bitcoin`s Sound Money Properties Series

#5: Immutable & Incorruptible

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

IMMUTABLE

1 : not capable of or susceptible to change

- merriamwebster.com

The history of the ledger is final and cannot be changed.

- Kiara Bickers, Author, Bitcoin Clarity

INCORRUPTIBLE

: incapable of corruption: such as

a : incapable of being bribed or morally corrupted

b : not subject to decay or dissolution

- merriamwebster.com

The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime.

- Satoshi Nakamoto

…we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power.

~ Satoshi Nakamoto

- .. our money has become highly mutable. Early forms of money maintained some degree of immutability because they were produced and stored in a decentralized manner.

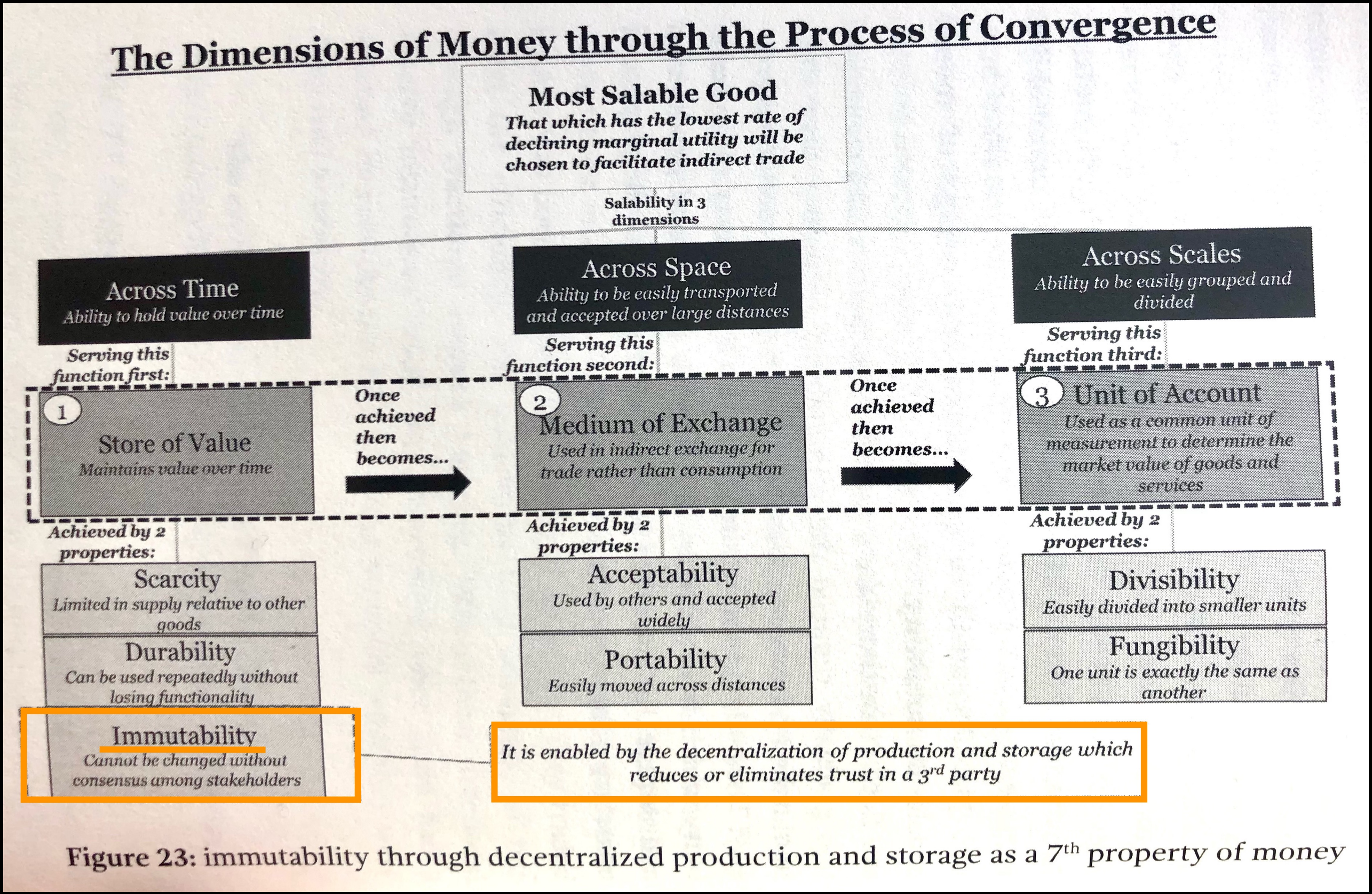
- The decentralized production and storage of money enables immutability.

