THE BITCOIN STANDARD

RESEARCH BULLETIN

Dr. Saifedean Ammous

February 2019, Volume 2, Issue 1

How to really kill Bitcoin

Contents

For a software program, Bitcoin is unusually morbid. Its death has been a constant topic of conversation since its birth. Satoshi's first emails were greeted with skeptics telling him how his project dies, and ten years later, skeptics have not relented in dreaming up gory fantasies for how this death is finally achieved. **The Bitcoin Obituaries** page has so far collected around 350 obituaries for Bitcoin, for an average of 35 deaths per year since inception, an impressive achievement for anyone, dead or alive. No other program or protocol seems to inspire such morbid fascination, and at the risk of triggering the people at Bitcoin Obituaries into adding me to their list of notoriously rabid nocoiners and anti-bitcoiners, I have decided to focus this paper on the economics of Bitcoin's death. We will look at the common threats to Bitcoin, the economic incentives involved, and their likelihood. I argue that the economic incentives around Bitcoin are key to its survival, which means that the threats people usually discuss are unlikely to be fatal to Bitcoin. Based on that, I argue that Bitcoin's death, if it were to occur, would have to come from developments that undermine the economic incentives to use Bitcoin, which I'll discuss in two such potential scenarios.

In Chapter 10 of ***The Bitcoin Standard***, I presented several of the most popular ways in which people imagine bitcoin could die. These were hacking, a 51% Attack, hardware backdoors, internet and infrastructure attacks, a rise in the cost of running a node and a drop in their numbers, the breaking of the SHA-256 hashing algorithm, and a return to sound money. In this bulletin we delve deeper into these attacks as well as some others, and will show that many share a deeper cause and can be grouped into different meta-categories of death.

I. Government attacks

The most commonly discussed scenario for Bitcoin's death is a government attack. Anyone who's lived in the twentieth century has been conditioned to assume that anything government doesn't like will be banned, and initially there's little reason to suspect Bitcoin will be different. This was the cause for my skepticism toward Bitcoin for years since I discovered it.

The form of government attack or ban can come in many varied forms, some of which were discussed in ***The Bitcoin Standard***, and are not the focus of this bulletin. Rather than discuss the technical feasibility of these individual attacks, I will focus on what I view as the deeper underlying economic incentives that make these attacks highly unlikely to succeed.

Bitcoin, at a functional level, is an extremely basic technological implementation that performs a very simple and easy task: the propagation of a block of transaction data usually of 1MB in size (although it can go up to 3.7MB), roughly every 10 minutes to thousands of network members worldwide. To be a peer on this peer-to-peer network, which allows you to validate your own transactions in accordance with the protocol's consensus rules, all one needs is a device capable of receiving up to 3.7MB of data every 10 minutes. To merely send or receive a transaction, without one's own node, only requires a device that can send a few hundred bytes of data.

As such, Bitcoin is a far simpler and lighter program than Amazon, Twitter, Facebook, Netflix, or many of the popular online services that involve more extensive interactions and operations. The technical requirements for sending a few megabytes of data around the world continue to get cheaper, simpler, and easier with the development of technology and the large accumulation of capital in the computer and communication industries. Currently, there are tens of billions of devices worldwide that are capable of sending and receiving data, including practically all the world's personal computers, smartphones, and tablets.

The common misconception many nocoiners have about how the internet works is that all these computers need to connect to some central server in order to access the internet, but that's simply not the case. The Internet does not have a central location that distributes content; the Internet is simply a protocol that any computer can use to connect to other computers. As long as two devices can be connected to one another physically or through various mechanisms to transmit data, then the Internet survives, and so can Bitcoin. Had the Internet been a centralized institution, then shutting it down would be straightforward, but while governments can certainly destroy or disable much of the globe's Internet infrastructure and inconvenience users, they cannot stop computers from communicating with one another. Because Bitcoin's computing requirements are as low as they are, and the value held in it is large enough to motivate people to try their best to maintain the network, it's likely that bitcoin transactions and blocks would continue to be generated through any kind of ban.

As Bitcoin continues to grow and attract more attention from the technical community, developers are innovating even further on the different ways to transmit Bitcoin data quicker and at lower costs. **Mesh networks** and **radio waves** are two of the most interesting examples, because they allow the use of the network even without a connection to the Internet. Even the absence of Internet capable devices is now not much of an impediment, as it is becoming easier to join the network with any device that can send and receive data. With the introduction of Bitcoin-specific satellites, the scale required of a government-sponsored attack continues to get exponentially larger.

Bitcoin has found a way to make access to a hard form of money globally available at a much lower cost than the previous alternative, gold. Since hard money is a hugely important and beneficial technology, people also have a strong incentive to meet the costs to be able to use this hard money. As time goes on, the liquidity and utility of bitcoin only increases, raising the incentive for people to use it and allowing them to overcome more and more serious barriers.

Ultimately, if Bitcoin provides value to its users, they will make the effort to ensure they are able to access it; that motivation, more than any technical aspect, is the real impediment to government attacks on Bitcoin. History provides many wonderful illustrations of the power of economic incentives and their ability to repeatedly overcome government regulations. A good introduction to this can be found in the great book **Forty Centuries of Wage and Price Controls: How Not to Fight Inflation**. History clearly shows how such attempts fail, because government edicts cannot overturn economic reality; all they can do is change the economic cost/benefit to specific actions, and cause people to adjust their behavior accordingly to still get the benefits while trying to avoid the costs. This is why price controls lead to shortages, black markets, queuing costs, and conflict, but can never lead to a reduction in prices that the government purports to intend.

Far from an effective way to destroy Bitcoin, a government clampdown would arguably strengthen it by blatantly advertising its real potential and value proposition to the world. Government attacks on Bitcoin can only happen with restrictions on individual and financial freedom, which are the best reasons to buy bitcoin. The simple statist mind assumes that reality is subject to government orders: if government bans X then X ceases to exist. In reality, it just makes the provision of X much more profitable, and increases the levels of risk that people are willing to undertake in order to provide it. For example, a government order to stop banks from allowing their clients to use their balances to buy bitcoin might hurt Bitcoin in the short run, but it would be a great advertisement; it would clearly communicate to people that the money in their bank accounts is not theirs to spend as they please, and instead is the government's money which is limited to only government approved uses. As this reality begins to sink into people's minds, more

and more will want to hold on to a monetary asset whose value is independent of government preferences and whims, and so the demand for bitcoin will likely rise (along with the profitability of supplying it).

