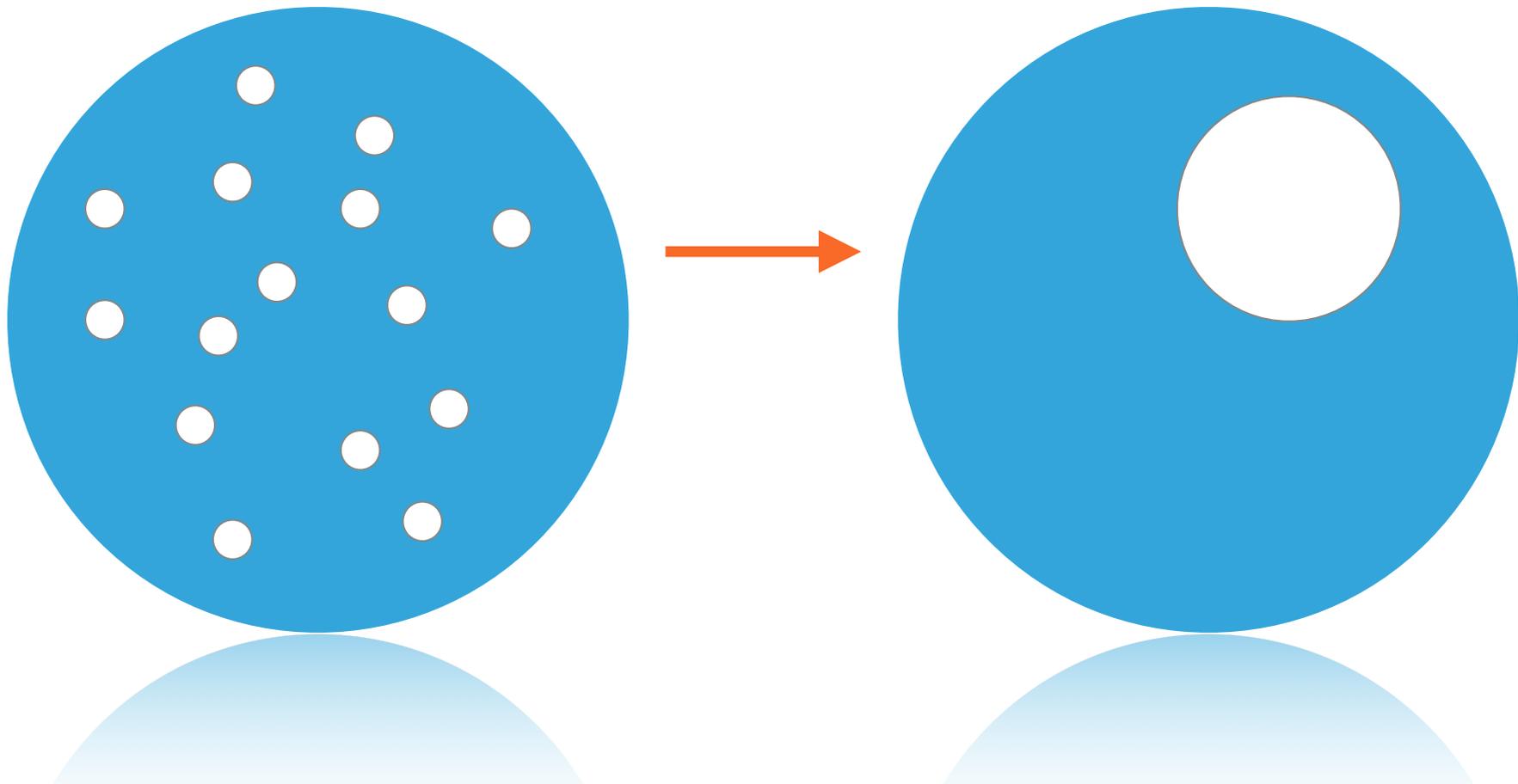
INTELLECTUAL ARBITRAGE



INTELLECTUAL ARBITRAGE



INTELLECTUAL ARBITRAGE



IDEA MARKETS TO PLUNDER

- ▶ Computer science
- ▶ Cryptonomics
- ▶ Social theory
- ▶ Metaphysics
- ▶ Political philosophy
- ▶ Philosophy of technology

BAILEY, RETTLER, WARMKE 2020

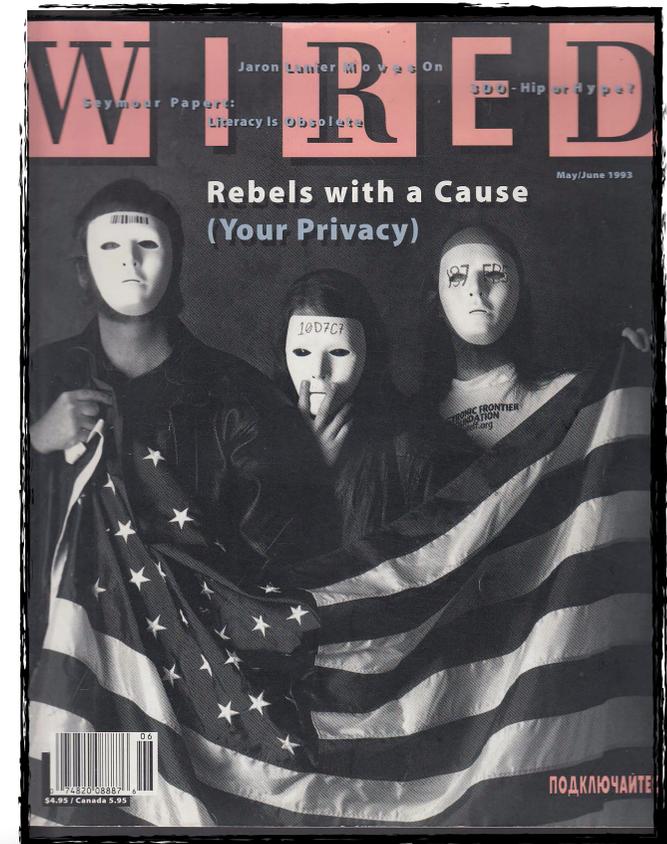
BAILEY, RETTLER, WARMKE FORTHCOMING

APPROACH

- ▶ Exploratory, sometimes speculative, as is fitting to the topic
- ▶ $P(\text{the stuff I'll say} \mid \text{what is known}) < 1$

BASICS: THE CYPHERPUNK DREAM

- ▶ To use cryptography to turn networked computers into engines of freedom, not oppression **HUGHES 1993**
- ▶ Cypherpunk conundrum: how do we get people to actually use freedom technology? **HUGHES 2012**
- ▶ This is often a bootstrapping problem – a problem of initial social coordination.



BASICS: NETWORK

- ▶ Bitcoin: a distributed, peer-to-peer network, defined by a certain protocol and associated ledger in which:
 - ▶ Users broadcast transactions
 - ▶ Nodes validate transactions and maintain copies of the ledger
 - ▶ Miners compete with one another to publish updates to the ledger (blocks)
 - ▶ Their sacrifice: processor cycles and electricity
 - ▶ Their reward: new amounts of the native asset, bitcoin (BTC)

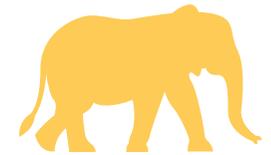
BASICS: ASSET

- ▶ BTC is an abstract synthetic commodity. SELGIN 2015
WARMKE 2021
 - ▶ BTC is to electricity (and processor cycles, through mining) as aluminium is to electricity (and bauxite, through smelting)
 - ▶ BTC is innately standardised CARTER 2021
- ▶ To control an amount of BTC (as encoded in a given UTXO) is to be able to use the network to send a certain kind of message. WARMKE MS

RESULT

- ▶ A base settlement layer...
- ▶ ... without trusted intermediaries
- ▶ ... that's censorship-resistant
- ▶ ... and that facilitates privacy and pseudonymity.
- ▶ A cypherpunk dream come true?
- ▶ NB: one needn't be a libertarian to think this is a good dream rather than a nightmare. The core cypherpunk idea is anti-authoritarian rather than, say, propertarian.

BUT WAIT...



- ▶ This is not why news outlets report on Bitcoin, and it has little to do with what they say!

 CNBC

Bitcoin climbs 10% as cryptocurrency market attempts a comeback from last week's plunge

Bitcoin last week slumped below \$50,000 for the first time since early March. It has risen 80% in 2021 with backing from institutional investors and ...

1 week ago



 CNA

Bitcoin: Boom or bust?

Bitcoin has been on a rollercoaster ride over the past few months. What do you need to know if you're thinking of investing in the ...

3 weeks ago



 Yahoo Finance

Bitcoin Rebounds After Hitting Lowest Level Since March

In the U.S., Coinbase Global Inc. gained 4.4%, while Riot Blockchain Inc. jumped 6.3%. Bitcoin has retained a gain of about 80% year-to-date as ...

1 week ago



 Yahoo News Singapore

Bitcoin price falters after breaking through technical barrier

Bitcoin (BTC-USD) came off two-week highs on Sunday morning, falling as much as 2.5% in London by 9.30am. On Friday, it had surpassed a ...

1 day ago



2.

THE MAIN QUESTION

HOW DO THESE THREE RELATE?

- ▶ Price
- ▶ Protocol
- ▶ Purpose

HOW DO THEY RELATE?

- ▶ Market price (bitcoin the asset)
 - ▶ BTC price reports what market participants are willing to give up to enjoy network privileges.
 - ▶ Blows around like the wind.
 - ▶ The decade-story is of a new asset class monetising – with considerable bumps along the way





HOW DO THEY RELATE?

- ▶ Protocol and its purpose (Bitcoin the network)
 - ▶ Design integrates decades of digital cash and cryptography gizmos, all in the service of cypherpunk goals. Above all, disintermediation; and from it, privacy, pseudonymity, and censorship-resistance
 - ▶ A peculiar supply schedule

MORE PRECISELY

- ▶ How does Bitcoin's protocol (and in particular, its supply schedule) bear on the market price of its native asset?
- ▶ And how does that price, in turn, bear on Bitcoin's capacity to make good on cypherpunk dreams?

WHY THE QUESTIONS MATTER

- ▶ Networks (social, monetary, gaming) are all the rage. It would be good to think clearly about their value.
- ▶ In the midst of speculative frenzy, it would be nice to know if there is any there there.
- ▶ It would also be nice to know whether Bitcoin managed to resolve the cypherpunk conundrum, and if so, how and at what cost and whether it can be done again.

