

it through violence. As a typical example in the past 5,000 years, a country or tribe would typically bomb the embassy or stronghold of another country or tribe and just take the gold and other assets the country was holding. Even in the electronic age, where the physical forms of money are disappearing in favor of numbers on a screen, those who control those numbers are in the power position. The Russian government learned this lesson the hard way in 2022, when the US notified them that they would be freezing them out of the SWIFT system and seizing their reserves, amounting to \$300b. The mechanics of the freeze were such that the reserves were not backed by any real money and were just ledger entries that the US and EU essentially deleted. It begins to make sense why Russia responded by working with the BRICS countries, who all viewed the seizure as a wake-up call, to stockpile gold and other hard assets to back a new currency. Additionally, Russia announced that they would accept bitcoin from friendly countries in exchange for its oil, while requiring rubles from unfriendly countries. It is not known whether anyone has taken them up on this offer, but the announcement itself speaks to the preferences of nations beginning to slowly move towards one where bitcoin is a part of it. Bitcoin is said to be the “money of enemies” because it doesn’t require trust, and after capriciously seizing so much money from Russia, we are likely moving into a world that will operate on far less trust than exists today.

When held in self-custody, bitcoin cannot be seized or taken if the holder refuses to give their private keys. Yes, it's possible for someone to compel a certain level of violence against an individual to coerce them into handing over their private keys, but the holder can also refuse and let his coins just be burned and unspendable forever. Prior to bitcoin, nobody had the option to refuse. They could be killed, and then have the attacker just take their property. Bitcoin uniquely resists confiscation at a personal level, and that extends to an institutional level, and ultimately a nation-state level. This can immediately be seen as valuable to countries like Russia and China, but even more so to bitcoin accumulators like El Salvador and Bhutan. It is a different game on planet Earth when your wealth can be stored in a form that cannot simply be taken by violence or coercion. Potential refugees can travel and cross borders with trillions of dollars associated with their secret words that they hold in their minds.

Once again, the losers of this innovation are the most powerful projectors of power in the current world order. The US has built a lot of wealth through seizures. Ironically, the majority of the wealth seized by the US has been in the form of bitcoin. While that might contradict the notion of this section, the bitcoin was taken in many cases from parties who did not hold the keys in self-custody. The US government was able to go to the exchange and compel them to hand over the private keys at the threat of prosecution. As an example, the government seized approximately 100,000 bitcoin from the Silk Road prosecution. Of these, 30,000

were from Ross Ulbricht (the creator), and another 70,000 were from funds that were stolen from other Silk Road participants. All in, in today's value, it's a \$10 billion seizure. The US seized another 100,000 coins from culprits who hacked the Bitfinex exchange in 2016. Another \$10B for its reserves. By contrast, the US government only recovered around \$4 billion from Bernie Madoff, just under \$2 billion from the 1MDB (Malaysian Development Berhad) scandal, and less than a billion from Pablo Escobar.

This is to say that the ability to resist confiscation is already causing high demand for bitcoin, and will only continue to do so as technologies for self-custodying bitcoin become easier, more robust, and more intuitive. This is a big reason why people hold their bitcoin even through the previously aforementioned massive drawdowns. Bitcoin is unique in that it can't be taken unless one allows it to. Once you convert it to dollars, it becomes fully seizable and censorable all over again. Five to ten years ago, it was extremely difficult to hold keys relative to today. It is very easy for individuals to custody their bitcoin in a non-confiscatable manner. It's a little more difficult right now for institutions, mainly due to security risks to those in the chain of custody.

This is rapidly improving with insurers like AnchorWatch developing custody solutions tailored for institutions, and in a few years, we'll be talking about how commonplace it is for institutions to be custodying their bitcoin. The power of keeping what you own is a basic human desire that wasn't