H/Rindex :: The Hashing Power and Robustness Index

Computational Power-weighted Benchmark for Global Blockchain and Crypto Market

HUSAM ABBOUD

SÃO PAULO - OCTOBER, 2017

*Discussion Paper**

ABSTRACT: Cryptocurrencies have grown exponentially and gained increasing attention in recent years, and while it's true that it's secure by design, "Security" remains the cornerstone of any and all cryptoassets.

To benchmark the global cryptocurrencies market from a security perspective, track current and historical market performance we construct the H/Rindex; a crypto hashing-weighted average, computed from the prices of selected cryptocurrencies and weighted by hashing-power of the constituents, a tool to be used by participants of crypto market that wish to gain exposure, trade risk for profit and by observers who wish to describe the market and its security characteristics: 1) The Hindex "Hashingrate index" Crypto Computational Power Average: is a cryptocurrencies computational power weighted index and 2) The Rindex "Robustness index" Crypto Robustness Index: is a crypto- currencies robustness and 51% attack resistance-weighted Index.

Keywords: Hindex, Rindex, Blockchain, Market, Cryptocurrency, Hashing rate, Distributed Ledgers, Bitcoin, Ethereum, Crypto Index, Distributed Ledgers, Token, Initial Coin Offerings, Tokens, Crypto.

---

* Discussion Paper Revision 2018-02-21, enclosed Spreadsheet URL: https://goo.gl/ocYBUw

TABLE OF CONTENTS

1) INTRODUCTION

Benchmark indexes trace their history to the late 1800s, when Charles Dow, co-founder of Dow Jones & Co., created The Dow Jones Industrial Average as a way to gauge the general direction of the market, today it shows how the largest and most influential publicly owned companies in the U.S have been trading, In the traditional financial industry, indices play fundamental roles as benchmarks, and to compare the return on specific investments, like S&P500 Made up of 500 of the most widely traded stocks in the U.S., or Nikkei 225 comprised of Japan's top 225 blue-chip companies traded on the Tokyo Stock Exchange or FTSE for the 100 companies listed on the London Stock Exchange, etc.

Cryptocurrencies; “Crypto” has been recognized as a new asset class, and while there are already several attempts to create a Crypto Index(s), the weighting modalities that have been used have imported empirical models from the traditional financial market with arbitrary parameters to try to fit them to Crypto. So we have the capitalization-weighted[1] indexes such as CRIX, Bletchley, TaiFu30, Crypto30, LBI, Smith + Crown SCI, and capped capitalization-weighted such as CRYPTO20, CCX30, and BIT20, smoothed capitalization-weighted such as CCI30, and the cherry-picked ones like ICONOMI DAA(s).

In the crypto universe, it all boils down to one word “Security”. So many factors are important for cryptocurrency adoption and price market value from the cryptographic algorithm, system features (*total supply*, *speed*, *transaction cost*, *privacy*, *anonymity*) to functionality (*smart-contract*, *distributed applications*), which could all add or subtract value in accordance with participant perception. The market value “Value-In-Exchange” is not determined by any inherent property in particular, nor by the amount of labor necessary to produce but rather by the importance a participant -an acting individual- places on it for the achievement of desired ends.

However, out of all internal and external factors Security remains at the core with substantially greater value, if not the greatest.

---

[1] Capitalization-weighted (*or Marketcap-weighted*), is a modality of weighting the index constituent by its market capitalization, The Market Capitalization of Cryptocurrency is calculated as = total number of coins (*or tokens*) in circulation times the value of each coin

Arguably all other factors' relative values (*and subsequently the price*) will diminish to approach zero if a cryptocurrency security is being jeopardized for an extended period. That being said, measuring the system robustness and how it's secured against vulnerabilities such as the 'double spending attack' and others shall be the genesis block of any valuation framework.