3.

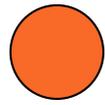
**ANSWER: BOOTSTRAPPING
THROUGH SPECULATION**

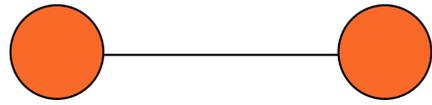
BOOTSTRAPPING

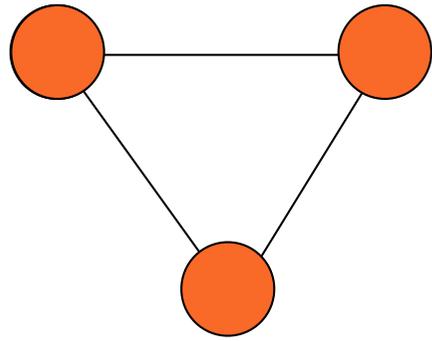
- ▶ How do we get people to actually use freedom technology?
- ▶ A problem of social coordination
 - ▶ Even if the optimal outcome is that everyone uses (Tor, PGP, Bitcoin)...
 - ▶ ... viable paths to that outcome make the relevant agents worse off along the way (switching costs, inconvenience, loss of data, reputational risk)
- ▶ Problem is very hard when it comes to network goods, even worse for distributed networks, and worst of all for monetary networks

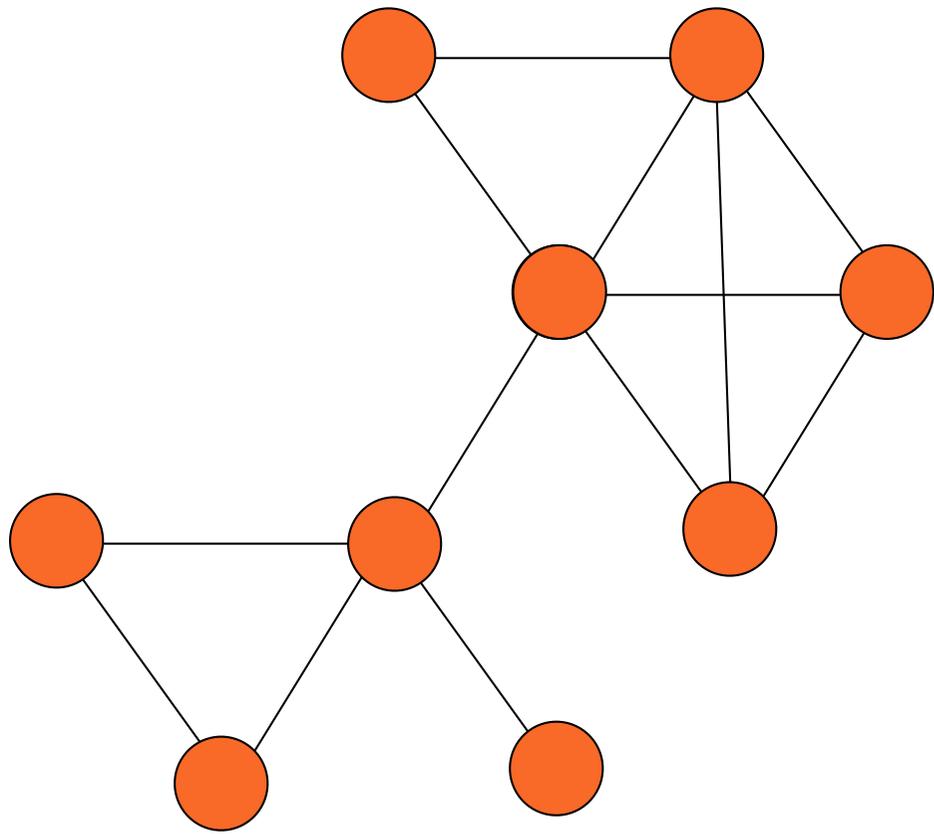
BOOTSTRAPPING

- ▶ Imagine: you've invented a new language
- ▶ Or a new way of encrypting network traffic
- ▶ Or a new money

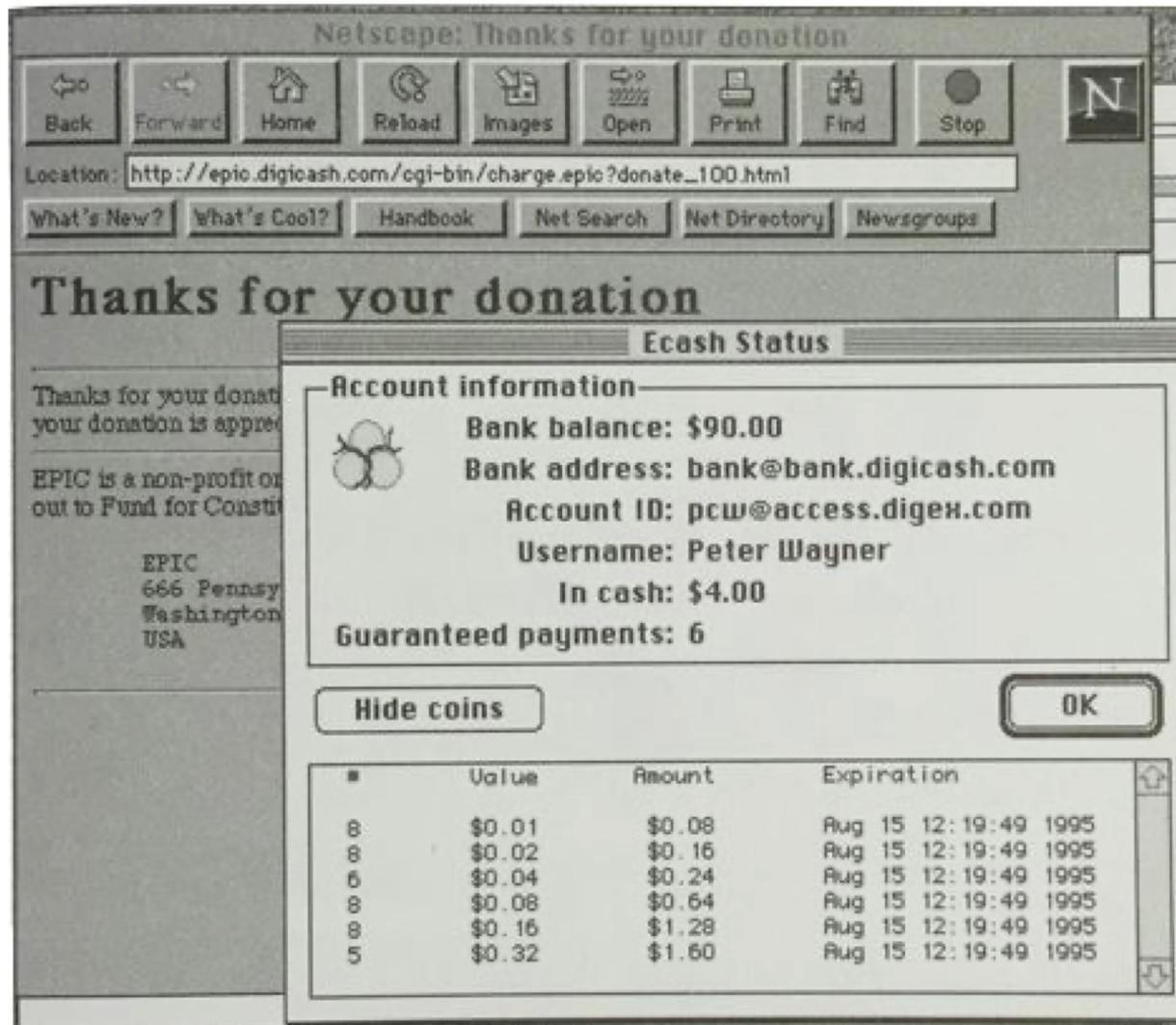








CASE STUDY: CHAUM'S DIGICASH



CASE STUDY: CHAUM'S DIGICASH

“Now, why did DigiCash fail? The main problem with DigiCash was that it was hard to persuade the banks and the merchants to adopt it. Since there weren't many merchants that accepted ecash, users didn't want it either. ”