An example of the counter-productivity of bans can be found in the drug war. For almost fifty years, the US government has killed and incarcerated millions of people in the US, Mexico, Colombia, Afghanistan, and many other places in the world in a feeble attempt to stop drugs that can still be bought on the street of every US city. Drugs come from plants that need to be grown under the sun, then processed and shipped around the world through a long network of suppliers before reaching the end consumer. Drug distribution is a far more complicated and demanding task than distributing Bitcoin blocks, which don't need physical supply lines and can be transmitted over the simplest data transfer technologies available. While drugs give their users a large incentive to consume and pay for them, it is still arguably not as strong as the monetary and economic incentive to use bitcoin, which can be a matter of life and death for many people. With a stronger incentive than drugs, and an infinitely easier distribution mechanism, any government that tries to ban bitcoin has a seemingly impossible task.

Another non-trivial obstacle for a government attack to overcome is that Bitcoin has arguably become too politically ingrained to be the subject of a clampdown. I think this tipping point was reached during the bull market of 2017, when the mainstream of American society really started buying and holding bitcoin. This point was driven home to me during the **testimony of CFTC Commissioner Christopher Giancarlo to US Congress**, when he explained how his niece was a hodler. It is extremely unlikely that members of Congress are going to pass laws that sic law enforcement against their own family and friends. Even the bankers that viscerally and rabidly hate Bitcoin (for good reason!) are watching helplessly as their children's interest in it grows. As JP Morgan, one of the US government's largest welfare recipients, enters the world of shitcoinery, it is worth remembering the hysterical episodes their CEO had during 2017 every time he was asked about Bitcoin. In particular, it's worth remembering how clearly agitated he was when recounting that his daughter had bought bitcoin, likely at a time when its returns exceeded those of her father's own portfolio. While you would not put much past Dimon, it's safe to assume that using his political influence to have people like his own daughter thrown in jail is a stretch too far.

What this all means is that Bitcoin now has a motivated and very vocal small minority of the population interested in it. A motivated and organized minority is likely to get its way in US politics for the simple reason that it cares more than other groups about its own issue, whereas the rest of the voters and special interest groups care about other issues. While people think of democracy as the rule of the majority, it is more accurate to think

of it as the rule of the organized minorities. Corn farmers, for example, are a tiny fraction of the total population of the US but still manage to get enormous subsidies. Although these subsidies are a cost to everyone else in the US, they're a small cost to everyone; conversely, the benefit to corn farmers is massive, and they have every incentive to make it their prime voting and lobbying issue. From a politician's perspective, going with the corn lobbyists will get you votes and money, but going against it will only get you enemies and no supporters, because almost no one is hurt so much from corn subsidies to base their vote on it.

Bitcoin's motivated minority is growing into this kind of force in political systems worldwide. Any politician that attempts to clampdown on Bitcoin will be faced with indifference by the vast majority of the population, and strong opposition from bitcoiners.

My personal view is that in the last few years Bitcoin is a genie that has grown beyond the ability of governments to put it back in its bottle. The secret is out, and millions of people worldwide have heard of it and are interested in using it. They are willing to invest time and effort into ensuring it continues to be available for them. Government clampdowns may inflict suffering on individual bitcoiners, but I doubt that it will be able to kill Bitcoin itself.

II. Software bugs

Back in September of last year, a bug was found in the code of Bitcoin Core versions 0.14 to 0.16.2 which could have allowed for increasing the total supply of bitcoins above 21 million. Had the bug been discovered by a malicious actor, they may have been able to use it to attack the network. **Jimmy Song has provided a great analysis** of this incident, and he suggests that although the likely ramifications of exploiting this bug would have created problems for the network, it was unlikely to have been fatal.

Nonetheless, the episode made vivid one more type of threat afflicting bitcoin: malfunctioning code, or software bugs. Whether through an innocent mistake in the coding, or through the malevolent design of an attacker, it is not inconceivable that there could be problems with the Bitcoin code that could cause it to malfunction.

The threat of bugs and malfunction is far more serious for Bitcoin than for most other computer programs, because Bitcoin's value proposition depends on its immutability, reliability, and complete predictability. If it is evolving to fulfil the role of digital gold, then the most important characteristic Bitcoin needs to copy from gold is its constant re-

liability and predictable supply. A bug that hinders the operation of the software or allows some users to create more coins will severely compromise the network and the likelihood that it would continue to succeed in that digital gold role.

Rather than focus on the technical details of this bug and how it was fixed (which Jimmy's article discusses), I would like to focus on how Bitcoin's open source development counters this threat, and how individual users could help reduce the likelihood that it could affect them.

Linus Torvalds, the original creator of the Linux operating system, famously said that "with enough eyeballs, all bugs are rendered shallow"; and that is a great explanation of the prime value proposition of open source software. While open source software usually relies on the efforts of volunteers that are not paid to be fully focused professionally on the software, its collaborative nature can attract many people to review the code and improve it, which helps prevent critical bugs from emerging. This has proven a surprisingly successful and robust model. Whereas proprietary software development resorts to employing a few full-time highly focused individuals, open source development allows anyone to contribute and gives all users of the software the choice to adopt anyone's contributions. The process of constant innovation variation and user selection creates a strong evolutionary pressure that drives the code's improvement.

Open source development is also a wonderful example of **Friedrich Hayek's concept of Spontaneous Order**, or order that emerges not through any preconceived individual design, but through human action. **Vernon Smith builds on Hayek's work** to differentiate between two types of rationality in human affairs: constructivist rationality, and emergent rationality. Constructivist rationality refers to conscious human design to bring something into being; it is similar to designing a car, a house, or any technical object that requires top-down design. The triumph of enlightenment thinking and industrial revolution, while being enormously beneficial to humanity, has nonetheless created a bias in the mind of the educated to view everything as the result of constructivist rational design. But the majority of market and societal institutions were never top-down designed by one designer, they emerged over many years through the actions and interactions of individuals. Hayek argues that the majority of the human institutions that shape our lives, from language, to customs, to economic institutions, ethics, and manners, are all emergent products of human action, and not the conscious effort of human design.

This simple but powerful concept is pivotal in understanding how human society functions; it is also something that victims of state education have the most trouble comprehending, as statist education relies on convincing students that everything needs to be rationally planned and controlled. It is also essential in understanding how Bitcoin has continued to evolve after Satoshi left the project with nobody in charge of

it. In the 8 years or so since he has disappeared, the bitcoin software has improved significantly, and yet no single individual can possibly be viewed as responsible for these changes. While each individual change to the software can be viewed as a product of rational design by one or a few programmers, the choice of which changes get adopted by users, how the changes build on one another, and the general direction of open source development are a complex and emergent result of the interaction of variations and individual choices.