And while it's true that cryptocurrencies have no particular intrinsic value in traditional definitions, the cryptocurrency dominant value is inherited from its network hashing power and the capacity of the nodes of that blockchain network to be secured against vulnerabilities

Definition 1. *The transvaluation of intrinsic value in crypto universe is the computational power of the decentralized network (often the hashrate)*

2) CRYPTO ROBUSTNESS - NETWORK SECURITY

Blockchain cryptoassets in general and cryptocurrencies in particular are secure by design, however, the question remains - how secure are they? And how would you measure it? And to do so we are going to discuss vulnerabilities and types of major attack vectors as factors for network robustness

a) Consensus 51% attacks resistance factor

The consensus mechanism is a vital feature of a blockchain as it ensures that the majority (*if not all participants*) of a distributed ledger are in agreement on the data being proposed to update the ledger and enable the network to keep functioning even if some of its members are failing.

Furthermore, this same consensus mechanism is vulnerable to attack by miners (*pools, or cartel*) If they control 51% or more[2] of hashing power, and they attempt to use their hashing power for destructive ends. They could prevent transactions from being confirmed, reverse recent transactions sent, cause double-spending transactions or execute denial-of-service attacks against specific transactions or addresses including other miners or pools.

[2] The 51% attack scenario doesn't actually require 51% of the hashing power. In fact, such an attack can be attempted with a smaller percentage, further 51% is only what makes it guaranteed to succeed, Security research groups have used statistical modeling to claim that various types of consensus attacks are possible with as little as 30% of the hashing power, - A. Antonopulos (2017)

Undoubtedly, such a consensus attack would erode confidence in cryptocurrencies in the short term, possibly causing a significant price decline, since the cost of such an attack is significantly high. We assume miners would be working in their best financial interest and a decline in price is no good when you can use your hashing power to actually find blocks. This argument might made sense during the time of Satoshi Nakamoto, - *and despite the fact that the attacker may not be motivated by profit*-, such an attack is actually financially beneficial and profitable in today's world with exchange increasingly allowing margin trading, short-selling, future contracts, and flexible order-fulfillment options. For example, the attacker could simply short-sell/put a crypto instrument across multiple major exchanges, and benefit substantially from a price decline.

Cost of 51% attack is a critical factor to be considered in our valuation: the higher the cost (*barrier to entry*), the safer and more robust the network is.

> **Definition 2:** The 51% attack cost is what would cost to produce (*or control*) 51% of total hashing power of a cryptocurrency network, and that can be calculated as acquisition cost of the hardware needed to generate the current hashing power + running cost of electricity.

First we identify the most efficient mining equipment for that cryptocurrency hashing algorithm, then how much hashing power that unit produces, and how many units we need to produce the 51% of hashing power of the network (*+ adding cost of electricity accordingly*)

> *ex. Antminer S9*[3] *is the most efficient ASIC miner for bitcoin today, each unit costs $1265 and offers a hashrate of 13 500 GH/s.*
>
> *Current bitcoin hashrate is 21,528,020,746.00 GH/s; It means that we need 1,594,668 Unites of Antminer S9 (21,528,020,746.00 / 13,500 = 1,594,668) to produce the current hashrate of the network, and that would cost $2,027,780,087.00 = 1,594,668 Unites * $1265 Price (about ~2 billions dollars) + ~$10mm electricity per day to run a 51% attack on bitcoin network*

[3] CryptoCompare S9 Antminer AISC (accessed 2017-10-24)

	Market Cap	% of Marketcap	Hashrate	Cost of 51% Attach
2018-02-24		*vs. Total Crypto*	*GH/s*	
Bitcoin	$167,352,524,294	38.53%	21,528,020,746.00	$2,027,780,087.45
Ethereum	$82,148,847,206	18.91%	239,444.00	$1,912,870,227.20
Bitcoin Cash	$20,459,062,503	4.71%	2,415,000,000.57	$227,475,111.16
Litecoin	$11,336,745,338	2.61%	141,383.00	$462,255,084.76
Dash	$4,700,852,343	1.08%	265,013.85	$616,496,413.08
Monero	$4,344,711,269	1.00%	1.00	$543,039,479.91
Ethereum Classic	$3,905,093,534	0.90%	12,631.00	$100,906,532.80
Zcash	$1,303,665,136	0.30%	0.53	$542,039,974.12