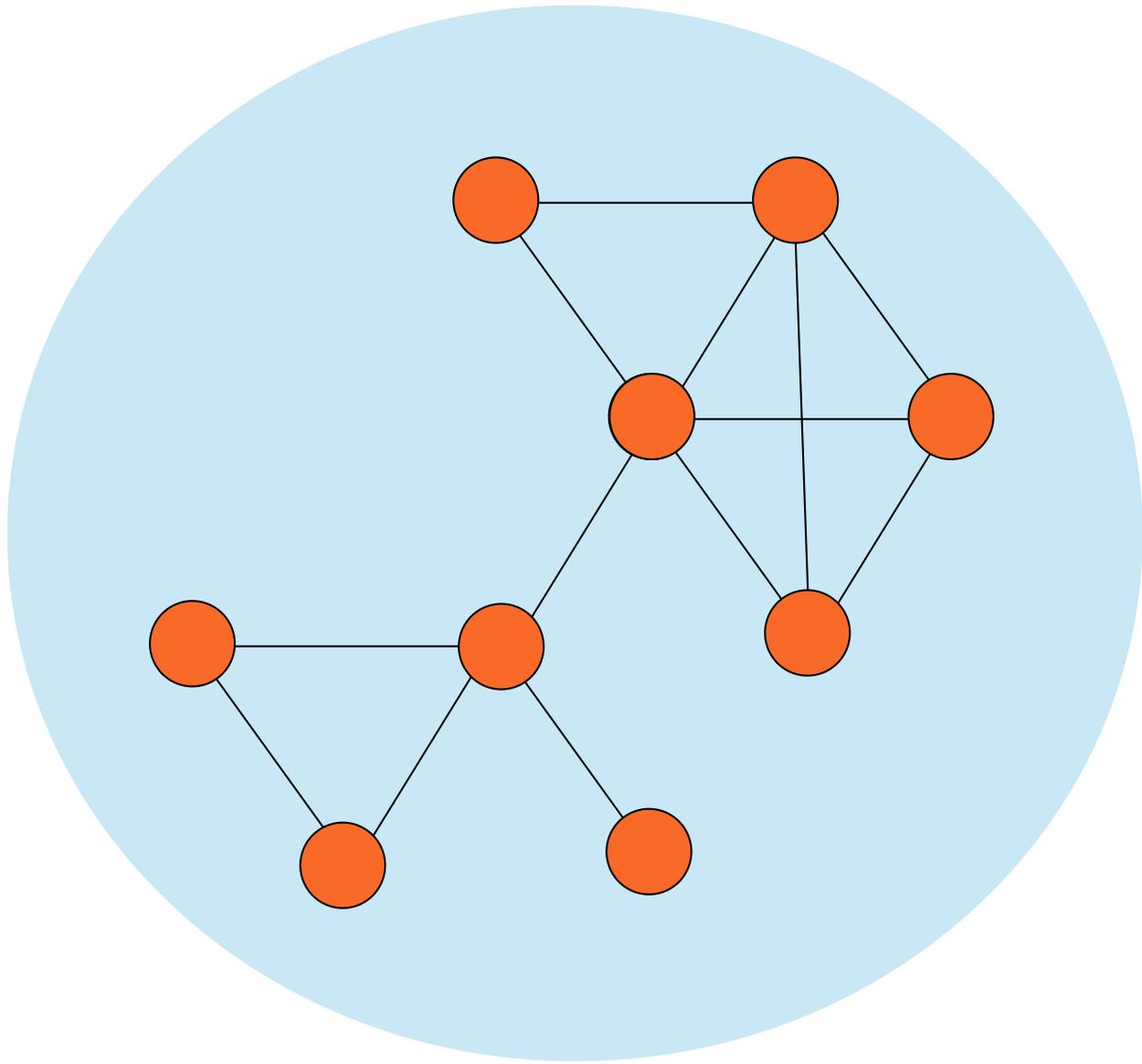
NARAYANAN ET AL 2016

CASE STUDY: CHAUM'S DIGICASH

- ▶ If you build it, they probably won't come

THE USUAL TRICKS (ALONE) ARE LIMITED

- ▶ Non-exchange value (BTC isn't shiny)
- ▶ BTC as collectible (limits to status symbol, niftiness factor)
- ▶ Centrally distributed and antecedently valuable enticements to participate (no actor to implement)
- ▶ Ideology (too fringe; risky)
- ▶ Ransomware (forced liabilities denominated in BTC)



IDEOLOGICAL BOOTSTRAPPING REJECTED

“The developers expect that this will result in a...
currency outside the reach of any government.”

- Teppy, July 2010

“I am definitely not making an[y] such taunt or
assertion”

- Satoshi Nakamoto, July 2010

SUPPLY

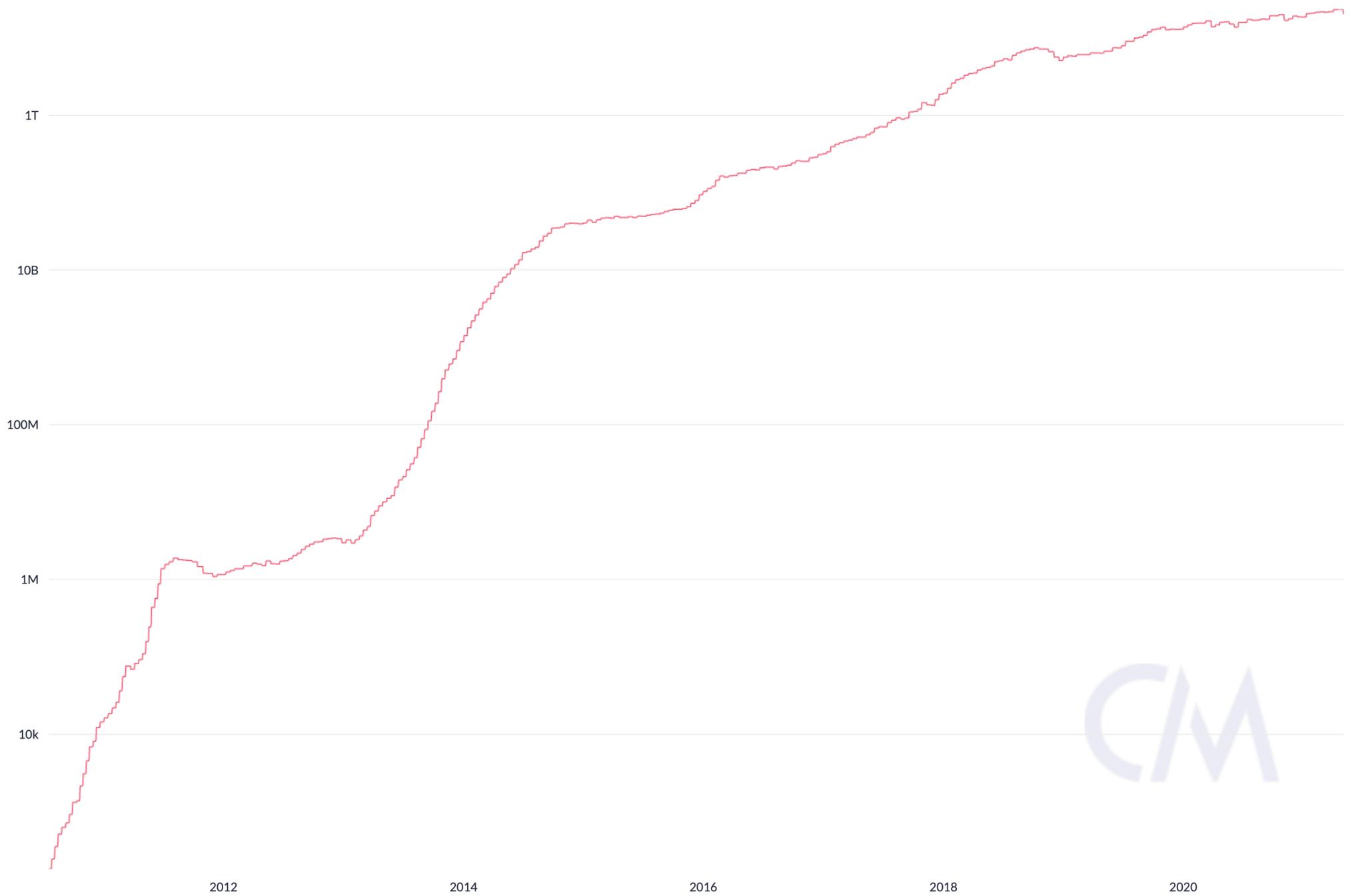
- ▶ Three distinctive features of Bitcoin's protocol conspire to ensure a predictable and ultimately fixed supply schedule
 - ▶ Difficulty adjustment
 - ▶ Periodic halving
 - ▶ Supply cap

SUPPLY

- ▶ Three distinctive features of Bitcoin's protocol conspire to ensure a predictable and ultimately fixed supply schedule
 - ▶ **Difficulty adjustment**
 - ▶ Periodic halving
 - ▶ Supply cap

BTC: A VERY UNUSUAL COMMODITY

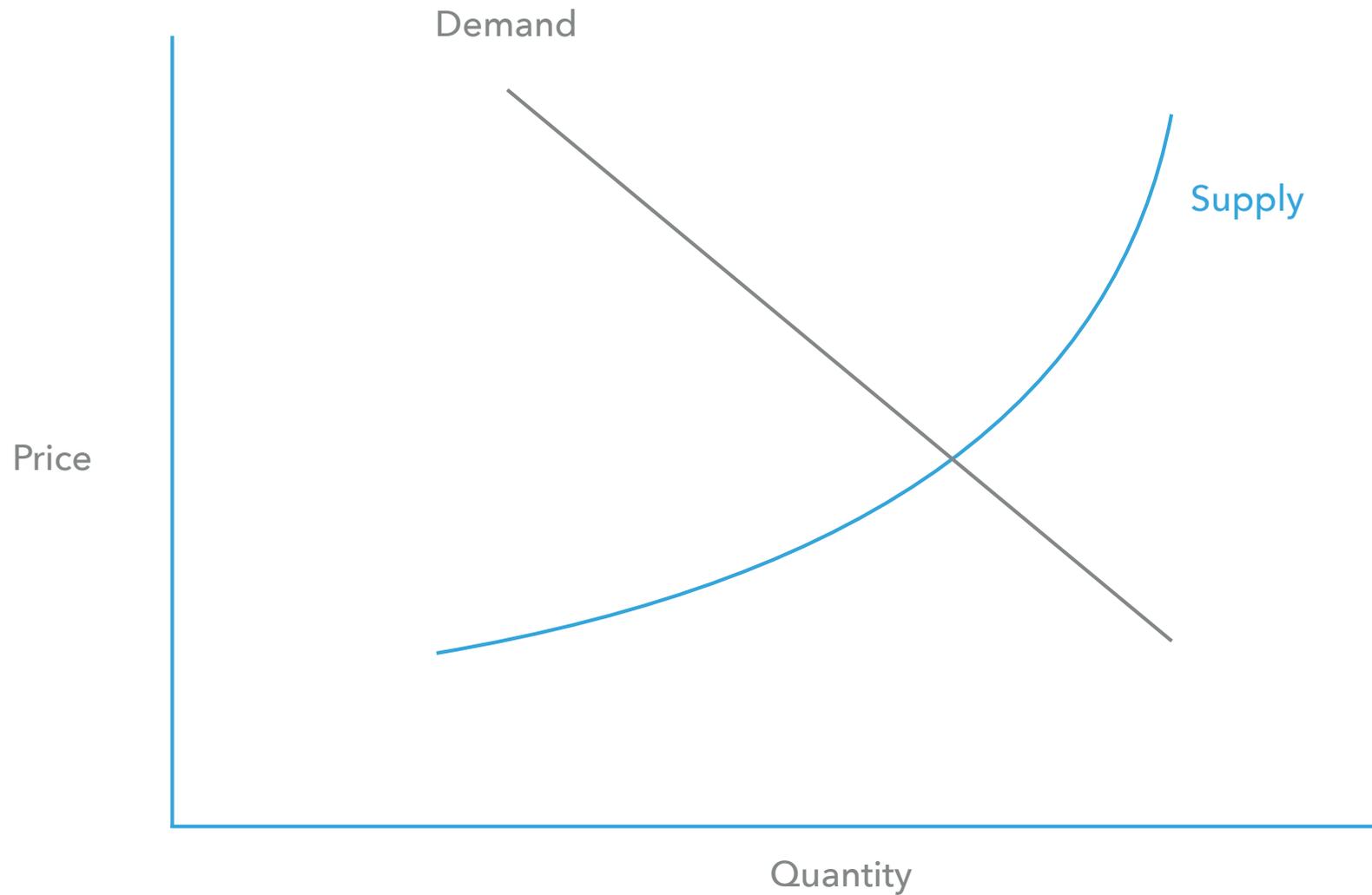
- ▶ When aluminium price rises, more of it gets smelted
- ▶ When BTC price rises (falls), miners can indeed mine more (less) of it – for a time
- ▶ But every 2016 blocks, the protocol adjusts the proof-of-work target (the lower the target, the more work required). Nodes reject proposed blocks unless the hash of their header is lower than or equal to that target.
- ▶ Consequence: no matter how frantic or lazy Bitcoin miners are, blocks arrive, on average, every ten minutes