This is one of the most infuriating aspects of Bitcoin to statists and people who have no familiarity with Austrian concepts of spontaneous and emergent order. Lawyers, Keynesians, and all manners of people in thrall of their powerful government are constantly seeking out the person in charge of Bitcoin, and try their best to demand someone be held legally responsible for it, attempting to corporatize Bitcoin's structure and have clear chains of command and responsibility. These people simply cannot understand the concept of voluntary collaboration, and that a user who downloads open source software does so at their own discretion, not at the responsibility of the person who volunteered their time to building it.

Bitcoin's lack of central control, and the absence of a constructivist rational approach to its programming, is far from a disadvantage; conversely, it is the most effective way for it to remain predictably neutral. This lack of central control also offers a huge edge for dealing with software bugs, because a wide variety of eyeballs from all over the world examine the code and try to find mistakes within it. This is the process that keeps all manner of open source software running, as mentioned by Linus, and in the case of Bitcoin the process is put on the powerful steroids of economic incentive of thousands of people who have a vested interest in Bitcoin succeeding. In other words, what protects Bitcoin from software bugs, ultimately, is the economic incentive for its users to remove and deal with bugs as quickly as they emerge. And the recent bug is a good example of that. While it might have been theoretically possible for a well-funded attacker to exploit the bug, realistically it was highly unlikely due to the economic incentive for all Bitcoin users to detect these bugs before they can be exploited. Attacking Bitcoin offers very little economic reward, and so is unlikely to attract the same number of motivated eyeballs. An attack on Bitcoin is destined to be a top-down design with a few focused highly skilled individuals trying to execute it. Bitcoin's defense consists of many thousands of users and coders constantly vigilant and defending against anything bad happening.

As Jimmy concludes:

> ***Bugs will always exist, but the important thing is to have a robust process for dealing with them. Open source software development has shown itself to be more reliable in the long run. Bitcoin adds to it strong economic incentives for many economic parties from developers to businesses to invest heavily in this process as well.***

It is impossible to conclusively prove the absence of bugs in a piece of software, because one can only ever dismiss the bugs they can imagine, while the potential bugs are always larger than a single analyst's brain. It is nonetheless possible to have strong economic incentives for managing and dealing with these bugs. Beyond that, Bitcoin's extremely conservative and meticulous design itself ensures there is another layer of safety for dealing with any critical software failures: the ability to roll back the chain and return to the historical state before the bug had struck. This would likely mean that any critical bug will be temporary rather than permanent. If one were to compare this to aircraft maintenance, it would be akin to having a function that allows you to return a crashing flight to its pre-crash state and perform maintenance on it, inconveniencing the passengers rather than leading to their death.

The second point to take from this incident is about the speed at which Bitcoin software upgrades happen. For a project whose main value proposition is immutability, a case could be made that the current speed of upgrades and iterations in Bitcoin development is a little too fast; users might benefit from being slower with their upgrading, letting newer versions of software get tested slowly and gradually on progressively larger sections of the network nodes before they are widely adopted and accepted as stable.

There is currently no pressing need to upgrade Bitcoin or improve its capabilities. For what it does, it faces no serious competition from any digital currency. Its only competition are central banks and global gold shipments. It is far cheaper than both for what it does, and its current capacity for final settlement is unmatched.

Even by Bitcoin's proven existing capabilities of only half a million transactions per day, which it demonstrated it could safely carry out in December 2017, and even with transaction fees that are 10 times higher than the maximum they reached last December (i.e. even with a $500 transaction fee), it is still a huge bargain for what it does; it could find significant demand either as a direct network for international payments, or as a settlement layer for a large network of Bitcoin full nodes that carry out the function of banks (either digitally or in physical locations).

There is no scaling crisis for these significant use cases, there is no impending technical threat that is likely to doom Bitcoin, and as such there are no compelling reasons why Bitcoin should change drastically from what it is currently. This is why, for users, it probably makes sense to be lagging adopters on minor updates, and to select for software versions with less frequent upgrades.

For bitcoin to succeed, it needs another, say, twenty years of functioning exactly as reliably as it has (and not necessarily at any larger scale) in order for it to be implanted in the mind of most adults as a simple and reliable boring piece of open source software that anyone can use in predictable ways. It will take a generation that has come to hear of the idea of a form of money that is not controlled by governments. It will, sadly, take the death of the most bit-

ter elder nocoiners, who amassed their wealth and credibility in the constructivist rational monetary policy era and who are wholly unwilling (and in many cases, incapable) to understand the certainty of hard digital money.

When people talk about the slow rate of bitcoin adoption, the limitation is never in software capabilities or scaling capacity. The market has shown consistent capacity for scaling solutions, both on-chain and off-chain. Demand for block space is an extremely competitive market, and geniuses are constantly innovating ways of utilizing it more efficiently. Even if Bitcoin successfully serves as a base layer for settlement, and secondary layer solutions develop on top of it, it would still be an enormous improvement over the current monetary system because it would be far more decentralized and harder to capture by government. There is no pressing need to risk Bitcoin's progress toward fulfilling that use case in order to upgrade its technical capabilities. Provided Bitcoin continues operating successfully, the delay in bitcoin adoption is purely a matter of time needing to do its inevitable thing and pass. It's the same reason any technology takes time to spread. Most users will never become technically competent enough to understand all the nuances of its functioning. But time is needed. People need to see the technology operating successfully, safely, reliably, and consistently for a significant period of time. Most people eventually got on airplanes not because they studied jet aviation, but because they had seen and heard of airplanes operating reliably for years before they got into them. Similarly, people will start to trust a digital form of storage not due to an extensive study of bitcoin and cryptography, but rather after seeing it work reliably for years for others.

The critical thing, then, is not scaling, privacy, or user-friendliness, the critical thing is Bitcoin's survival. The major milestone for Bitcoin is its ability to continue as one chain of undisputed transactions among its holders. This would mean that Bitcoin's governance and security system has succeeded at all times in achieving consensus among its participants on the validity of the ledger of transactions.

III. Failure of economic incentives

The Bank of International Settlement has recently **published a report** in which it concludes Bitcoin's incentives model is unsustainable and likely to lead to security failure if Bitcoin were to grow in economic importance. The report is largely based on a **recent paper by Chicago School ecnomist Eric Budish**, which finds that bitcoin's security model will be vulnerable to attack as the block reward shifts from offering mainly new coins, as is the case now, to consisting mainly of transaction fees, as is expected in the future.