Table A1: Cost of 51% Attack across all major PoW cryptocurrencies

The selected crypto and sample data of our research here is limited to Proof-of-Work (PoW) hashing algorithm cryptocurrencies, further it can be easily extended to Proof-of-Stake (PoS) cryptos like Lisk, Waves and to any other crypto with a verifiable blockchain consensus mechanism, though other robustness factors (*and beside 51% attack cost*) have to come in play then as 51% attack by design is way more expensive in PoS -*and impractical*- than it's with PoW.

b) Cryptographic attack resistance factor

History has proven that cryptographic schemes can and will be broken, it's just a matter of time, and developments in quantum computing may play a big role in this in the future, multiple forms of cryptographic attack from preimage attack, to collision attack to all the effect of broken hashing primitives.

The good news is that there is always a possibility of shifting to a stronger algorithm, a protocol upgrade -and forking- to evolve the cryptographic schemes used whenever they get broken. This is as long as there are a community and core developers behind to react swiftly and dynamically, not only for pure cryptographic vulnerabilities but code general security flows.[4]

[4] Other forms of attacks to be explored and factored accordingly as Partitioning attacks, Routing Attacks, and Social engineering attacks, I. Giechaskiel; C. Cremers; K. B. Rasmussen (2016)

3) CRYPTO COMPUTATIONAL POWER

We will measure the computational power of a cryptocurrency network in comparison to another cryptocurrency and to the overall crypto. In order to construct a computational power average and hashing power-weighted index.

There are multiple forms and units used to measure the computational performance of a system, the first that comes to mind is using an already existing unit standard for measurement, like IPS (*Instructions per second*) mainly for processing speed or FLOPs (*floating point operations per second*); which is widely used in fields of scientific computations to measure and compare supercomputer systems. It would be so much easier if we could use an already existing unit to measure cryptocurrency network computational capacity, however Integer Operations (*the one used for hashing*) and Floating Point Operations are not comparable. There is no direct conversion between FLOPS and hashes because hashes involve integer operations (*whole number math*) and FLOPS involves obviously floating point math

> *Though, there was an attempt to approximate calculations and according to bitcoinCharts.com 1 Hash = ~12,700 FLOPs, note that 1 Hash of bitcoin hash function, Comparing computational power of Bitcoin ~8,000 PetaHash/s to Top500 supercomputers combined 748.4 PetaFLOP/s, the Bitcoin network is approximately 161 hundred-thousand times the computational power of the Top500 supercomputers combined*

The network hashrate for most cryptocurrencies are known and propagated figures, (*hashrate measures the number of times a hash function can be computed per second*). However, the hash function varies by network and therefore a direct comparison of hash rates across networks is not very relevant. Instead, it's possible to measure if we use an Adjustment Factor that enables us to compare a like-for-like metric.

Algorithm Hash Adjustment Factor is like you say ETHash of Ethereum is 80k slower (^80k more operations) than SHA-256 of Bitcoin, so If Bitcoin's global hashrate is currently 20,000,000 Terahash per second and Ethereum's network is 200 TH/s, using an adjustment factor the hashrate of 200 TH/s of Ethereum's network is equivalent to about 16,000,000 in Bitcoin hashrate, and Ethereum's network computational power is about 80% of Bitcoin network

ALGORITHM ADJUSTMENT FACTOR

While it is complex to calculate the Algorithm Adjustment Factor between two hashing algorithms with a high level of accuracy, It's quite simple to calculate and get a reasonably fair estimation, we propose the following methodologies A) Adjustment factor by Mining profitability and B) Adjustment factor by Implied Watts per GH/s

a) Adjustment factor by Mining profitability

By calculating how much hashpower a miner will need to employ in order to generate the equivalent of an arbitrary constant amount, like $100k USD of that cryptocurrency;

Example: 4,000,020 GH/s hashing power needed to generate 10 BTC equivalent to $100k USD in a month, compared to ~ 50 GH/s to generate 110ETH the equivalent of $100k.