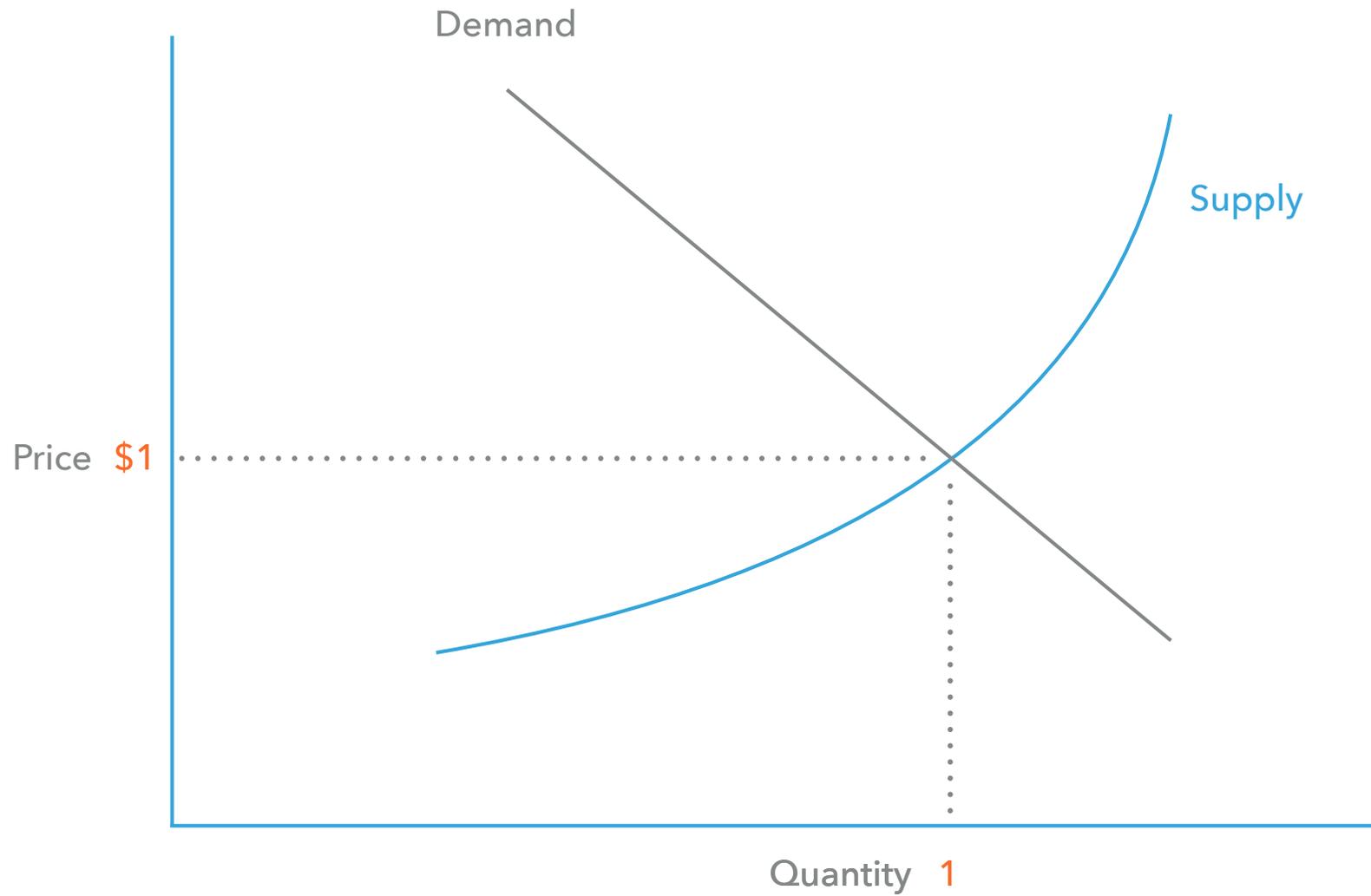
PRICE THEORY

- ▶ A commodity's equilibrium market price lies where its supply and demand curves intersect
- ▶ Demand curves slope down
- ▶ Supply curves slope up
- ▶ Bitcoin's supply is unusually and irremediably inelastic (close to vertical). It does not respond to price!