The BIS fundamentally fails to understand that economics is based on a subjectivist conception of value, and not on an objectivist conception of value. This is the starting point of all disagreement in economics, and the underlying difference between correct Austrian economics and the fiat economics taught at universities and popularized by bureaucracies like the BIS.

As elucidated by the father of Austrian economics Carl Menger, all value is subjective and cannot exist outside of human consciousness. Objects have no value intrinsic to them, it is only human consciousness that prescribes value to them. Value is not an objective attribute of objects that can be calculated like mass, temperature, or volume. It cannot be computed objectively because it is constantly shifting in the human consciousness as time passes and conditions change. Value is determined at the margin, at the specific time and place that the valuing individual is making the decision.

On the contrary, all the main non-Austrian schools of economic thought hold value to be objectively determined. The Marxists think value is determined by labor inputs, while most other mainstream economists think of it as a function of production costs. These schools of thought conflate value with price, and thus assume that both are determined by the cost of production.

From the mainstream perspective, producers produce things at a certain cost, and consumers then need to pay that price to compensate them for these goods. From the Austrian perspective, humans subjectively value things, and producers try to supply them at that price.

Unsurprisingly, the BIS bases its critique on the work of a Chicago school economist. While Chicago economists are generally viewed as pro-free market, their strictly objectivist and positivist methodology has very little in common with the Austrians. The paper makes the classic mistake of putting cost before value. In reality, there is no fixed bitcoin security expenditure that is needed for proof of work to successfully protect the network. It is the very fact that people subjectively value bitcoin that creates demand for holding it and for transacting with it. The bitcoin asset cannot be owned outside of transactions confirmed in bitcoin blocks, which inevitably creates a market for this scarce block space. Bitcoin's difficulty adjustment algorithm ensures the scarcity of this block space (and thus the bitcoin token itself) by raising the hash power, and thus the cost, required to produce these blocks. The cost to

produce bitcoin blocks is merely a reflection of the market's valuation of bitcoin, which is ultimately the subjective value people place on it when transacting with it on the market for other moneys or goods and services.

If the market places a value on bitcoin block space, an economic incentive will exist for miners to provide this block space securely. The manner in which users will pay for this block space may differ, but the cost is real nonetheless. In all markets, the presence of demand incentivizes entrepreneurs to find the most effective ways to provide the good that people want; the costs and the methods of payment can differ widely, but if the demand exists, the good will be supplied.

Consequently, if there is enough demand for holding bitcoin, then demand will exist for transacting it widely and people will pay the transaction fees necessary to get their transactions into blocks. The notion that block space will go unbid despite their desire to obtain and hold on to their bitcoin is absurd. The BIS emphasizes its deep ignorance of economics and prices when it presents a scenario in which demand for bitcoin is so high as to necessitate massive security expenditure, while demand for block space is nonexistent. In reality, the opposite is always the case. Block space is very scarce and people are constantly finding new ways to use it more resourcefully. This demand is inextricably linked to demand for bitcoin: if demand for bitcoin increases, transaction fees will go up and push scaling solutions onto the second layer, making on-chain transactions more valuable settlement transactions which can pay higher transaction fees.

Due to the difficulty adjustment algorithm, the cost of making a bitcoin block is always going to hover around the value of the total reward offered by the block (including the block reward and transaction fees). Given that the average block today is around 1 MB of data and has a total reward of around $50,000, the going rate for a single byte of data on the bitcoin blockchain is around $0.05, making it the most expensive byte of data in the world. By comparison, a byte on a commercially available hard drive is worth around a trillionth of that.

Should demand for bitcoin exist, then demand for bitcoin blocksize must exist because it is the only way in which bitcoin can be owned and transacted. It is perfectly feasible, of course, that demand for bitcoin might one day decline, or even collapse. In such a case, it necessarily follows that bitcoin's value will decline enormously, and the value of its block space will follow. The network could fail due to a collapse in demand, as discussed in the sections below, but that is irrelevant to whether the mining is being rewarded mainly through inflation or transaction fees.

As it currently stands, compensation is incurred in the inflation that will dilute the value of your coins as a percentage of total bitcoins. Even if they don't think of it that way, it is happening. New coins come on the market every day and depress the price of existing coins, effectively devaluing holders'

coins. In the future, the majority of the cost will shift toward the transaction fee needed to obtain your coin, and there is no reason to presume that the market participants who desire the block space necessary to own bitcoin would not pay for it using this other method. There is a real cost to bitcoin which holders are happy to incur because bitcoin is still useful even after taking these costs into account.

If users don't pay transaction fees, then miners won't solve the proof of work problems and transactions won't confirm. This will put pressure on coin owners to pay transaction fees so their transactions get confirmed, and fees will rise.

We already have evidence that strongly suggests bitcoin users will be happy to pay transaction fees. In December 2017 during the last bitcoin bull market, fees rose to around $50 per transaction. Yet despite this increase, there was still very high demand for transactions, which suggests that if people want to hold hard money the transaction fee has a lot of room to grow. If one were to look at the exchange fees people usually pay to buy bitcoin around the world, we find that they are usually much larger than the on-chain transaction fees. Bitcoiners still have no problem paying these extra fees, so it is hard to imagine them giving up on bitcoin because on-chain fees have increased. Premiums for buying bitcoin in places where exchanges do not operate are even higher, and it is not uncommon for buyers on localbitcoins to accept a 10 or 15% markup.

If my contention is correct that bitcoin is the hardest form of money ever invented, it is absolutely inconceivable that demand for it will be destroyed by people's realization that they cannot use this technology for free. Every form of money transfer will involve some transaction cost and bitcoin is no different. If people value bitcoin, the economic incentives of the system have proven resilient enough to motivate people to spend the resources needed to keep their network secure. If Bitcoin dies, it will not have died because of misaligned economic incentives (high transaction fees). It will have died because the demand for it has declined.

If demand for bitcoin declines or disappears, then the price will likely crash and Bitcoin will collapse and/or be attacked, regardless of if the miners are being paid in inflation or transaction fees. But if bitcoin continues to appreciate for the next 20 years, even at a rate no more than one tenth of its historical growth rate over the past ten years, it will become a global settlement network with value in the trillions of today's dollars. Would people not be willing to pay for the daily settlement of hundreds of billions of dollars across the world?