4,000,020/50 ≈ 80,000 is the Algorithm Adjustment Factor to convert for comparison from ETHash to Bitcoin hashing algorithm SHA-256

$$Algorithm\ Adjustment\ Factor\ A1 = \frac{HashRate^{v}_{btc}}{HashRate^{v}_{crypto}} \qquad (E1)$$

Where ***v*** is a fixed value (*ex. $100k*), ***crypto*** *is the Cryptocurrency*, ***Hashrate*** *is the Cryptocurrency network hashrate* needed to be employed

To calculate Bitcoin Hashrate needed to generate equivalent of giving $\boldsymbol{v}$ value, in an attribute of the SHA-256 algorithm:

$$Hashrate_{btc}^{v} = \left(\frac{v}{btc_{price} \cdot sec}\right) \frac{d \cdot 2^{32}}{r} \qquad (E2)$$

Where ***Hashrate*** is the expected hashing power to be employed by a BTC miner, $\boldsymbol{btc_{price}}$ is current spot market price ($10,000 USD), $\boldsymbol{v}$ *is* fixed given value (*ex.* $100*k*)

The constant ***sec*** is number of seconds of the measurement period (*ex. 86,400 one day or 2,592,000 for one month*), ***d*** is the variable of network difficulty value (~ 3,017,500,000,000) and ***r*** the Block reward (*currently 12.5 btc per block*)

The constant 2^{32} relates to the normalized probability of a single hash per second solving a block

> Now let's put it all together $\left(\frac{\$100000}{\$10000 \cdot 2592000s}\right) \frac{3017500000000 \cdot 2^{32}}{12.5} \approx$ 4,000,020 GHs *Hashrate* needed for miner hardware running for one month to generate the BTC equivalent in value to $100k USD, *assuming that difficulty is constant during the test period.*

We can normalize the constants if we pegged the $\boldsymbol{v}$ value to fixed amount $100,000.00 and time to 1 month and for the mining algorithm, we can summarize the constants by $\mathbf{y}$, which would equal: $\mathbf{y}$ = 2^{32} * $100,000.00 / 2,592,000.00 second a month = 165,700,898.77 and the Equation (E2) can be rewritten as:

$$Hashrate_{btc}^{\$100k} = y \frac{d}{btc_{price} \cdot r} \quad (E3)$$

The only variables therefore are: $\boldsymbol{d}$ = difficulty, btc_{price} exchange rate, and $\boldsymbol{r}$ = block reward currently 12.5, (while $\boldsymbol{y}$ is constant 165,700,898.77 now)

$$Hashrate_{btc}^{\$100k} = 165,700,898.77 \frac{3,017,500,000,000}{10,000 \cdot 12.5} = 4,000,020$$ [5]

	Hashing Power to $100K	**Algo Adj. Factor**	**Hashrate Adjusted***	**Hashrate Adjusted**
	GHs updated on 2018-02-21	*miner profitability*	*GH/s * Algo Adj. Factor*	*vs. Bitcoin*
BTC	4080000.0000000	1	21,528,020,746.00	100.00%
ETH	50.3000000	81113	19,422,097,813.12	90.22%
BCH	4080000.0000000	1	2,415,000,000.57	11.22%
LTC	176.4000000	23129	3,270,082,993.20	15.19%
DASH	1265.0000000	3225	854,748,219.49	3.97%
XMR	0.0031050	1314009662	1,307,439,613.53	6.07%
ETC	67.0000000	60896	769,171,343.28	3.57%
ZEC	0.0007500	5440000000	2,859,546,880.00	13.28%

Table A2: Algorithm Adjustment Factor calculated from Mining profitability of each Hashing algorithm in compare to SHA-256 of Bitcoin, and Hashrate Adjusted, normalizing the hashrate of cryptocurrencies vs. bitcoin hashrate

[5] In a simplified manner most of online mining profitability calculator could get the job done, Bitcoin Mining Profitability, Ethereum Mining Profitability, etc, CryptoCompare *Retrieved* 2018-02-22

b) Adjustment factor by Implied Watts per GH/s

Another method is to divide the Implied Watts per GH/s of the most efficient mining equipment for two cryptocurrencies.