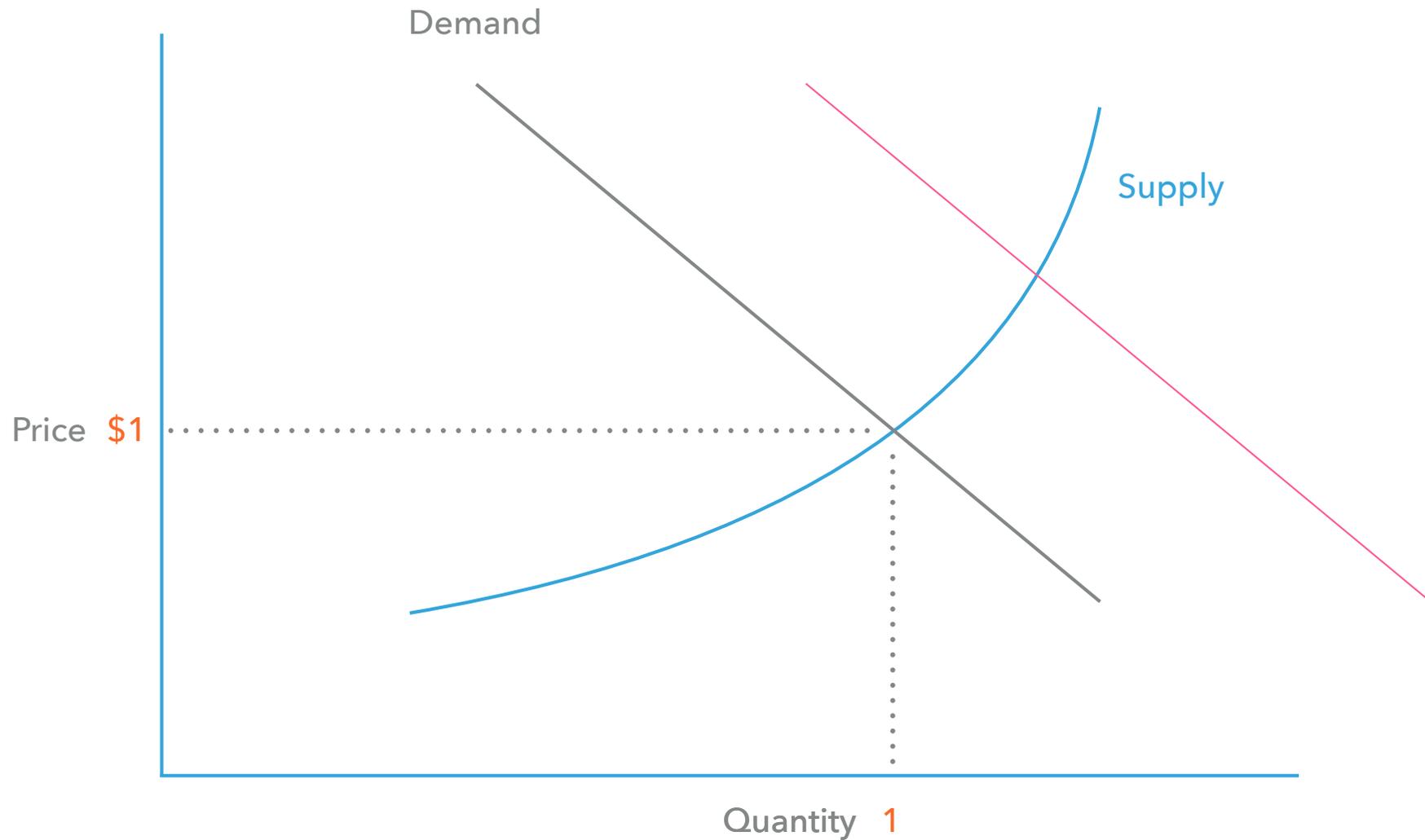
PRICE THEORY



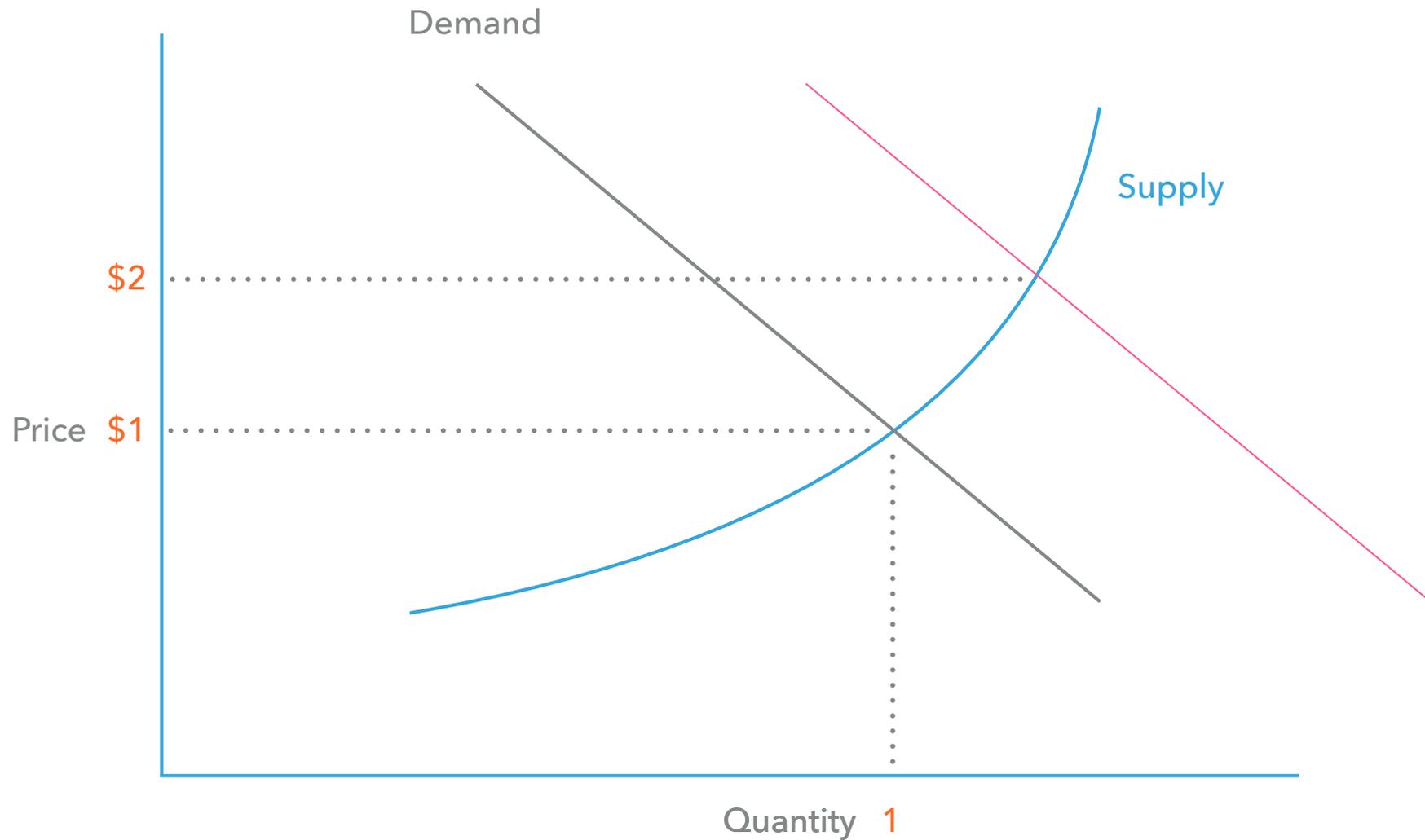
PRICE THEORY



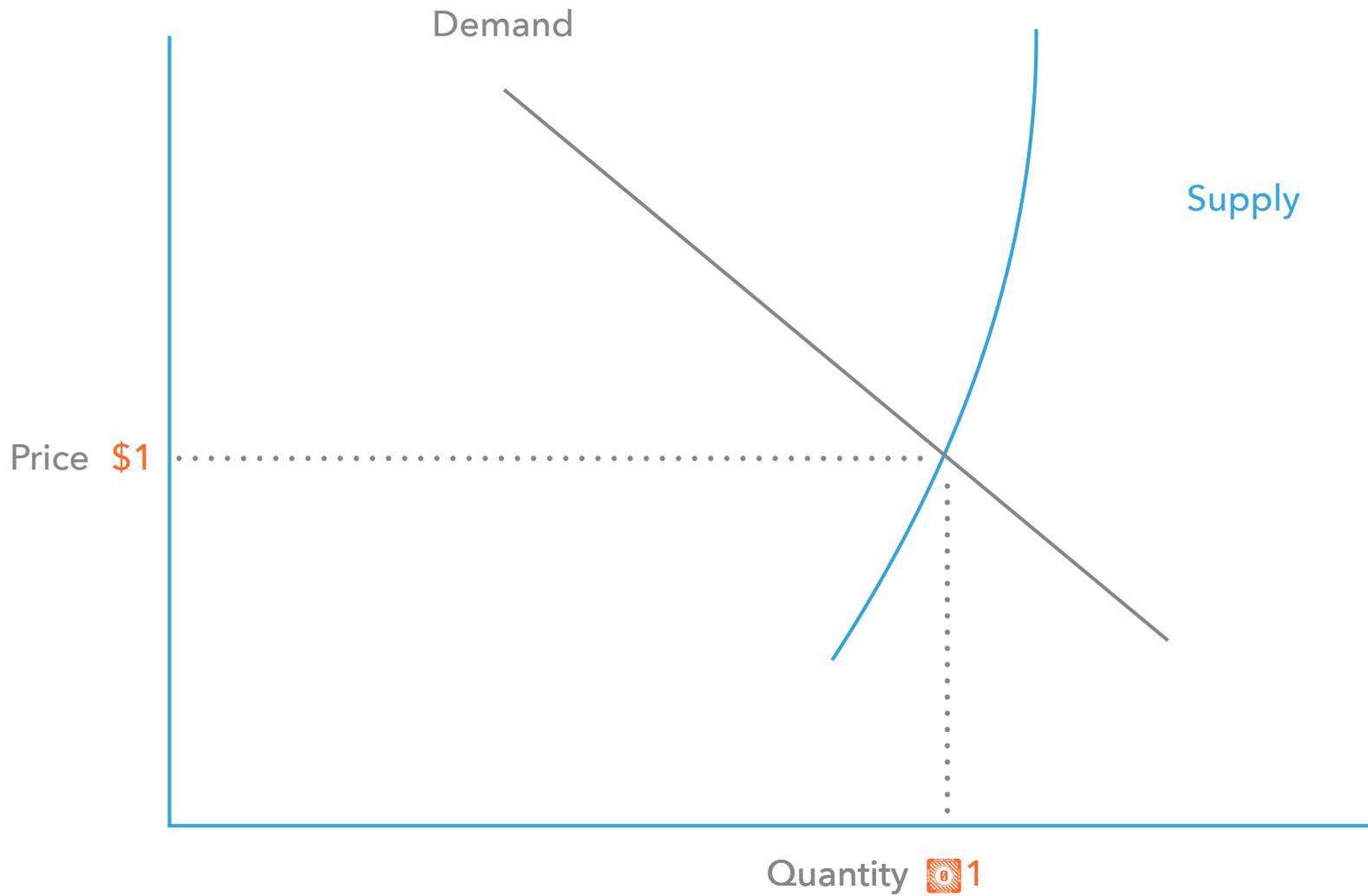
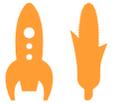
PRICE THEORY



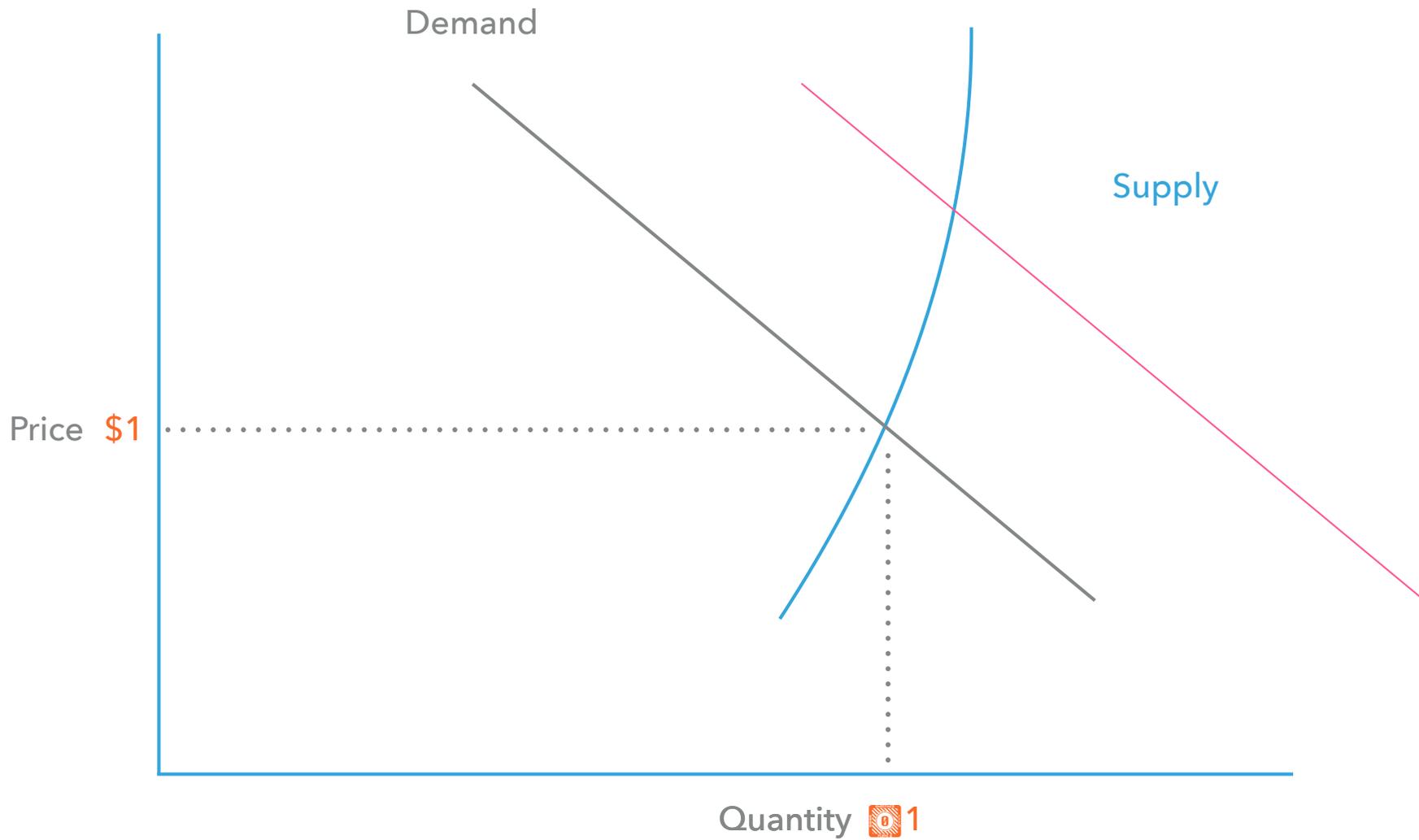
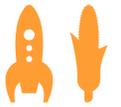
PRICE THEORY