The best way to gauge the willingness to pay for these fees is to look at settlement costs across the world today. The only real alternative to a bitcoin payment, as a form of hard cash whose value isn't the liability of a government, is the settlement of gold cash reserves, a hugely expensive process. Bitcoin transaction fees are an inconsequential rounding error compared to gold transaction fees. Given the unique service it provides, there is enormous scope for the growth in transaction fees on top of

the bitcoin network, which makes the BIS' concern trolling sound quite misplaced, if understandably motivated.

One counter-argument here is that transaction fees might provide some money to miners, but they will not be sufficient to attract enough mining hashpower to protect the network. The mistake here is to assume that a fixed amount of electricity or hashrate is needed to secure the network, when in reality no such stable level can exist because computing is a highly competitive industry where the cost of hashpower is always declining. The network hashpower that successfully protected Bitcoin from attack in 2014 is a tiny fraction of the total network hashrate today, and yet it was sufficient in 2014.
To be secure, Bitcoin does not need a fixed sum of electricity or hashrate; instead, it needs to create a liquid market in electricity and hashing power that constantly attracts a serious amount of capital infrastructure to produce mining hardware. By simply providing a highly liquid instrument as a reward for expending electricity and processing power, Bitcoin continues to attract the most efficient producers of electricity and processing power to monetize their resources. As long as this unique market continues to exist and offers valuable rewards, it will make any attack considerably expensive and unlikely to succeed. In particular, Bitcoin's unique impact on the electricity market, **as discussed in depth in TBSRB3**, means that Bitcoin is an insatiable buyer of any cheap electricity that exists anywhere in the world. Whereas any attacker will need to mobilize enormous amounts of expensive energy in centralized locations to try to attack the network, Bitcoin can draw on the cheapest sources of energy in many locations worldwide by offering rewards for selling electricity that producers would not be able to sell elsewhere.

According to the BIS, the limit in bitcoin transaction fees is a result of bitcoin's inability to scale. The BIS divides an incorrect estimate for security costs by the number of transactions that bitcoin can perform to calculate the fixed cost per transaction. Since the bitcoin subsidy is scheduled to run out, they reason that the cost of securing the network will have to be divided by the number of transactions and that only if people pay that transaction fee will Bitcoin survive. This narrowly defined formula itself (let alone the incorrect cost estimate as discussed above) clearly shows that the BIS is unfamiliar with Bitcoin's layered scaling approach. The number of on-chain transactions is not a meaningful limit to how many transactions can be carried out with bitcoin, because as explained in The Bitcoin Standard, Bitcoin's scaling will likely happen on second layer solutions, in a way somewhat similar to how gold banking scaled. Under a gold standard, not all transactions took place through physical gold moving hands. Physical gold was largely stored in banks, and for each movement of physical gold used to settle many transactions between financial institutions, financial instruments backed by that gold would change hands many times more. There is no reason why Bitcoin cannot scale like that, and in that case, each bitcoin transaction cannot be compared to individual consumer payments, but to large

settlement payments between financial institutions. If each on-chain bitcoin transaction is settling for many thousands of individual consumer payments, then even infinitely tiny transaction fees on consumer payments could add up to very large fees for individual on-chain settlement payments.

The BIS here is making the mistake than many bitcoin purists often commit, which is to suppose that bitcoin can only succeed and operate if every interaction with it is entirely trustless and decentralized, and if every user is able to make a completely trustless permissionless payment on its main chain. While this sounds nice in principle, in reality the level of security of a bitcoin transaction is absurd overkill for the vast majority of transactions that humans conduct in everyday life, for which less reliable systems are acceptable (even with the occasional security failure). There is no need for a coffee salesman to require on-chain verification of your payment, and the current credit card payment system is much cheaper and faster; even with a regular amount of small fraud, it continues to be a more effective solution for small consumer payments. The value of Bitcoin's decentralization is not in that every consumer purchase is uncensorable and trustless, but rather that it helps the network resist government attack and capture. Some purists seem to think the choice we have is between a world in which everyone is able to trustlessly use Bitcoin's on-chain base layer for all their transactions (no matter how trivial), and a world in which only the base layer of bitcoin is trustless and other layers involve trusted third parties. If that indeed were the choice, any bitcoiner would of course prefer trustlessness for all. However, engineering reality seems to suggest that the choice is actually between Bitcoin being trustless only at the base layer, or a fiat monetary system which is government-controlled at all layers.

If Bitcoin's "only" contribution is to make the world's monetary system's base layer and the money supply free from government control, that would be more than enough. The world of payment processing will vastly improve with a free market in banking and money, but even if nothing improves in it, bitcoin would still be a world-changing success. Trustlessness and immutability are not simple engineering features that can be copied and replicated, and the only proven example of a trustless system we have so far is Bitcoin's on-chain transaction, with a capacity of around half a million transactions per day. The idea that we can scale that level of security is becoming less tenable with time, but that is not really a problem that hinders the core proposition of bitcoin. The level of security bitcoin provides is only really necessary for the most important transactions in the world, while current security arrangements are ok for most coffee purchases.

Beyond the economic incentives for mining bitcoin, the deeper web of economic incentives to run and maintain bitcoin is what makes such a failure unlikely, even if the BIS' economic analysis were correct. If Bitcoin's proof-of-work were to prove compromised after block subsidy diminishes, and if mining hashrate began to decline as the cost to the network of hashrate became more expensive, it would be a

clear threat to bitcoin; in such a case, it should not be very difficult to get bitcoiners to agree on a fork that corrects this. Forks are extremely hard to implement with bitcoin for upgrades, but that would likely change in the case of emergencies.

Ultimately, doomsday scenarios in which Bitcoin fails due to a technical design glitch don't take into account the economic incentives to keep the system successfully running. As long as demand for digital hard money exists, many millions of people around the world are motivated to find solutions to continue to make it exist. Bitcoin has a very straightforward technical requirement to operate, and it performs a very simple job that requires very little and has enormous incentives backing it.

IV. Bitcoin scenarios

In **TBSRB1**, we discussed the possibility of Bitcoin being adopted by modern central banks. In **TBSRB2**, we discussed three different scenarios for Bitcoin monetization. In this month's TBSRB5, I will outline what I view as the two worst case scenarios for Bitcoin, where it fails and collapses. In total, this will give us six potential scenarios for how bitcoin's development could happen, which can be arranged in order of decreasing favorability for bitcoin as

Possible scenarios for Bitcoin:

1. Central bank adoption

In this scenario, global central banks decide to start using bitcoin as a reserve asset to settle trade between one another and back their local currencies. The political independence of international settlement and the hardness of the monetary asset would give countries who use bitcoin as a reserve asset an advantage over countries that haven't. As the price rises, more central banks will want to join. It is conceivable that in this sort of scenario, bitcoin, as the hardest money invented, would win the global monetary race as decisively as gold had won it in the nineteenth century.