Example:

Antminer S9 is one of most efficient miners for BTC with Hashing power of 13500 GH/s and 1375 watts, ~ 0.1W/GH (*0.1 watts needed per second to generate one gigahash*)

Radeon Rx 480 is also one of most efficient miners for ETH, with hashing power of 25.0 MH/s at 150 Watts, ~6000 W/GH (*about 6k watts needed per second to generate 25.0 megahash*, 0.025 GH)

By dividing the implied watts per GH/s of Ethereum miner by Bitcoin miner, 6000 / 0.1 = 60,000 is the Adjustment Factor

$$Algorithm\ Adjustment\ Factor\ A2 = \frac{Implied\ W/GHs^{\ CryptoMiner}}{Implied\ W/GHs^{\ BTCMiner}} \qquad (E4)$$

Where ***Implied W/GHs*** is Watts needed to generate one Gigahash (*which is calculated by dividing hardware power consumption in watts by hashrate of that hardware*) ***CryptoMiner*** *is the most efficient mining hardware equipment of Crypto, and* ***BTCMiner*** for this comparison is Antminer S9, with 0.1 Implied W/GHs

	Miner	Implied W/Ghs	Algo Adj. Factor	Hashrate Adjusted*	Hashrate Adjusted
			Implied W/Ghs	*GHs * Algo Adj. Factor*	*vs. Bitcoin*
BTC	Antminer S9	0.10	1	21,528,020,746.00	100.00%
ETH	Radeon Rx 480	6,000.00	58909	14,105,428,363.64	65.52%
BCH	Antminer S9	0.10	1	2,415,000,000.57	11.22%
LTC	L3+ Antminer	1,587.30	15584	2,203,371,428.57	10.23%
DASH	Baikal Quadruple	266.67	2618	693,854,437.00	3.22%
XMR	Mining Rig 4320	177,304,964.54	1740812379	1,732,108,317.21	8.05%
ETC	Radeon Rx 480	6,000.00	58909	744,080,727.27	3.46%
ZEC	nVidia GTC 1080	367,647,058.82	3609625668	1,897,406,951.87	8.81%

Table B1: Algorithm Adjustment Factor calculated from Implied Watts per GH/s for most most efficient mining equipment for each hashing algorithm in compare to SHA-256 of Bitcoin, and Hashrate Adjusted, normalizing the hashrate of cryptocurrencies vs. bitcoin hashrate

Out of both proposed general models **A1** and **A2** we can get a rough estimation of the Algorithm Adjustment Factor to compare the hashrate of cryptocurrency networks While the first model has the price of cryptocurrency as an indirect factor influencing the math, the second model has the efficiency, which is not necessarily equal and naturally evolving with time, as a factor. Not surprisingly both models produced relatively close results.

Clearly, this model is limited to Proof-of-Work (PoW) crypto-based protocols, and an attempt to measure (or compare) the hashrate across various algorithms like

SHA-256-based, Scrypt-based, Zerocoin-based, CryptoNote-based, ETHash-based and other PoW-based.

