bitcoin's

Sound Money Properties Series

#4: Censorship Resistant & Unconfiscatable

with @SimplestBTCBook and @DJSATOSHI18

- ₿ PORTABLE, DURABLE, DIVISIBLE, FUNGIBLE
- ₿ TRULY SCARCE
- ₿ DISTRIBUTED & DECENTRALIZED
- ₿ CENSORSHIP RESISTANT & UNCONFISCATABLE
- ₿ IMMUTABLE & INCORRUPTIBLE
- ₿ EASILY VERIFIABLE & CAN'T BE COUNTERFEITED
- ₿ PERMISSIONLESS, FRICTIONLESS & PEER-TO-PEER
- ₿ NEUTRAL & VOLUNTARY
- ₿ TRANSPARENT, OPEN-SOURCE & AUDITABLE
- ₿ BORDERLESS
- ₿ PROVIDES SETTLEMENT FINALITY
- ₿ PSUEDONYMOUS & TRUSTLESS
- ₿ SECURE & SCALABLE
- ₿ DISINFLATIONARY/DEFLATIONARY

UNCONFISCATABLE

: that which cannot be confiscated, or taken without permission

CENSOR

: a person who supervises conduct and morals

: a magistrate in ancient Rome who was responsible for supervising public morality

RESIST

: to exert oneself so as to counteract or defeat

: to exert force in opposition

CENSORSHIP RESISTANCE

A property of a system that is designed to make blocking information from being read, heard, seen or processed difficult or costly.

~ Kiara Bickers, Author: Bitcoin Clarity

Why is

CENSORSHIP RESISTANCE

important as a property of truly sound money?

- In order for a truly free market to develop and to function, we need money that cannot be controlled or manipulated.

- We need money that people are able to spend freely amongst themselves, as they see fit, when they see fit.

- We are sovereign beings with the sovereign right to transact using sovereign money that no one, no government, no institution, no organization, no matter how large or small, no matter how powerful, can censor or stop.

There are a few different angles to bitcoin's censorship resistance:

- ₿ It cannot be censored at the protocol level by the developers without the agreement of the nodes.

- ₿ It cannot be censored by the government or anyone else. No one can tell you when or to whom you can send your bitcoin. No one can stop you from sending it.

- ₿ No one can stop the Bitcoin network from working to verify and validate your transactions.

It would require every single node and miner to go offline forever to stop bitcoin.

- A new attribute, which has become increasingly important in our modern, digital society with pervasive surveillance, is censorship resistance.
- That is, how difficult it is for an external party such as a corporation or state to prevent the owner of the good from keeping and using it.
- Goods that are censorship resistant are ideal for those living under regimes that are trying to enforce capital controls, or to outlaw various forms of peaceful trade.

~ Vijay Boyapati

Censorship-Resistant Transactions

The decentralized architecture of the bitcoin network means no single entity has the power to prevent a transaction from propagating through the network. As long as a transaction is considered valid, it will be accepted by nodes and eventually included in a block by miners. Additionally, the pseudonymous nature of bitcoin means it is difficult to link a transaction to any specific party when privacy-preserving best practices are used.

High-Value Settlement

Moving a billion dollars of value across the world, securely and in minutes, for a few dollars worth of fees is now possible via the Bitcoin network. This makes it a far more attractive method of settlement than traditional financial infrastructure for high-value transactions such as transfers between large corporations, governments and central banks.

From: Few Understand This: A Visual Guide to Bitcoin's Rise by @anilsaidso

- Bitcoin is censorship resistant in the sense that no single entity has the ability to reverse a Bitcoin transaction or blacklist a wallet or address. Any node can broadcast a transaction, and any miner can mine any transaction. Thus, censoring a Bitcoin transaction is virtually impossible.

- When a Bitcoin transaction is submitted to the network, it is relayed from node to node until it has reached most nodes. These nodes keep unconfirmed transactions in a database called the mempool, and miners gather transactions from the mempool to build the blocks they attempt to add to the chain. When a miner mines a block with a transaction in it, that transaction is removed from the mempool and is considered confirmed.

- This process has relatively few chokepoints. As long as an individual can reach a node on the Bitcoin network, they can broadcast a transaction and trust that it will be confirmed.

- In order to preempt the attempts of governments or other large organizations to censor transactions, Bitcoin developers have engineered many unique ways of broadcasting transactions, including over mesh networks, satellites, and HAM radio.

~ River Financial: Censorship Resistance

- A key feature of bitcoin is that you, as the owner of BTC, are in full control. You can take control of the private keys yourself, and not rely on anyone else in order to transact with your bitcoin.
- This is different than every other form of digital payment/money. Be it your bank account, paypal, venmo, credit cards, etc, there is always someone else authorizing transactions on your behalf.
- Not so with bitcoin. You can use your keys to submit transactions to the bitcoin network directly, and your transactions will be executed.

~ CaseBitcoin.com

- This full control capability also means no one can take your bitcoin from you without your permission.
- Again, unlike every other form of digital money and wealth storage, there is no one who can simply confiscate your bitcoin with the stroke of a pen or click of a button on some bank or government computer system somewhere.
- At the limit, seizing bitcoin from someone requires physically compelling them, which creates a much higher bar than a bank freezing an account, for example.

~ CaseBitcoin.com

₿ This marriage of digital and unseizable (or unconfiscatable) is one of the key things that makes bitcoin uniquely useful in our modern times. Gold that you're in physical possession of, and perhaps fine art, shares this property of not being easily seizable.

₿ But by being digital, bitcoin is far more practical to deal with. It is far easier and cheaper to store securely yourself, and the ability to move it anywhere on the planet instantly without having to physically carry anything makes it far superior chaos insurance.

~ CaseBitcoin.com

Thanks for listening!

Feedback always welcome!

Next week we will discuss the properties of
Immutability and Incorruptibiliy