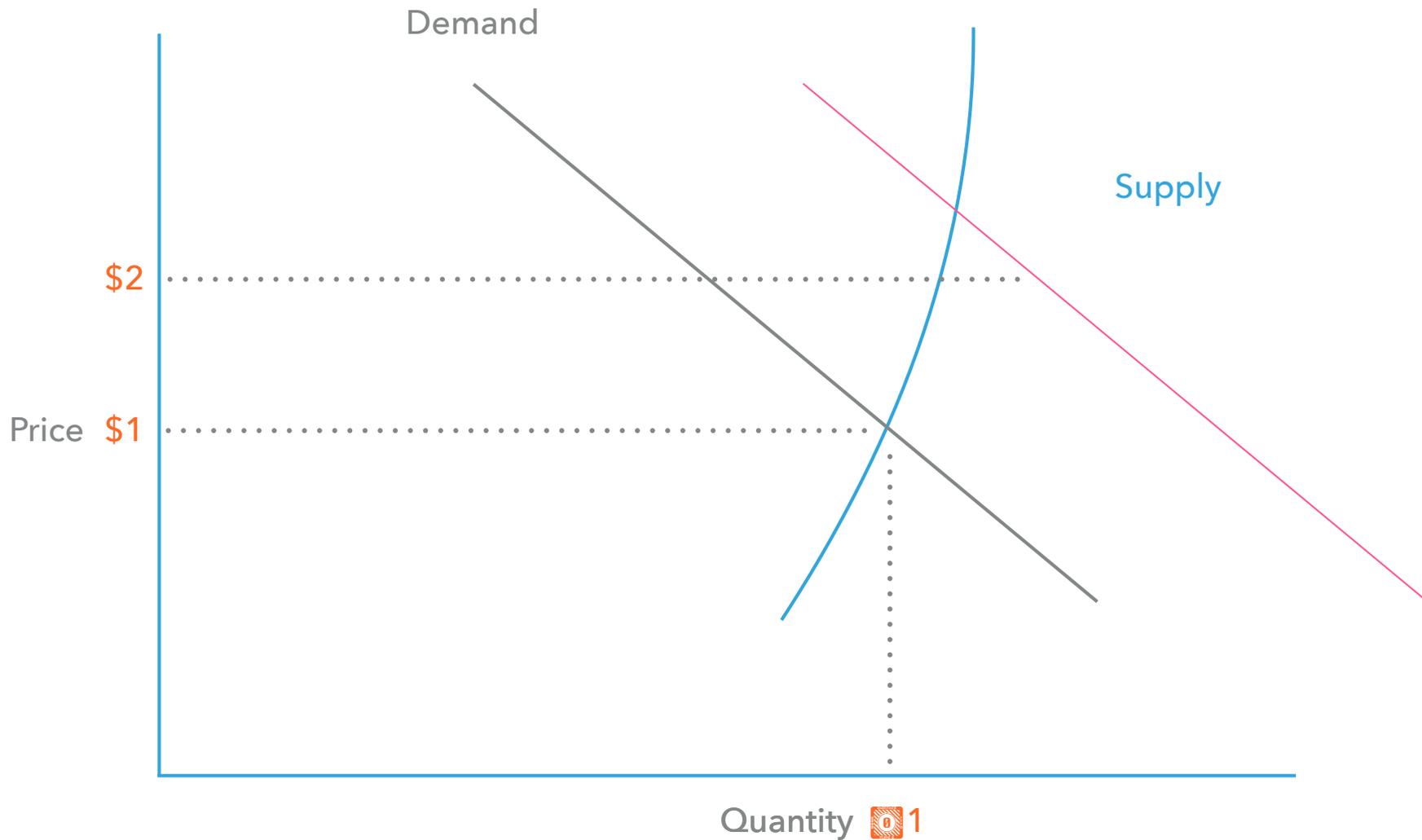
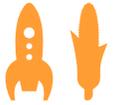
PRICE THEORY



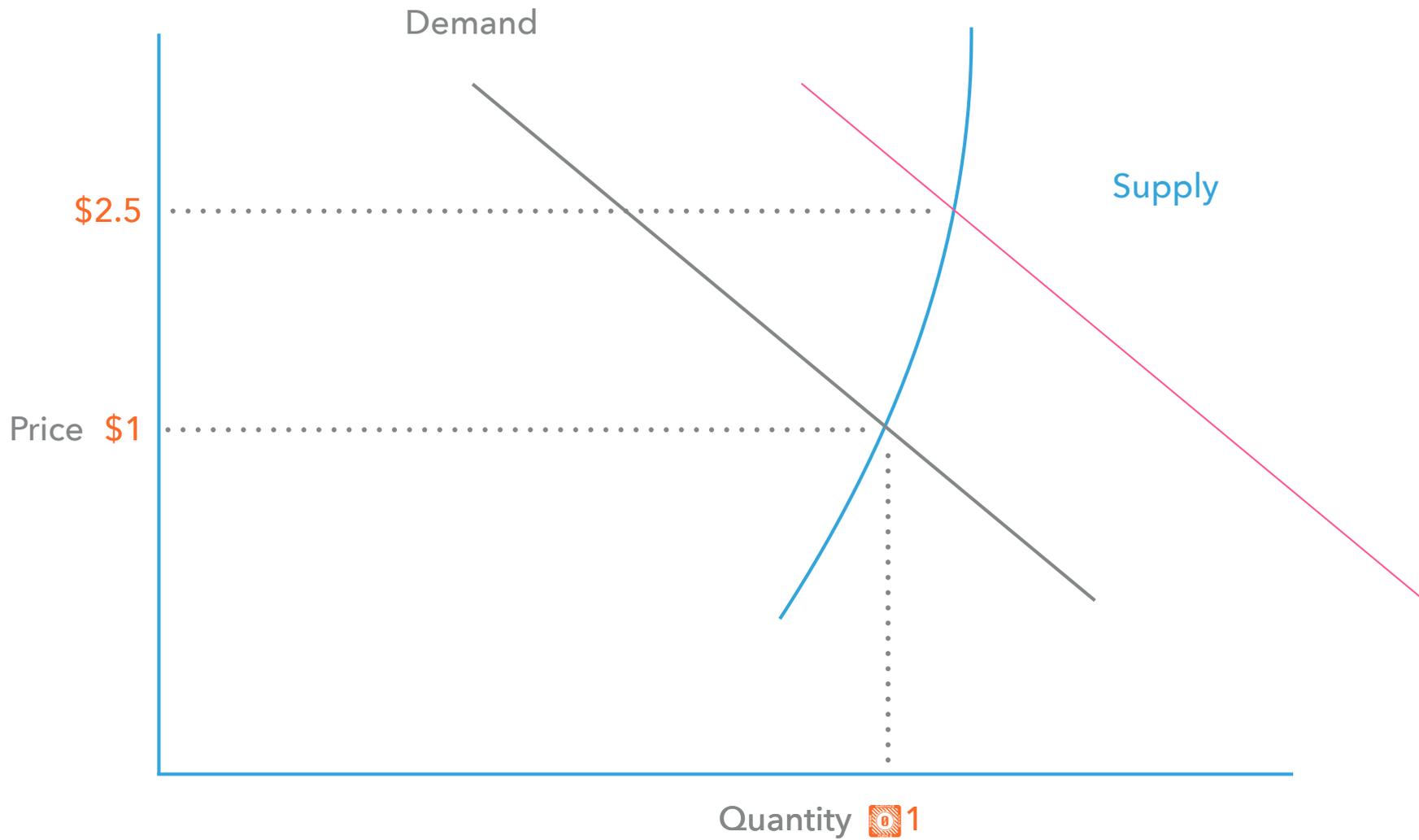
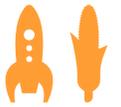
PRICE THEORY



PRICE THEORY



PRICE THEORY

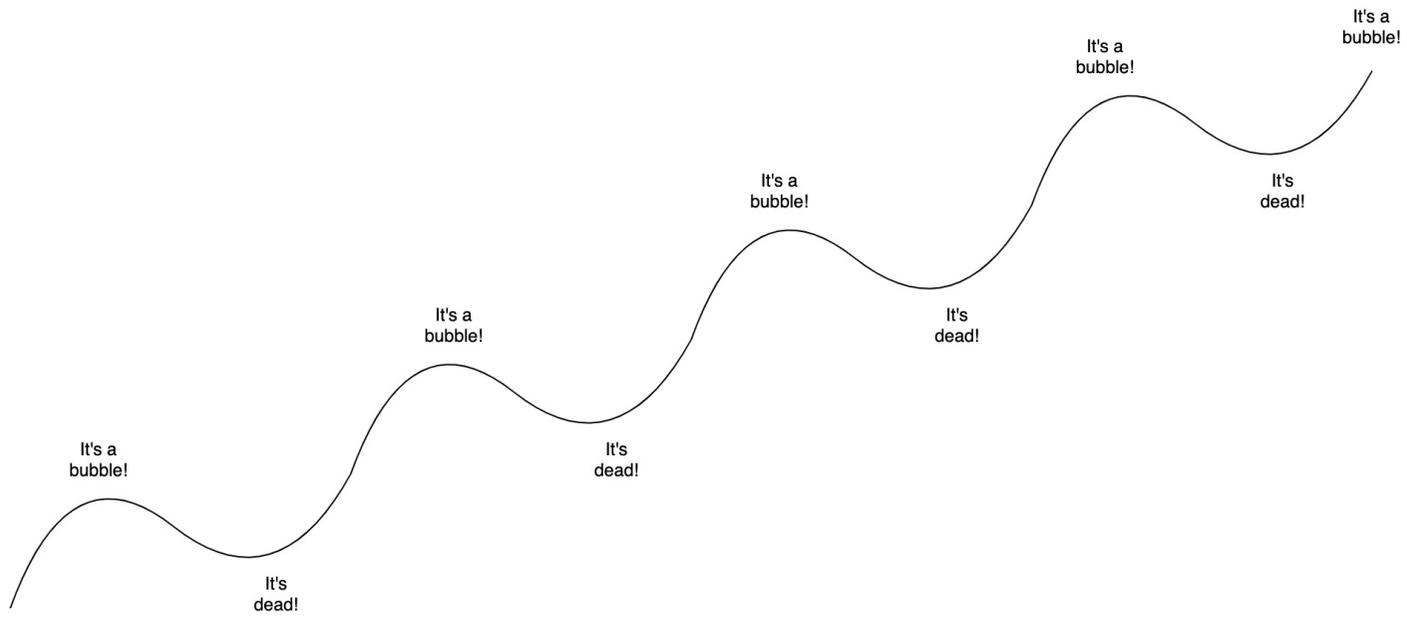


ADJUSTMENT, NOT CAP

- ▶ The point here is slightly more subtle than a familiar one, which concerns the 21m supply cap NORLAND AND PUTNAM 2019
- ▶ Bitcoin's inelastic supply is a consequence of the protocol's supply schedule, in totality (cap, halving, adjustment)
- ▶ But it's the difficulty adjustment (not the supply cap) that plays a controlling role here
- ▶ Counterfactual: supply cap without difficulty adjustment