4) INDEX CONSTRUCTION

We propose two versions to be tested for criticisms and discussions, (A) Computational Power (B) Robustness

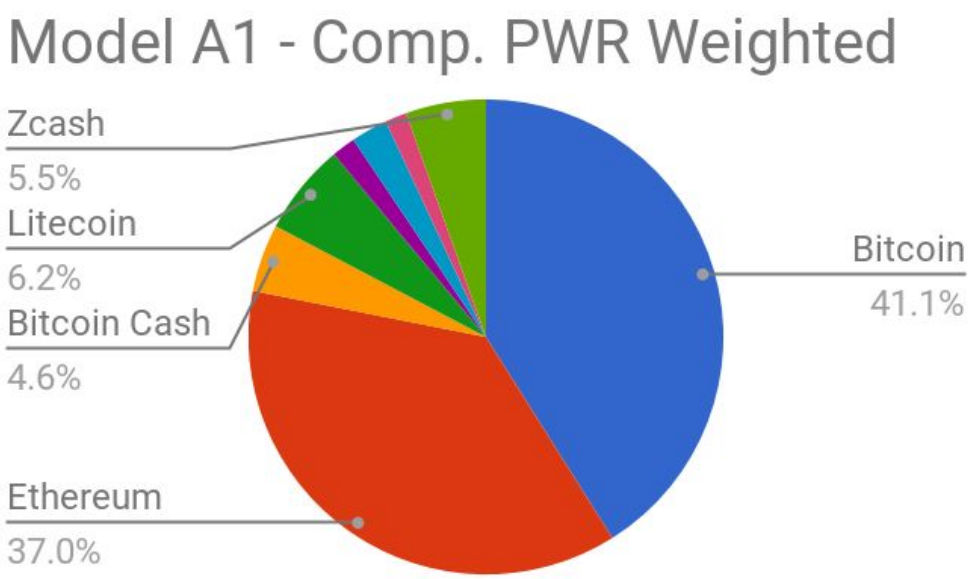
a) Hindex: Hashing Rate and Computational Power Weighted - *Model A*

We calculate each constituent -*crypto network computational power- as*: Constituent Network Hashrate * Algorithm Adjustment Factor

Constituents will be represented by their percentage of total computational power of index

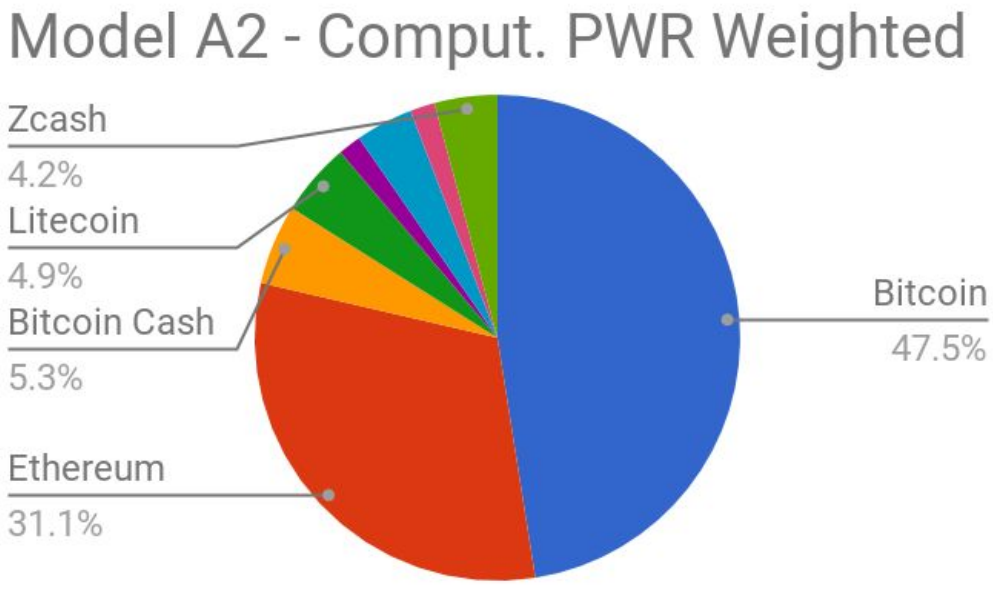
Model A1 *Computational Powered measured by Mining profitability Adjustment factor model A1*

