CHAPTER FOUR

Censorship Resistance

CRYPTO CONSENSUS VIEW	UNBOUNDED CAPITAL VIEW
Censorship resistance is an essential property of Bitcoin and other blockchains.	Censorship resistance as it is commonly understood is a liability that makes Bitcoin less useful.

Like trustlessness, censorship resistance is thought to be an essential quality of Bitcoin and other blockchains by the crypto consensus. While the degree to which censorship resistance is necessary or attainable differs within the crypto consensus, it is seen as a positive quality worth maximizing within the constraints posed by other goals in a platform. In our view, censorship resistance as it is commonly understood equates to extralegal status for blockchain based activity. We do not see this as a valuable quality.

Although we agree that there are benefits to users from censorship resistance outside of extralegal status, we think these are more likely to be achieved by a version of Bitcoin that scales, BSV, rather than blockchains that sacrifice efficiency to try and achieve censorship resistance or extralegal status through code. To us, that goal is the inheritance of some of Bitcoin's early adopters who sought to use it as a replacement for E-Gold, a failed cryptocurrency that was widely used for illicit purposes.

WHAT IS CENSORSHIP RESISTANCE?

In the same way trustlessness uses the word trust, the narrative around censorship resistance derives a lot of momentum through use of the word censorship. Censorship is widely considered to be bad, and resisting it is therefore good. But in the context of Bitcoin, what does censorship actually look like? What is it specifically that the crypto consensus wants to resist?

Censorship resistance – the ability for anyone to use Bitcoin without being denied service – can really be divided into two categories: censorship by miners and censorship from governments. This censorship can come in two forms: rejecting transactions and changing the contents of the database. Rejecting transactions is equivalent to a denial of service. For example, if a government issued a freezing order on certain funds, the miners would reject transactions attempting to spend these funds. If a single miner included a transaction containing these in a block, the other miners would reject that block.

The second form of censorship, changing the database, is more potent. Changing the database in a way that follows the rules of Bitcoin is extremely difficult and expensive. We will discuss this more in the next chapter. However, changes can be made that don't follow the rules to meet the goals of a miner or government. For example, if a government wanted to reassign stolen funds, they could add an invalid transaction to the database that miners could then treat as valid. In a sense, this would be extending the rules to accommodate law.

These forms of censorship could be used to make Bitcoin far less valuable. If miners routinely denied service or appended invalid transactions that stole people's balances, Bitcoin would quickly become useless. What is relevant, however, is not what can be done but what would be done, and that is a function of economic incentives. If these mechanisms are available to miners and governments, how would they be used? Would they be used in manners that help or hurt Bitcoin? In our view, this is the important question, and our belief is that, in practice, these forms of censorship would be used to Bitcoin's benefit.

CENSORSHIP IN PRACTICE

It is our view that miners have very little ability or incentive to censor specific individuals or entities. We will expand on this in Chapter 6. However, it is worth highlighting a form

of censorship being practiced by miners which is non-specific to any particular individual but instead censors harmful transactions that hurt the value of Bitcoin as a network.

In BSV, valid transactions are currently being censored through the "first seen rule." Consider that a signed transaction has two states: already included in the Bitcoin ledger and not yet included in the Bitcoin ledger. Before a signed transaction is included in Bitcoin, another signed transaction could be generated spending the same coins. The original Bitcoin protocol used inclusion in the ledger as a way to make sure coins weren't spent twice, but there was no clear way of distinguishing which transaction not yet included in the ledger would ultimately be included. This posed an issue to users who wanted to spend money as soon as they received it, or at least be sure that a signed transaction sent to miners was as good as cash in the bank.

Miners created a solution through transaction censorship. They only accept the first transaction they see which spent those coins. If I pay you BSV and then try to send it back to myself, the miners reject that second transaction assuming it is received second. If a block is mined which includes that second transaction, the block will be rejected, meaning that miners do not include the second transaction. This is a form of censorship which enables a key feature: zero-confirmation transactions. In BTC, this rule is not present. This means that waiting for ledger confirmations, preferably more than one, is best practice. This results in confirmation in seconds on BSV and industry best-practice confirmation times of 60 minutes or more on BTC. Because this form of censorship improves the performance of the system by denying what is likely either an accident or a crime, it is hard to make the case that censorship resistance is always good.

One may argue that this isn't censorship but is instead a new rule. That is a reasonable way of describing it, but it's a distinction without a difference. Bitcoin comes with a certain ruleset, but nothing about those rules prohibits miners from rejecting transactions they feel are not in their best interest to mine into blocks. In creating the first-seen rule, miners are in a way 51% attacking the network. They form a majority coalition to enforce rules not native to Bitcoin. This works because the miners are incentivized to make Bitcoin valuable. Censoring these transactions makes Bitcoin more valuable, so the miners do it.