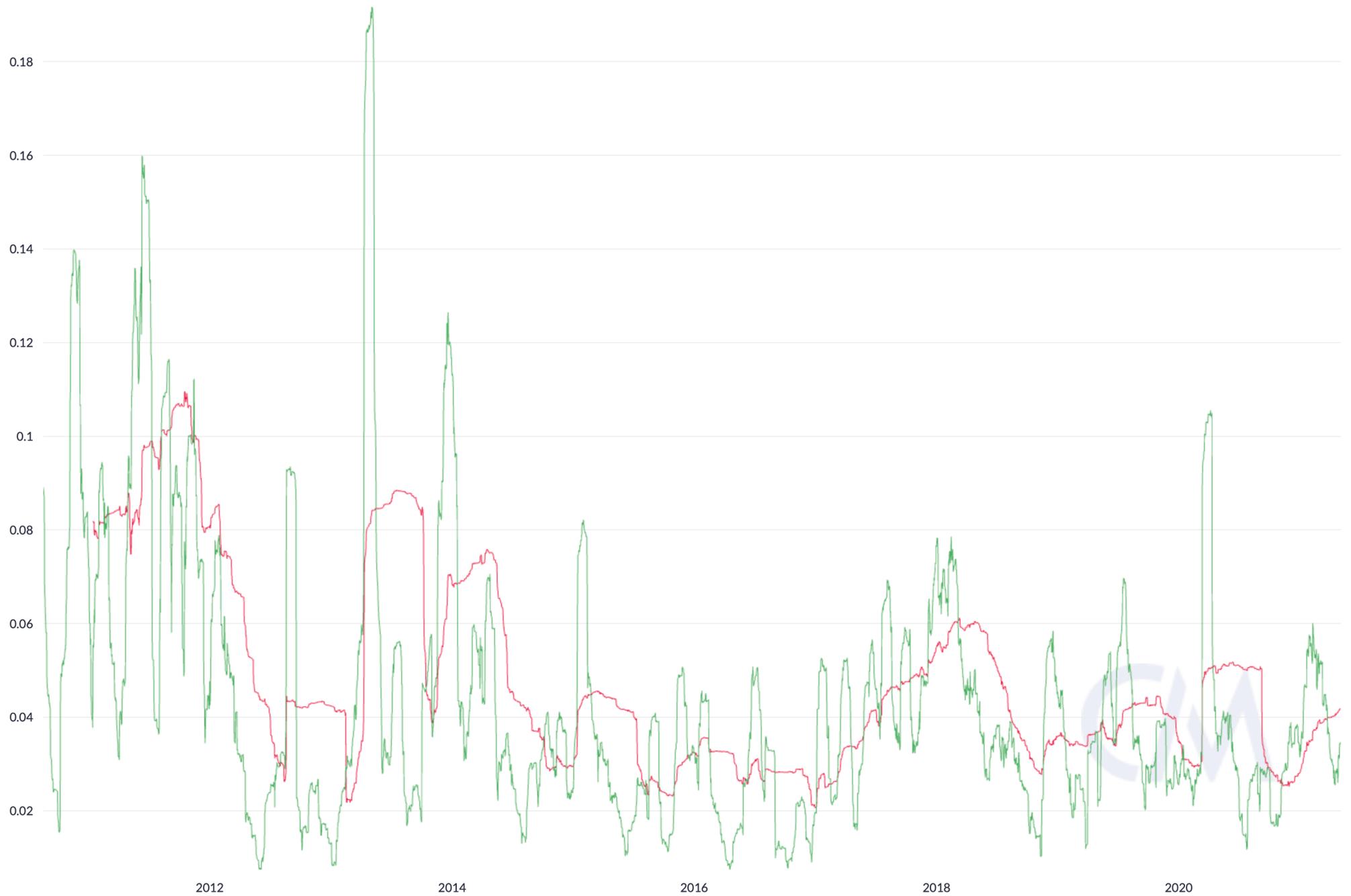
CONSEQUENCES

- ▶ BTC's market price is unusually and irremediably sensitive to fluctuations in demand
- ▶ It is, accordingly, volatile
- ▶ What's true of the upside is true of the down: mania (or bubble-talk) and despair (or death-talk)



(@craigwarmke)





DETAILS DETAILS

- ▶ There are econometric disputes about how to best measure volatility (standard deviation vs. median absolute variation) KONING 2019

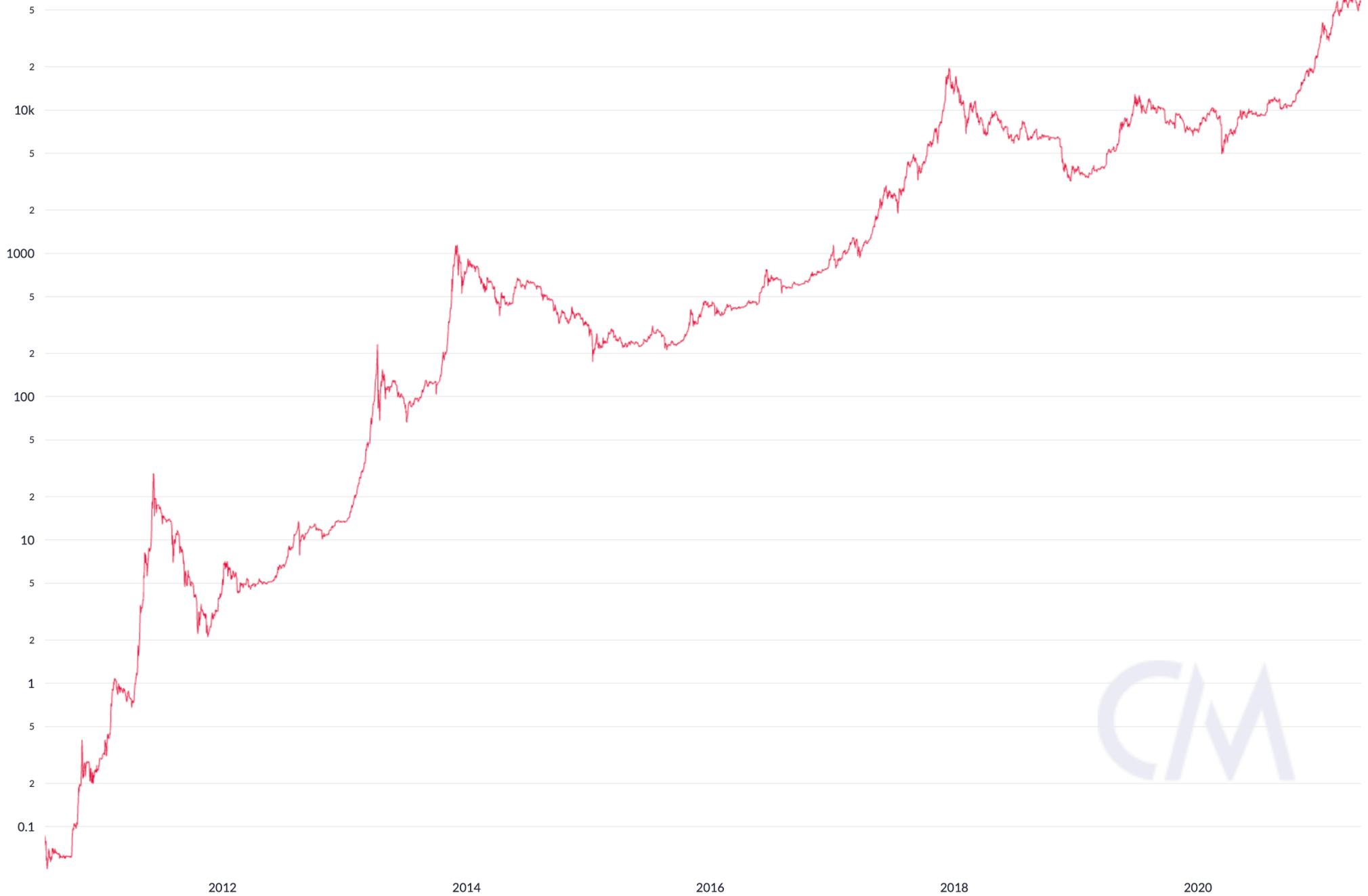
CONSEQUENCES

- ▶ That said: BTC is a great asset to trade. Speculators thrive on volatility
- ▶ Traders provide liquidity: entry and exit
- ▶ Liquidity attracts liquidity, and as a result the asset is monetising while the network's reach expands
- ▶ Speculation overcomes powerful incumbent network effects

NAIR AND CACHANOSKY 2016

CONSEQUENCES

- ▶ Despite speculative booms and busts, Bitcoin has bested the bubble naysayers – at least three times, and in at least three ways:
 - ▶ Recovery from (80%) crashes
 - ▶ New highs (3x or more)
 - ▶ Endogenous network fundamentals tend towards steady growth
- ▶ One bubble is a bubble. Three, with higher lows and higher highs is adoption.



4.

ALCHEMY

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ Key distinction:
 - ▶ Number (Will) Go Up
 - ▶ Number (Already) Go Up

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ Key distinction:
 - ▶ Number (Will) Go Up
 - ▶ Number (Already) Go Up

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ A tempting thought: monetisation through speculation is at war with cypherpunk ambitions (greed vs. freedom)
- ▶ The thought is fallacious

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ Scaling through economic density (more value settled/byte)
- ▶ Privacy and pseudonymity
 - ▶ Network handles higher-value TXes, without revelation (privacy through obscurity)
 - ▶ Value settled in private TXes (e.g., CoinJoin)

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ Censorship-resistance

- ▶ Healthy swarm of nodes makes for a resilient network (see <https://bitnodes.io> for a live map of discoverable nodes)

- ▶ Users need not touch fiat currencies at all

LUTHER 2016A

- ▶ Banning Bitcoin is quixotic

GLADSTEIN 2021A

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

▶ Development

Category	#repos	#issues	#watchers	#devs	#commits
Data analysis	25	95	103	80	1,539
Development	223	32,114	79,050	1,661	181,875
Documentation	6	17	23	17	186
Mining	11	41	58	36	2,116
Node	26	6,952	10,030	421	28,065
Payment	27	626	1,067	84	8,580
Services	86	5,366	6,153	387	26,023
Trade	31	2,180	5,501	180	14,578
Wallet	46	6,062	5,309	291	34,173

OSMAN & BAYSAL 2021

▶ Infrastructure for the rest of us – on-ramps, off-ramps: monetary sovereignty and savings technology for the least well-off

RETLER 2021

▶ These factors are reflexive. For example, attention spurs developer attention to new privacy techniques.