	Hashrate GH/s	Algo Adj. Factor	Hashrate Adjusted*	Hashrate Adjusted	Index % - Model A1
2018-02-21	43,152.00	*miner profitability*	*GH/s * Algo Adj. Factor*	*vs. Bitcoin*	*Comp. PWR Weighted //1*
Bitcoin	21,528,020,746.00	1	21,528,020,746	100.00%	41%
Ethereum	239,444.00	81113	19,422,097,813	90.22%	37%
Bitcoin Cash	2,415,000,000.57	1	2,415,000,001	11.22%	5%
Litecoin	141,383.00	23129	3,270,082,993	15.19%	6%
Dash	265,013.85	3225	854,748,219	3.97%	2%
Monero	1.00	1314009662	1,307,439,614	6.07%	2%
Ethereum Classic	12,631.00	60896	769,171,343	3.57%	1%
Zcash	0.53	5440000000	2,859,546,880	13.28%	5%


Model A1 - Comp. PWR Weighted
Zcash
5.5%
Litecoin
6.2%
Bitcoin Cash
4.6%
Ethereum
37.0%
Bitcoin
41.1%

Model A2 *Computational Power measured by Implied W/GHs of most efficient mining equipment Adjustment factor model A2*

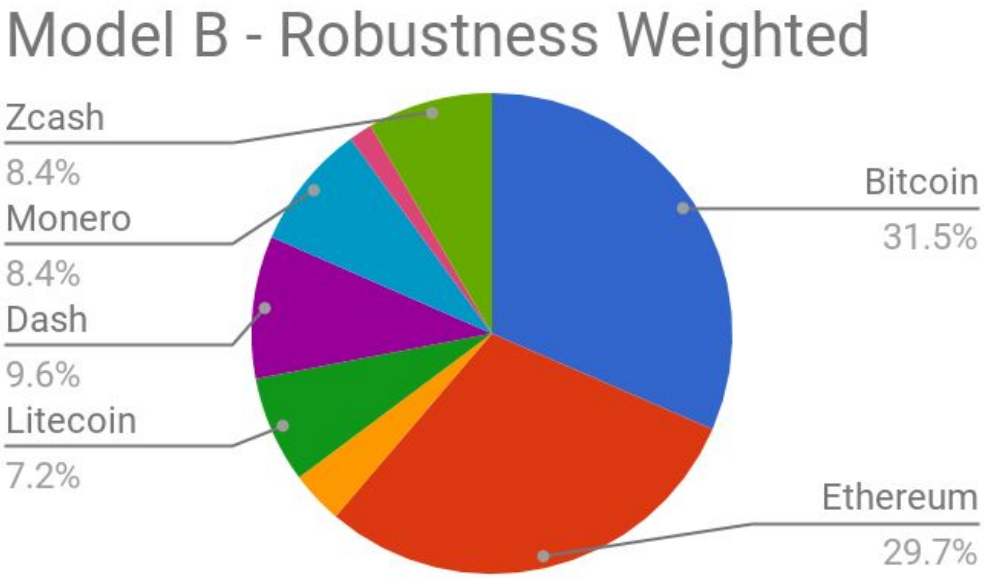
	Hashrate GH/s	Algo Adj. Factor	Hashrate Adjusted*	Hashrate Adjusted	Index % - Model A2
2018-02-21	$43,152	*Implied W/Ghs*	*GHs * Algo Adj. Factor*	*vs. Bitcoin*	*Comp. PWR Weighted //2*
Bitcoin	21,528,020,746.00	1	21,528,020,746	100.00%	48%
Ethereum	239,444.00	58909	14,105,428,364	65.52%	31%
Bitcoin Cash	2,415,000,000.57	1	2,415,000,001	11.22%	5%
Litecoin	141,383.00	15584	2,203,371,429	10.23%	5%
Dash	265,013.85	2618	693,854,437	3.22%	2%
Monero	1.00	1740812379	1,732,108,317	8.05%	4%
Ethereum Classic	12,631.00	58909	744,080,727	3.46%	2%
Zcash	0.53	3609625668	1,897,406,952	8.81%	4%



b) Rindex: Robustness weighted - *Model B*

We calculate each cryptocurrency constituent robustness (*currently the quantified factor is 51% attack cost, while other factors used binary for selection criteria*); And each constituent will be represented by its 51% attack cost as a percentage of all index constituents 51% attack cost.