It is interesting to note why this feature is not present on BTC. Because block sizes are limited on BTC to increase decentralization, there is often a long line of transactions waiting to be included in a block. Paying higher fees lets a transaction move up in line. Now, what if someone sends a transaction at the going fee rate and then traffic spikes?

At this point, their transaction may not go through for hours or days. The workaround is that they can create a new transaction spending the same coins for a higher fee. This destroys the ability to trust that transactions not included in a block won't be spent twice, but what's waiting a few hours or days in the name of decentralization?

TO EMBRACE LAW OR NOT TO EMBRACE LAW

Censorship resistance can certainly have value. Most would argue, for example, that censorship resistance is good in the sense that free speech is good. If political dissidents were prevented from using Bitcoin the way they can be prevented from using a system like PayPal, this would be an undesirable quality of Bitcoin to many, Unbounded Capital included. What is meant by censorship resistance to many, however, is the ability to operate outside of **all** laws.

Bitcoin can be an extremely private system. Transactions are pseudonymous, and massive scale makes tracing extremely expensive. In BTC, expensive transactions lead users to adopt an account model where payments go from one address to another. With the cheap transactions common on BSV, payments can operate on a many to many basis. If I am sending $10, I can send that in 1000 cent sized transactions to 1000 individual addresses. At 2022's fees this added privacy would cost me around ten cents, about 15 times less than it would cost me to send a single BTC transaction. These techniques make tracing and censorship by profit-seeking miners extremely unlikely since identifying possible targets of censorship would be so costly. Governments, however, are more likely to bear a high cost when they are highly motivated to track criminals or other individuals and organizations. Further, governments can force users to hand over information through existing offline legal means. For these and a host of other reasons, censorship is most likely to come from governments. Because these government actions have significant costs, Bitcoin isn't likely to be used to track petty crimes. This tracking capability is likely to be reserved for large criminal organizations and make Bitcoin far less useful to them.

While there can be costs to users from government censorship, there can also be significant benefits. It is disturbing to think of peaceful dissidents having their funds frozen, but it is comforting knowing that stolen funds can also be frozen and ultimately reassigned. Non-seizable assets are also non-recoverable assets. It is possible to have funds reassigned on Bitcoin, although it would likely require a highly expensive international

court order. This requirement would prohibit virtually all countries from oppressing their own people through censorship of Bitcoin transactions. However, it would permit countries working together to stop major crimes and coordinate to reassign stolen or lost funds. Bitcoin at scale both creates privacy that prohibits mass surveillance and makes auditing systems and proving lawfulness far easier.

With law as a security layer, the incentive to steal Bitcoin is very low because it can be easily tracked if the starting point is known as it would be by the victim of theft. In particular, large honeypots like exchanges and custodians could rest assured with the knowledge that theft or human error could be corrected. Further, by embracing law at the protocol level, BSV businesses and businesses building upon scalable blockchains such as BSV adopt a mindset of compliance. This is far less common on other protocols. Many were funded through illegal security sales in the form of ICOs, and the feeling that decentralization places one outside of the domain of individual jurisdictions has created an attitude about compliance which makes adoption difficult for individuals and enterprises for whom compliance is a must.

STATE-FREE, NON-SEIZABLE, DIGITAL GOLD

Much of the popularity and market cap of BTC comes from its perception as a useful inflation hedge. It is argued that its digital scarcity makes BTC valuable as a store of value, a role which should be accompanied by a sizable market cap. However, it isn't typically made very clear why non-confiscability is necessary for Bitcoin to serve this function.

Multicoin Capital describes the opportunity for state-free money in their Mega Crypto Theses:

> *Because fiat money is bound by trust in human institutions rather than physics, we have to place immense trust in the human institutions that govern money.*
>
> *There is a massive opportunity for a trust-minimized money. A natively digital, bearer asset bound by physics, math, and free-market economics rather than human institutions. That money will be the global, state-free measure of value, i.e. money.*

Another way of saying this could be that it's good to have forms of money that governments can't inflate. It doesn't follow that censorship resistance as commonly understood is also necessary. However, it is clear from Multicoin Capital and the crypto consensus'

bodies of work that non-seizability is a priority for stores of value. Why can't digital gold be confiscatable and valuable? Which is better for storing value – a seizable, recoverable asset or a non-seizable, non-recoverable asset? The latter is a much better target for theft, and presents much greater risks if mistakes are made during transfers. At Unbounded Capital, we think Bitcoin could be used as a store of value, but that a censorship resistant, non-seizable version is much less likely to serve this function long term.