But as discussed in more detail in **TBSRB1**, I do not find this scenario compelling, primarily because:

> ***the mental models governing the people in power in governments and central banks all over the world, the self-interest of these elites which lies in maintaining inflationary money at home, and the threat of US military and economic power against any defections from the dollar standard all lead me to be highly skeptical of the possibility that central banks will adopt Bitcoin any time soon.***

2. Hyperinflation

My impression is that a majority of bitcoiners imagine that bitcoin's rise must be accompanied by hyperinflationary collapse of government money. In **TBSRB2**, I offer a detailed explanation of why I think this is far from certain.

> *The key is to remember that the process of money creation in the current monetary system is driven by lending and credit creation, whether in the narrow banking system or the shadow banking system.*
>
> *With artificially manipulated interest rates, it becomes harder and harder for people to save for the future, and thus more likely that they get into debt. Fractional reserve based credit creation does not just increase the money supply, the flip side of this coin is that money supply increases and lower interest rates drive demand for more credit creation.*
>
> *When the value of money is constantly dropping, and interest rates are artificially low, people will move from saving to borrowing. But when a new and completely decentralized, depoliticized, and automated hard money enters into the economic calculations of the individual today, that individual's relationship with credit is likely to change. With the presence of a hard money that can appreciate in value over time, people's need for credit will likely decline. As those who move to Bitcoin witness its value appreciate, they find themselves able to pay off their debts sooner. As they become debt free with hard savings that nobody can inflate, they're likely to start living off of their savings and accumulating more, rather than continuing to borrow and pay interest.*
>
> *As more people pay off their loans and fewer people demand new loans, the financial system's credit creation is contracted significantly, and as a result, the growth in the supply of money slows down, or possibly even reverses into a shrinking supply.*
>
> *The availability of bitcoin as a hard store of value will seriously undermine the value proposition of going into debt that keeps the current monetary system able to create money. It is true that demand for government money would be reduced as people move to bitcoin, but the flipside of this process is that supply is also reduced, rather than expanded, as the appreciation in bitcoin's value makes individuals less likely to demand credit.*

3. Smooth upgrade

As discussed in TBSRB2, the calamity that was government-run money allowed for the monetization of debt. As discussed in *The Bitcoin Standard*, anything which can be used as money will offer a large incentive for people to produce more of it, and debt is no exception. As debt became a form of money, anyone who could produce monetizable debt was able to practically print money. Banks and governments, and their central banking bastard children, are the only entities legally allowed to create

money through the creation of debt, and they have inflated the supply of their money enormously by plastering the entire planet with debt. Bitcoin is a neat technological solution to this problem because it introduces a superior monetary asset that cannot be stopped by government. Bitcoin getting monetized means more and more people will choose to hold it rather than government money, and more importantly, perhaps, that fewer people will want to take on government debt, and thus, less government money will be created.

4. Monetary vigilante in the shadows

If we accept the premise that bitcoin popularity is an inverse function of the popularity of central bank policies, then bitcoin adoption might be most effectively stalled through improvements in central banking monetary policies around the world. It is an empirical question whose answer we will have to observe in the real world, and to examine just how good a monetary policy would be needed to kill growth in demand for bitcoin.

As discussed in TBSRB2, it is quite conceivable that if the majority of the world's central banks were able to achieve monetary policies as successful as those of the 1990s in major western economies, (without the financial bubbles, which, of course, is no walk in the park) then demand for bitcoin would be stalled from growing too quickly. Austrian economists and sound money fanatics will find much that is wrong with the central planning of monetary policy as it was practiced by most global central banks in the 1990s, and will correctly point out that this mirage of stability that the central banks offered came at the expense of creating larger fragilities which came crumbling periodically with asset bubbles and market collapses. But the average citizen arguably does not care a lot about this, and if central banks have the extra fear of bitcoin to discipline them, they might end up doing a better job than even in the 1990s, and in the process undermine demand for bitcoin. Due to the very nature of government-controlled central banking, financial crises will occur, governments will find it hard to resist the temptation to inflate in various episodes, and bitcoin will likely continue to have some marginal demand keeping it and its network alive.

But continuing on the premise that bitcoin adoption is stalled through effective monetary policy, what would be the result of returning monetary policy to the best form of monetary policy the modern world has seen? In other words, forget about the 1990s, what would be the impact on bitcoin if we returned to the monetary system of the 1890's?

V. Government gold standard

As discussed briefly in The Bitcoin Standard, the government policy that would likely be the most destructive to bitcoin would be implementing a gold standard similar to that of the end of the nineteenth century. All government restrictions on bitcoin are restrictions on financial freedom, and these are exactly what create demand for bitcoin, creating more incentives for people to use and hold bitcoin. Given that the technical requirements for operating bitcoin are increasingly simpler to attain, the government activities that aim to restrict bitcoin will inevitably result in more incentives for people to overcome these restrictions.

Contrary to the statist instinct to want to ban anything that sounds objectionable, the more effective path for governments to undermine bitcoin would be to undermine the economic incentive for people to use it, which would mean increasing the financial and monetary freedoms that individuals have. The monetary system that would allow governments to maintain some form of monetary control while allowing the largest margin for free market in money would be the adoption of the gold standard. While theoretically a government could introduce a hard money standard with its own currency, and commit to not increasing the supply beyond a specific percent, such a commitment will never be as credible as using gold as money and thus tying government's hands. A government commitment to low inflation and relative financial freedom would likely prevent mass adoption, but actually returning to a gold standard could have more serious ramifications for bitcoin.

A world with a gold standard would look very different from today's world, particularly in terms of the role of government and the extent to which it would intervene in its citizens' lives. If one thinks of the main drivers of bitcoin adoption, none of these existed under the gold standard.

Under the gold standard, there were no examples of hyperinflation or high inflation as we witness across the world today, driving significant demand for bitcoin. Governments were highly unlikely to impose high taxes that would provide a very large incentive for storing wealth in moneys outside the reach of the state. The notion of a war on drugs or chemicals was an absurd idea at that time, as governments could not finance such ridiculously unproductive nanny policing and the heavy cost it inflicts on society. Arguably, as discussed in Chapter 8 of ***The Bitcoin Standard***, it is the absence of a politically-neutral market-chosen medium of exchange, that is at the root of financial markets becoming highly volatile markets for short-term gambling rather than a mechanism for the long-term allocation of capital, as it was in the gold standard era. I would argue that a move back to hard money would even seriously curb the gambling instinct that has driven much of the demand for bitcoin. In a society with hard money, people are likely to be far more discerning with allocating their hard money and as a result, the demand for experimental highly volatile digital cash is likely to be lower.