- Recall that there are 6 monetary properties, and centralization gradually reduced the immutability of money over time.

- Immutability, however, is not characterized as a monetary property.

- Thus, ideal money should have a 7th property of immutability which is enabled by the decentralization of production and storage.

~ Eric Yakes, The 7th Property, pg 55



The Dimensions of Money through the Process of Convergence

Most Salable Good
That which has the lowest rate of declining marginal utility will be chosen to facilitate indirect trade

Salability in 3 dimensions

Across Time
Ability to hold value over time

Across Space
Ability to be easily transported and accepted over large distances

Across Scales
Ability to be easily grouped and divided

Serving this function first:

1 Store of Value
Maintains value over time

Once achieved then becomes...

Serving this function second:

2 Medium of Exchange
Used in indirect exchange for trade rather than consumption

Once achieved then becomes...

Serving this function third:

3 Unit of Account
Used as a common unit of measurement to determine the market value of goods and services

Achieved by 2 properties:

Scarcity
Limited in supply relative to other goods

Durability
Can be used repeatedly without losing functionality

Achieved by 2 properties:

Acceptability
Used by others and accepted widely

Portability
Easily moved across distances

Achieved by 2 properties:

Divisibility
Easily divided into smaller units

Fungibility
One unit is exactly the same as another

Immutability
Cannot be changed without consensus among stakeholders

It is enabled by the decentralization of production and storage which reduces or eliminates trust in a 3rd party

Figure 23: immutability through decentralized production and storage as a 7th property of money

From: The 7th Property: Bitcoin & the Monetary Revolution by Eric Yakes, pg 56

IMMUTABLE

- Bitcoin maintains a high level of immutability on two levels.

- Firstly, Bitcoin's consensus protocol is resistant to change, and the core aspects of the protocol, most importantly Bitcoin's strict monetary policy, can never be changed.

- This immutability is enforced by the tens of thousands of Bitcoin nodes who independently run the same code and agree to the same ruleset.

- No single party, neither miners, nor governments, is able to change Bitcoin's consensus rules without convincing these tens of thousands of nodes to agree to their proposed changes.

~ River.com, Immutability

- Secondly, Bitcoin’s blockchain is immutable in the sense that its history cannot be easily rewritten.

- This allows merchants to trust Bitcoin payments more easily than fiat payments.

- Bitcoin’s blockchain is append-only, meaning that once a block is embedded in the chain, it is practically infeasible to remove or alter it. This makes Bitcoin’s history immutable.

- This property is enforced by the SHA-256 hash function. When a miner hashes a block hoping to find a valid hash, the hash of the previous block is included in that block.

- Thanks to the properties of a hash function, if the hash of the previous block changes, this will change the current block’s hash, invalidating the Proof-of-Work and thus the entire block.

~ River.com, Immutability

- For example, if the blockchain has 500 blocks, Block #400’s hash will include Block #399’s hash. If a single piece of Block #399 is altered, Block #399’s hash will change, causing Block #400’s hash to change and so on, all the way until Block #500. Every block after #399 will be invalidated.
- This trait prevents anyone from altering a block once it is part of the blockchain without completely rebuilding the blockchain.
- Bitcoin’s immutability is neither absolute nor unassailable. If an attacker were to control a majority of all computing power on the bitcoin network, they could alter past blocks in what is called a 51% attack.
- It is imperative that Bitcoin maintain a significant and decentralized hash rate in order to keep the cost of such an attack beyond the means of any entity.

~ River.com, Immutability

This immutability is not a feature of the Bitcoin software, which is trivial to change for anyone with coding skills, but rather is grounded in the economics of the currency and network, and stems from the difficulty of getting every member of the network to adopt the same changes to the software.