DECENTRALIZATION AND CENSORSHIP RESISTANCE

Many of the decisions made in Bitcoin and the broader cryptocurrency space to this point are hard to understand without realizing that the primary motivation behind them is to maximize the chance that these networks can operate outside of the scope of **all** laws. The importance of this framing becomes more clear when we understand the extralegal use cases imagined and designed by some of Bitcoin's early adopters. Once the importance of functioning in an extralegal context is established, we can better understand the cryptocurrency consensus' acceptance of inefficiency and their assumption that code is a necessary and desirable substitute for law.

BITCOIN EARLY ADOPTERS AND USE CASES

It's possible that many of Bitcoin's earliest adopters were users of failed predecessors like E-Gold. E-Gold was a gold-backed online cash that launched in the late 1990s and grew to over one million accounts by 2004. Anyone with an email could register an E-Gold account. The required personal information could be easily faked. Regardless of the intentions of E-Gold's founder, who claims to have earnestly started E-Gold as a legitimate operation, the anonymity provided by the service made it a popular online currency and make-shift bank for criminals. E-Gold was particularly attractive to operators of credit card scams, money launderers, and illegal pornographers whose black market operations needed a way to easily move money internationally without the risk of exposing their identities. E-Gold's popularity among criminals eventually attracted the attention of governments and ultimately led to its demise. In 2007 E-Gold's founders were indicted for money laundering, conspiracy, and operating an unlicensed money transmitting business. In July 2008, three months before the release of the Bitcoin whitepaper, they pled guilty, and E-Gold was no more.

Given the coincidental timing of E-Gold's failure and Bitcoin's launch, it's likely that many early Bitcoin users were introduced to the technology in the context of its potential to replace E-Gold as extralegal money. As early as 2010, Bitcoin enthusiasts were on forums **troubleshooting how to best use Bitcoin in the creation of an online heroin store**. The next year, the online black marketplace *Silk Road* was launched and became one of the first popular commercial applications to use Bitcoin. On *Silk Road*, users bought and sold illicit goods with Bitcoin, demonstrating their belief that it was useful as extralegal money.

INEFFICIENCY AS A FEATURE, NOT A BUG

How was E-Gold shut down? Because the network was operated by a group of identifiable individuals, the government was able to easily apply pressure and cease operations. A reasonable theory for how to avoid this fate could be to remove the central point of failure that a database operator creates. Because Bitcoin was designed to create a database without reliance on any central party, it's understandable why ideologically motivated early adopters understood it as an improved and more robust form of extralegal money relative to E-Gold.

However, Bitcoin's future success posed a dilemma. As users of the network, Bitcoin's early adopters wanted it to succeed and become a widely used online money, since its utility would grow with each new user. However, too much success would be accompanied by economies of scale leading to Bitcoin mining being done in large data centers. The scale of these data centers would make Bitcoin's operators as easily identifiable as E-Gold's, and thus offer no robustness in the event that Bitcoin was abetting the evasion of law. Thus, if Bitcoin was intended to be E-Gold 2.0 it needed to be successful, but not too successful. This required trade offs which were eventually made by BTC, like limiting the computational growth of the blockchain and removing its smart contracting functionality. In removing these features, BTC's developers forced network operators to keep Bitcoin computationally small, decentralized, and thus inefficient. Influential BTC thought leaders like Nick Szabo, who had spent the 1990s and early 2000s thinking publicly about how to remedy the weaknesses of centralization experienced by E-Gold, have gone as far as suggesting that inefficiency is a key feature of Bitcoin. In a **Multicoin Capital blog post** they support Szabo's suggestion, writing

> *"Nick Szabo frames trustlessness as an inverse function of technical efficiency. Basically, the less efficient the computer, the more difficult it is to manipulate. The more*

difficult it is to manipulate, the more you can trust it, therefore making it trustless. In other words, to paraphrase Szabo, blockchains trade technical efficiency for social scalability."

Because of this perspective, it was the goal of BTC developers who desired the creation of E-Gold 2.0 to make Bitcoin as inefficient as possible. In this they succeeded. The logic required to end up at this backwards conclusion only makes sense under the assumption that Bitcoin's utility as an extralegal tool is paramount.

CODE AS LAW

A necessary logical conclusion of assuming that BTC's value depends on its usefulness as an extralegal money is that law cannot be a part of any system that interacts with it. This sounds obvious and largely desirable for individuals who are exchanging illegal goods online, but without law present, the ability to enforce contracts is made more difficult. What's to stop someone from sending you subpar drugs after receiving payment in anonymous and non-reversible BTC as E-Gold 2.0? In physical black markets, contracts are often enforced through the threat of violence. In an anonymous online black market, physical violence isn't an option. To remedy this, the developers of online black markets like *Silk Road* concluded that code must replace law. If the drugs aren't delivered as described, sellers could be punished through reputational violence rather than physical violence. More technically complicated systems of escrow were theorized to guarantee the ability to exchange with BTC "trustlessly." While the assumption that code is law in the context of online blackmarket activity makes some sense, why are users extending this assumption to virtually all of today's legitimate cryptocurrency projects which operate in a context where legal recourse is available if someone defrauds you?