A move to a gold standard would undermine all of these drivers of bitcoin adoption, and it remains

an open question whether in such a world demand for bitcoin would be enough to prevent attacks and secure the network.

While many bitcoiners are dismissive of the monetary role of gold as being an analog heavy inefficient version of bitcoin, I would urge them to be more cautious, as gold has been written off many times before, and yet it has been playing a monetary role for thousands of years, and there are good reasons to still believe its days are not over yet.

Gold currently has a far larger liquidity pool than bitcoin. The value of all the mined gold stored and held is in the range of around $8 Trillion, more than 100 times larger than the value that is stored in all the bitcoins currently in circulation. This very large pool of liquidity means gold currently has far more salability than bitcoin. In other words, for someone looking to buy or sell something, the probability that they will find a counterparty for that trade willing to pay or accept gold is far larger than the chance of finding someone willing to pay or accept bitcoin. A move to gold would be far more palatable for the majority of the world's population, since they either own gold or currencies backed by gold. Gold also has a 6,000 year first mover advantage over bitcoin, it is easier and more intuitive for people to understand trade in gold coins or gold-backed assets. Handling private keys securely is not exactly very easy, and is arguably outside the scope of technical competence of many, if not a majority of, people alive today. Such objections have been leveled at every new technology, of course, but in many cases people have learned to use difficult new technologies like cars, computers, and phones because it was very useful. Bitcoin might well turn out the same, over time, but there is one factor that makes this more tricky because competence in the use of bitcoin is related to competence in programming, a highly specialized field in which the highest levels of competence are concentrated in a very small number of people. The hierarchical nature of this knowledge means the vast majority of people will always be at a strategic disadvantage compared to a small number of people with much better technical skills. Even though the code is open source and people can verify it before they run it, the ability to understand and operate with the code will never be equally distributed. It might just be the case that this kind of asymmetry in knowledge and competence will lead to the constant proliferation of scams, thefts, and hacks that prevent the widespread adoption of bitcoin and keeps it on the fringes. The sounder the government-offered monetary alternative, the less likely such burdens are to be overcome. A return to the gold standard offers the best chance for a government-controlled monetary system to survive the threat of bitcoin.

A gold standard would curtail the ability of government to intervene in the banking system and protect incumbents from outsiders, which would likely unleash innovation and experimentation in financial systems. With free market competition and innovation, it is not difficult to imagine the development of highly convenient payment technologies backed by gold. There is no reason that any of the modern

payment innovations developed over fiat money and digital currencies cannot be implemented on top of gold, with 100% reserve backing.

How realistic is this threat to bitcoin? For starters, even if this were to all come to pass, it might just delay the adoption of bitcoin, but not change the long-term reality that would arguably be dictated by the higher stock-to-flow ratio of bitcoin. Even if new adoption of bitcoin slows down considerably, and there are significant crashes in the price, the slow increase in the supply will still make bitcoin likely to recover and appreciate in the long run and hold value better than more inflationary alternatives.

Is there a possibility of a return to the gold standard? Politically, democratically and intellectually, no. Modern political institutions, academia, media, and public opinion are largely shaped by Keynesians and statists. The monetary role of gold is viewed with scorn and disdain among the vast majority of the educated and influential members of society. There are simply too many Kenneth Rogoffs, Paul Krugmans, and David Graebers selling people the delusion that government control of money and banking is an improvement over having the free market select the hardest money. Those people will never believe in gold, and will continue to shape public opinion and political power toward centralization and political control and monopolies over money. The corporate interests that benefit from easy money are far too strong to imagine any kind of monetary reform emerging from the political process.

VI. Failure on the free market

While bitcoin is indeed free market money, it does not necessarily follow that bitcoin would succeed on a free market for money. The longer I think of this, the more I begin to consider the possibility that bitcoin is a free market solution to the problem of government control over money, but it is not necessarily the money that would be chosen on a market free of government control. For as long as governments place restrictions on money, bitcoin can thrive as a method of going around them, but if these restrictions are eased, that might deprive bitcoin of the oxygen it needs, demand for going around monetary restrictions.

Bitcoin is a technology built and optimized for one design consideration: resisting government capture, and nothing else. Bitcoin is not optimized for user experience, convenience, or speed of use; it sacrifices all these considerations to achieve immutability and resistance to censorship. This is extremely valuable in a world in which governments restrict individuals' monetary freedom, but how valuable is it in a world in which they do not?

The problem of bitcoin adoption is different from the adoption of any other technology or applica-

tion in that bitcoin's adoption involves decisions about liquidity and cash balances. People cannot just wake up one morning and decide to only deal with bitcoin, they have obligations to pay or be paid in different currencies, and they have savings accumulated in different currencies. They want to maximize their chances of being able to pay the money that their sellers want in exchange for their goods, and to be paid the money that buyers want to pay them. An individual's choice of medium of exchange is primarily determined by the differing liquidity pools around them, or the different degrees of salability for different moneys, as explained by Menger and discussed in more detail in The Bitcoin Standard. An individual's choice of money is likely to be the money that has the largest pool of liquidity, allowing the individual the largest number of trading opportunities, and providing them the best chance of exchanging their goods with the least loss of value.

Salability is also a self-reinforcing trend, as was illustrated by gold and silver in the nineteenth century, and also explained in The Bitcoin Standard. A money with larger salability will be likely to be more attractive as a store of value than a money with less salability, and that in turn will lead to the more salable money becoming even more salable, while the less salable money continues to lose its salability. Consider for a moment the possibility that bitcoin does indeed succeed in destroying government fiat currencies through speculative attacks, in a manner similar to the second scenario discussed above. Or consider the possibility that governments move toward freer banking and a competitive monetary system, without moving to a gold standard, but by allowing individual enterprise to provide consumers with a wide variety of choices in their monetary medium. In other words, imagine a completely free market in the choice of money, and try to imagine the consequences it would have for bitcoin.