FICSÓR ET AL 2021

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ Caveat: miner fees are denominated in BTC



- ▶ Do they price out non-speculators and impede other uses of the network?
- ▶ Not obviously: high fees drive users to Lightning and other L2 solutions (see <https://bitcoinvisuals.com/lightning>)

MONETISED BITCOIN IS FREEDOM TECHNOLOGY, AT SCALE

- ▶ Monetisation through speculation is not at war with cypherpunk ambitions.
- ▶ The driving force (speculative greed) turns out to be irrelevant.

GLADSTEIN 2021B

▶ Hence:

 **Alex Gladstein**  @gladstein · Jun 4, 2020
Replying to @santisiri
Bitcoin is a machine that turns greed into freedom. That's why it works so well!

- ▶ Is this all by design? Also irrelevant. But an intriguing question!

BY DESIGN? (MOON MATH; NOT TO BE TAKEN SERIOUSLY!)

"As an amusing thought experiment, imagine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from \$100 trillion to \$300 trillion. **With 20 million coins, that gives each coin a value of about \$10 million.**

So the possibility of generating coins today with a few cents of compute time may be quite a good bet, with a payoff of something like 100 million to 1! Even if the odds of Bitcoin succeeding to this degree are slim, are they really 100 million to one against? Something to think about... "

- Hal Finney, January 2009

BY DESIGN?

“It might make sense just to get some in case it catches on. If enough people think the same way, that becomes a self fulfilling prophecy. Once it gets bootstrapped, there are so many applications...”

- Satoshi Nakamoto, January 2009

WORKING HYPOTHESIS

- ▶ Bitcoin succeeded where other cypherpunk projects failed.
- ▶ In particular, it harnessed speculative greed to overcome powerful incumbent network effects
- ▶ The mechanism through which this alchemy occurs can be described more carefully, and contrasts with that deployed by other successful networks

POSITIVE AND NEGATIVE LIBERTIES

BERLIN 1958

HUGHES 2012

- ▶ Positive liberties: abilities and the opportunities to exercise them (to walk, to eat...)
- ▶ Negative liberties: absences of external constraints (absence of censorship, domination, surveillance...)
- ▶ A vexed distinction, but useful nonetheless

BLAU 2004

POSITIVE AND NEGATIVE LIBERTIES

- ▶ Hypothesis: people, by and large, *want* positive liberties more than they want negative liberties. But we *need* negative liberties to flourish nonetheless.
- ▶ Observation: the cypherpunk dream is all about achieving negative liberties through technology.

POSITIVE AND NEGATIVE LIBERTIES

- ▶ If the hypothesis and observation are correct, there is little sense in offering freedom technology (negative liberty) alone.
- ▶ The problem is compounded when the technology in question involves network goods.

POSITIVE AND NEGATIVE LIBERTIES

- ▶ But... what if you got paid to solve a bootstrapping problem? What if you were reimbursed for pursuing negative liberty for yourself and others?
- ▶ Whether by design or not, this is what Bitcoin has done for its early adopters.
- ▶ Model: achieve negative liberty through monetary enticements (you can think of these as facilitating positive liberty)

POSITIVE AND NEGATIVE LIBERTIES

- ▶ The model in view is the precise opposite of that deployed by other networks.
- ▶ Facebook, for example, offers you positive liberties; in exchange you give up negative liberties. Endure a little censorship, domination, surveillance, and in exchange, an avalanche of positive liberties fall on your head.
- ▶ Open question: is Bitcoin's fundamental strategy repeatable? Is it being repeated elsewhere?

LIMITS

- ▶ Ongoing fungibility
 - ▶ Will regulated, custodial BTC products (BlockFi, Robinhood, PayPal) created walled gardens that will never touch the Bitcoin network?
 - ▶ Will those walled gardens facilitate a “two Bitcoins” world, each sides of the wall mutually non-fungible?
 - ▶ Answers aren't yet obvious, and those who'd say “yes” to either question have yet to make a convincing case.
- ▶ Beyond Bitcoin

LOOKING AHEAD

- ▶ Significant progress has been made in solving a bootstrapping problem that has plagued other cypherpunk efforts (and digital cash in particular). An impressive feat.
- ▶ But a transition problem has been thereby created: significant BTC volatility is predicted by standard price theory, borne out in practice, and is, I'd guess, with us for the foreseeable future.

TRANSITION

- ▶ The problem here is not the canard “bitcoin is too volatile to be a currency” (a *terrible* argument).
 - ▶ (“bad currency now” ≠ “bad currency forever”)
 - ▶ (“bad currency forever” ≠ “useless”)
- ▶ It is rather: can BTC’s notorious volatility ever be tamed so as to make it even more useful, for more people, in more ways?

TRANSITION: STATING THE PROBLEM

- ▶ Parameters
 - ▶ Price stability (with respect to consumer goods, say)
 - ▶ Without protocol change (supply remains wildly inelastic)
- ▶ Solutions within those parameters require stable demand.
- ▶ Open question: what variables best predict demand, and are they likely to stabilise? Are there historical examples to draw on? (e.g., AMZN)

SPECULATING ABOUT SPECULATION

- ▶ Can speculative demand transform into something more stable?
- ▶ Caveat: the distinction here is not nearly so clear-cut as many imagine
- ▶ From:
 - ▶ Keynesian beauty contests to fundamentals
 - ▶ Short-term to long
 - ▶ Risk-seeking to risk management (or even risk aversion)

GARBER 1990

SPECULATING ABOUT SPECULATION

- ▶ Very Bad Argument: “BTC isn’t scarce, because they’ll clone Bitcoin”
 - ▶ Nothing else can offer all of BTC’s fundamentals: settlement assurances, network effects, etc.
 - ▶ Demand that is informed by these fundamentals discriminates sharply between BTC and other crypto assets
 - ▶ *Purely* speculative demand, by contrast, need not.

SPECULATING ABOUT SPECULATION

- ▶ Much More Interesting Argument: proliferation of crypto assets provides supply elasticity to match speculative demand, a stabilising force for the space as a whole.
 - ▶ Scenario: *purely* speculative liquidity exits BTC for new opportunities, while non-speculative demand steps up to the plate and takes its place (especially demand tethered to risk management or allocation mandates)
 - ▶ Is this happening, at scale?
 - ▶ So far, the answer is not “no”, and it may be “yes” (institutions). On-chain metrics are helpful here (@ wonomic)

CONCLUSIONS

- ▶ That thing you hear about in the headlines – BTC's price – does bear a systematic relationship to the protocol itself.
- ▶ And the story of that price is the story of freedom technology, at scale. Somewhere, somehow, a cypherpunk is smiling.



ACKNOWLEDGEMENTS

- ▶ For questions, comments, feedback, and inspiration, I thank:
 - ▶ Bradley and Craig
 - ▶ TC
 - ▶ Middlesex University's Computer Science Colloquium
 - ▶ And #bitcoin Twitter (especially @gladstein and @nic__carter)

- ▶ Bailey, Andrew (2020): "Of All Trades"
- ▶ Bailey, Andrew and Bradley Rettler & Craig Warmke (2020): "Why Bitcoin Needs Philosophy"
- ▶ Bailey, Andrew and Bradley Rettler & Craig Warmke (forthcoming): "Cryptocurrency: Philosophy, Politics, and Economics"
- ▶ Ballantyne, Nathan (2020): "Epistemic Trespassing"
- ▶ Beltramini, Enrico (2020): "Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement"
- ▶ Berlin, Isaiah (1958): "Two Concepts of Liberty"
- ▶ Blau, Adrian (2004): "Against Positive and Negative Freedom"
- ▶ Carter, Nic (2021): "Elemental Bitcoin is Money"
- ▶ Cuen, Leigh (2020): "What an Uptick in 'Coinjoins' Says About Bitcoin's Value Proposition"
- ▶ Dotson, Kristie (2013): "How is This Paper Philosophy?"
- ▶ Ficsór, Ádám and Yuval Kogman, Lucas Ontivero, & István András Seres (2021): "WabiSabi: Centrally Coordinated CoinJoins with Variable Amounts"
- ▶ Garber, Peter M. (1990). "Famous First Bubbles"
- ▶ Gladstein, Alex (2021a): "Can Governments Stop Bitcoin?"
- ▶ Gladstein, Alex (2021b): "Bitcoin is a Trojan Horse for Freedom"
- ▶ Hughes, Eric (1993): "A Cypherpunk's Manifesto"
- ▶ Hughes, Eric (2012): "Putting the Personal Back in Personal Computers"
- ▶ Koning, JP (2019): "Is Bitcoin Getting Less Volatile?"
- ▶ Luther, William (2016a): "The Political Economy of Bitcoin"
- ▶ Luther, William (2016b): "Cryptocurrencies, Network Effects, and Switching Costs"
- ▶ Luther, William (2019): "Getting Off the Ground: The Case of Bitcoin"
- ▶ Nakamoto, Satoshi (2008): "Bitcoin: A Peer-to-Peer Electronic Cash System:"
- ▶ Nair, Malavika and Nicolás Cachanosky (2016): "Bitcoin and entrepreneurship: breaking the network effect"
- ▶ Narayanan, Arvind and Joseph Bonneau, Edward Felten, Andrew Miller, & Steven Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies*
- ▶ Norland, Eric and Blu Putnam (2019). "Bitcoin Economics"
- ▶ Osman, Khadija and Olga Baysal (2021): "Health is Wealth: Evaluating the Health of the Bitcoin Ecosystem in GitHub"
- ▶ Rettler, Bradley (2021): "The rich get richer, the poor get Bitcoin"
- ▶ Selgin, George (2015): "Synthetic Commodity Money"
- ▶ Van Wirdum, Aaron (2018): "The Genesis Files: How David Chaum's eCash Spawned A Cypherpunk Dream"
- ▶ Warmke, Craig (2021): "What is Bitcoin?"
- ▶ Warmke, Craig (manuscript): "Electronic Coins"
- ▶ Wei, Yanhao and Anthony Dukes (2021): "Cryptocurrency Adoption with Speculative Bubble Prices"