Unfortunately for many cryptocurrency investors' sensemaking, the framing of what one might desire for Bitcoin in a black market context stuck, and has since extended to the legitimate cryptocurrency and blockchain ecosystem. As a result, inefficient solutions to solving trustlessness have become a necessity with the economic incentives from law removed. Law has become understood as something that is either undesirable or ineffective in regulating cryptocurrency. In the context of legitimate goods and services, the desire to remove law simply doesn't make sense. If one is acting within the law, there is no reason one would not be able to leverage legal remedies if one was robbed. Importantly,

if the assumption that one *cannot* and *should not* have access to legal recourse is baked into the majority of projects using blockchain technology, the resources dedicated to their development will be inefficiently allocated to try and solve an invented risk that logically would only apply to a black market context.

One such example of misallocated resources that presupposed code replacing law is the decentralized platform **Augur**. *Augur* is a decentralized prediction market and was an early success story of DApps. A key innovation of *Augur* was the ability to trustlessly serve as a decentralized oracle which could translate off-chain reality into on-chain outcomes. Imagine you want to place a sports bet in a trustless and decentralized context. How can you know if the Chicago Bulls won or lost last night's game in order to determine the outcome of the bet? If building a betting application in the context of law you would simply appoint a trusted oracle who would relay the information after it happens. An easy solution would be Google or a large institution without incentive to lie. If in reality the Bulls win but Google misreports the outcome claiming that the Bulls lost, defrauded gamblers would be able to hold Google accountable through law. In the code as law context of the cryptocurrency consensus which informed *Augur's* design, the use of law as a backstop is not possible. As a result, *Augur* has invested extensive time and capital resources into designing a network with perfectly calibrated incentives such that the platform can determine the factual conclusion without needing to rely on any one individual.

The problem with this, of course, is that balancing the incentives through code such that the system is perfectly free from error is virtually impossible. In 2019, *Augur* was experiencing significant problems with **scammers using the platform to create misleading and invalid markets as a means of stealing user funds**. The reality is that without consequences from law acting as a disincentive, scammers will inevitably find loopholes to exploit and rob users. Writing the perfect code is not a realistic expectation, and pouring resources into attempting it is a waste when extremely simple and effective solutions currently exist under the protection of law.

BTC AS E-GOLD 2.0

The parallels between E-Gold Founder Doug Jackson's vision for E-Gold and the current state-free money/digital gold vision for BTC are striking. **As described in a Wired exposé** written in 2009, one year after Jackson's guilty plea,

"Jackson envisioned (E-Gold as a) private, international currency that would circulate independent of government controls, and stand impervious to the (stock) market's highs and lows. Brimming with evangelical enthusiasm, Jackson proclaimed (E-Gold) a cure for the modern monetary system's ills and described it at one point as 'an epochal change in human destiny' and 'probably the greatest benefit to humanity that's ever been thought of.'"

Compare this to **one of Multicoin Capital's three crypto mega theses** on "Global State-Free Money."

"There is a massive opportunity for a trust-minimized money. A natively digital, bearer asset bound by physics, math, and free-market economics rather than human institutions. That money will be the global, state-free measure of value, i.e. money. The simplest way to think about the opportunity for a global, state-free money is digital gold....The transition from a trust-based economy to one of self-sovereignty will be behind one of the largest wealth transfers in human history."

Multicoin Capital goes on to claim that global state-free money like BTC is "seizure free," like "a Swiss bank account in your head," and imagines it addressing a market as large as $100 trillion.

The demise of E-Gold was preordained by its success and usefulness in evading the laws of powerful governments like the United States. If extralegal status is a key value proposition of BTC as the cryptocurrency consensus claims, how will powerful governments respond to its success? Because E-Gold was technically centralized on servers operated by its founders, it was relatively easily shut down once its illegality was identified. The ideologically motivated developers in charge of BTC appear to be betting that decentralization can save them from E-Gold's fate. Even if ideologically motivated protocol developers are able to avoid this outcome for the underlying BTC network, for most, it's unlikely that the costs paid in crippling BTC's efficiency and removing the safeguards of law will make the benefit worthwhile. Besides criminals using BTC as state-free digital gold, the cost/benefit analysis of limiting Bitcoin's usefulness doesn't make sense. For all legitimate use cases of Bitcoin, the removal of law in favor of decentralization and rule by code-as-law has dramatically reduced the network's utility rather than increased it.