In such a free market, individuals will choose the money which they find to be the most saleable, and most likely to be exchanged for other goods and services. As it stands, the total value of over-ground mined gold, or the global liquidity pool of gold, is around 100 times larger than the total value of mined bitcoin, or the global liquidity pool of bitcoin. This is a natural outcome of gold's huge 6,000-year first-mover-advantage over bitcoin. Gold has been produced all over the world for millennia and is an indelible part of all human cultures that have viewed it as precious. Today it continues to be held by central banks, but also, is widely used as a store of value and medium of exchange all over the world. Gold is still the dowry necessary to get married all over the world. The majority of humans own some gold, either in the form of coins, bars, or jewelry. In a situation in which alternatives collapse, people are far more likely to go back to trading in gold because of the properties that gave it its monetary role in the first place, but more importantly perhaps, because of the very large pool of liquidity that has been accumulating over thousands of years.

The implication of this is that for the average individual who wants to sell a good or service in a

post-fiat world the likelihood that their counterparty will have gold to pay is roughly 100 times the likelihood that they would have bitcoin to pay. That makes each individual far more likely to want to accept gold as money than bitcoin, and that, in turn reinforces the same trend with all other individuals. As it stands, a free market in money is not likely to be beneficial to bitcoin, because in the one metric that matters most, liquidity, bitcoin is incomparable to gold. Bitcoin needs government controls and restrictions to drive demand for it. The freer the global market for money, the more likely that any monetary competition will lead to gold winning in a winner-take-all scenario similar to how the nineteenth century competition between gold and silver unfolded. For bitcoin to have a chance, it needs government laws and restrictions to continue to drive people to look for hard money alternatives, thus increasing its value and the size of its pool of liquidity.

Beyond liquidity, and when it comes to issues of ease of use, many bitcoin promoters seem a little too enthusiastic in their assumptions on the ease of using bitcoin, and how willing people are to learn them. While I entirely agree that these technical barriers will be overcome by people who need to get around government restrictions, I am not sure there is a strong enough motivation to learn them in a world where these restrictions don't exist and people can default to using gold in all its tried and tested familiarity.

The non-digital nature of gold, and its physical heft and high cost of transfer compared to bitcoin are not serious obstacles for gold regaining a monetary role on a free market, they are only obstacles to the extent that they allow governments to prevent a global banking system to emerge around gold. In a free market, there is no reason that the most advanced payment technology implemented over fiat money or bitcoin could be used on top of gold. Instant digital payments with very few settlement transactions in physical gold are pretty straightforward to build from an engineering perspective, the real barrier to their development has always been political. In a world in which government restrictions on money disappear, the development of a gold-based financial infrastructure is likely to be faster and more advanced than a bitcoin-based financial infrastructure, because of the larger liquidity of gold attracting more development and investment.

Ironically, it appears that bitcoin is dependent on the governments it was built to counter for its survival. A world without government abuse of money is a world in which bitcoin is superfluous, and monetary tradition and history will likely move us back to a gold-based monetary standard. For bitcoin to continue to succeed and grow, it requires governments to continue to follow bad monetary policies that drive people to hold more bitcoin, raising its price, increasing the pool of liquidity, making it more likely for others to join this pool of liquidity. The longer that bad government monetary policy continues, the more liquidity bitcoin is likely to amass, the closer it gets to gold's liquidity, and the better its chances of unseating gold as humanity's prime money in a free market. The more govern-

ments reform their monetary policies and allow their citizens financial freedom, the less demand there is for bitcoin, and the less likely bitcoin's network is to grow.

VII. So, how do you REALLY kill bitcoin?

Based on the discussion above, it is my belief that bitcoin's health is largely (but not always) an inverse function of the quality of the monetary and financial policies of the world's governments and central banks. We could divide government monetary policies into six different scenarios, and assess their impact on bitcoin:

1- Monetary policies worsen
2- Monetary policy continues as usual
3- Improvements in monetary policy
4- A government bitcoin standard
5- A government gold standard
6- A free market in money

For Case 1, imagine a world with 10 more Venezuelas and a growing number of people in desperate need for a hard money. Demand for bitcoin would rise, and its liquidity would continue to increase, potentially rivalling gold. This scenario would likely witness many hyperinflations and currency wars, and the longer it continues, the more liquidity bitcoin amasses and the more likely it is to emerge as money in the future. The worse the monetary policy is, however, the faster these collapses happen, and the less likely bitcoin's liquidity will grow to a level allowing it to compete with gold in the future.

Case 2 would be the continuation of the current state of affairs with mildly inflationary monetary policy in most countries, and a few basket cases of hyperinflation and high inflation around the world. In this scenario, demand for bitcoin continues to grow gradually and we would be likely to experience the 'smooth upgrade' scenario for bitcoin adoption discussed above.

Should monetary policy improve, as in Case 3, one would expect demand for bitcoin to subside, and though it may survive, it will likely continue as a small niche technology whose main value is in providing citizens with a chance to escape their governments' worst monetary policies, which in turn likely puts a limit on how bad government policies become, which in turn slows down bitcoin growth an adoption.

Should governments adopt bitcoin as their monetary standard, that would likely increase bitcoin's liquidity enormously, and likely make it the dominant form of money in the world, but do not count on this happening any time soon.

In case 5, a further improvement in monetary policy through the adoption of a gold standard, would

likely be the most effective government weapon to fight bitcoin, allowing governments to stifle its growth while maintaining some control over the financial and monetary systems.

Finally, in case 6, a completely free market in money, or the absence of monetary policy, is the best monetary policy possible, and in that case, bitcoin would arguably lose its raison d'etre, and unless it had built up a very large liquidity pool by then, it will likely fail to dislodge gold as the world's prime money.

Bitcoin's survival and success is more likely in the scenarios in which the world's central banks' policies are similar to those that have prevailed over the past few decades, not much worse or better. Improvements in central banks' monetary policies, lower inflation and fewer business cycles would likely reduce demand for bitcoin. A severe worsening of monetary policy which would lead to more widespread collapse of national currencies could also jeopardize bitcoin if it results in more free market competition between monetary alternatives without government intervention, at a time when bitcoin still has very little global liquidity. The good news for bitcoin is that the most likely courses of action for governments for the foreseeable future are in its favor. The bad news for bitcoin is that by being built to resist government control, it is inevitably and inextricably affected by how governments behave, and might in fact be reliant on their monetary policies not improving or deteriorating too much for its survival.

Thank you very much for subscribing to ***The Bitcoin Standard Research Bulletin***.

Please feel free to share this bulletin with any friends you would think might be interested in subscribing to this newsletter, and also, to share excerpts or screenshots from the text on social media.

All the best,
Saifedean Ammous

To subscribe: **www.patreon.com/saifedean**.
Or email **thebitcoinstandard@gmail.com** for instructions on how to subscribe through bitcoin or paypal.