Bitcoin's status quo can be understood as a stable Schelling Point, which provides a useful incentive for all participants to stick to it, while the move away from it will always involve a significant risk of loss.

~ Saifedean Ammous, Author 'The Bitcoin Standard'

From: Immutability: Bitcoin’s Superpower

by Aleksander Svetski

- To go ‘back in time’ and change one transaction on the Bitcoin Ledger, it would not only require you to accumulate enough mining equipment (capital cost), but it would also require you to expend enough energy (in the form of electrical power) to win the proof of work game, and validate the blocks from that point forward all the way through to today.

- This is not only financially insane, but almost practically impossible.

- It’s the cost of validating transactions and maintaining the network of distributed but consistent ledgers that gives .. Bitcoin its immutability.

- For someone to change something on this network in the past, it would cost billions.

- In fact, it would require something like 3 trillion (with a “T”) modern, high-end laptops worth of computing power just to change ONE transaction on Bitcoin.

- That is the definition of immutable.

- It’s this “Proof of Work” that brings the cost into Bitcoin and forms the basis of its game theory.

- Proof of work is the bridge between the digital and the real world, and the sunk cost of capital and work done is what makes it immutable.

- People hear words like “cryptography” or “encryption” or “hashing” together with terms such as “blockchain” and mistakenly assume that it’s somehow got something to do with immutability.

- They also hear that “mining uses lots of electricity” and “is bad for the environment” from those with an ineptitude to math, probability or game theory, and by not understanding the broader recipe at work here; they think that they can discard “that expensive proof of work” part, and keep the nice, fluffy, inexpensive software [blockchain] part.

From: Immutability: Bitcoin’s Superpower
by Aleksander Svetski

- But as we’ve established; there’s a problem with that line of thought.
- If there is no cost to change something; then we’re back where we started, i.e.; taking someone’s word that this is the way it is.
- Security and Immutability are functions of cost.
- Proof of work is the part that looped all the other elements together and helped us, for the first time in history; associate a real world cost to an ephemeral, fungible, digital object.

From: Immutability: Bitcoin’s Superpower
by Aleksander Svetski

- Furthermore; because proof of work is a compounding phenomenon; it only gets stronger and more immutable with time.

- This is at the core of why people say “Bitcoin is anti-fragile”. It benefits from the passage of time (lindy effect).

- Bitcoin is the first time we’ve had a digital good, that functions like something physical. And because it’s bound by math, it’s able to be verifiably scarce, whilst maintaining the scalability that only comes with something that is natively digital.

~ From: Immutability: Bitcoin’s Superpower by Aleksander Svetski

From: Immutability: Bitcoin’s Superpower
by Aleksander Svetski

#Bitcoin is a bank in cyberspace, run by incorruptible software, offering a global, affordable, simple, & secure savings account to billions of people that don’t have the option or desire to run their own hedge fund.

~ Michael Saylor

Its computational proof of the order of events is what makes it independently verifiable and irreversible.

~ Gigi

- Bitcoin is the most secure network, not because it has the best cryptography, but because it has the most accumulated computational proof.
- Cryptographic algorithms can be copied for free.
- Computational proof can not.

~ From: ‘The Other Side of the Coin -
Computational proof of the chronological order of transactions’ by derGigi

And because the computational proof is entangled with Bitcoin's ruleset and age,

and because you and you alone are responsible for enforcing said ruleset,

and because the threshold that defines the validity of said computational proof had to grow organically,

and because you can neither copy history nor electricity,

one can only arrive at one conclusion:

there is no second best.

~ From: 'The Other Side of the Coin - Computational proof of the chronological order of transactions' by derGigi

“Bitcoin is the first example of a new form of life. It lives and breathes on the internet. It lives because it can pay people to keep it alive. […] It can’t be changed. It can’t be argued with. It can’t be tampered with. It can’t be corrupted. It can’t be stopped. […] If nuclear war destroyed half of our planet, it would continue to live, uncorrupted. ”

- Ralph Merkle
Inventor of cryptographic hashing and Merkle Trees, used in Bitcoin

Thanks for listening!

Feedback always welcome!

Next week we will discuss the fact that bitcoin is easily

Verifiable and Cannot be Counterfeited.