	Market Cap	% of Marketcap	Hashrate GH/s	Cost of 51% Attach	Index % - Model B
2018-02-21		*vs. Total Crypto*	43,152		*Robustness Weighted*
Bitcoin	$167,718,371,080	41.83%	21,528,020,746.00	$2,027,780,087.45	31.52%
Ethereum	$73,666,238,524	18.37%	239,444.00	$1,912,870,227.20	29.74%
Bitcoin Cash	$18,301,236,553	4.56%	2,415,000,000.57	$227,475,111.16	3.54%
Litecoin	$10,263,353,772	2.56%	141,383.00	$462,255,084.76	7.19%
Dash	$4,095,322,437	1.02%	265,013.85	$616,496,413.08	9.58%
Monero	$4,941,283,788	1.23%	1.00	$543,039,479.91	8.44%
Ethereum Classic	$2,400,823,509	0.60%	12,631.00	$100,906,532.80	1.57%
Zcash	$1,173,510,334	0.29%	0.53	$542,039,974.12	8.43%



5) SELECTION CRITERIA

A Cryptocurrency (coin) has to fulfill all of the following criteria to be considered part of the index:

- Open source Cryptocurrency Coin *(not token)*
- Decentralized and has node quantity of: *TBD ex. 300 nodes*
- Use known well-tested cryptographic primitives
- Liquid and has a reasonable trading volume of: *TBD ex. n% of average*
- Active publicly for reasonable period of time: *TBD* ex. *6 months*
- Has active development team of: *TBD*
- Market cap of: *TBD ex. 10 million or 0.01% total crypto market cap*
- Traded Publicly on exchanges min. Of: *TBD ex. 3*

Unlike Cryptocurrency coins, Tokens (ERC20 of Ethereum, Waves, Omni etc) are inherently riskier as they carry out an external risk factor of the incubating platform, *besides its own*. Tokens wouldn't be part of the index with current models, and while market capitalization is not a factor of the calculation of any models on this index, whenever it becomes - or is added -, the overall market cap of hosted tokens should be added to the host platform market cap (if logically suitable) Think of it like 51% attack on Ethereum would erode confidence and drive price short for Ethereum and all its 8k tokens consequently, not only would the market cap of Ethereum shrink but all of ERC20 token's market cap accordingly.

6) INDEX CALCULATION

To compute the value of the Index:

$$Index\ Level\ =\ \frac{\sum\ (M_{it} \bullet P_i)}{Divisor} \qquad (E5)$$

Where $\mathbf{M_{it}}$ is the market capitalization of the crypto $\mathbf{i}$ at time point $\mathbf{t}$ and $\mathbf{P_i}$ is percentage of that crypto of the total as per the formulas of index construction model (A) Hashing - Computational Power (B) Robustness - 51% attack resistance,

The ***Divisor*** ensures that the changes in the quantity of constituents doesn't affect the value of the Index. ***Divisor*** starting *TBD* ex. 1000 and whenever the quantity of constituents changes; the ***Divisor*** has to be adjusted to ensure that just price changes cause changes in the value

7) CONCLUSION

Both Models (A) **Hindex**: Hashing - Computational Power (B) **Rindex**: Robustness - 51% attack resistance, have their own limitations and it's important to observe

- *Model A* is limited to crypto use PoW (*Proof-of-Work*) functions, and that excludes all non-PoW, yet PoW cryptos represent 85%+ total and its market cap

- *Model B* is more inclusive and beside the PoW examined in our study here it's capable of including cryptos of other consensus protocol, like PoS (*Proof of Stake*) cryptos as for Lisk, Waves and Nxt, PoI *Proof-of-Importance* as for NEM, and dBFT (*Delegated Byzantine Fault Tolerance*) as NEO etc, though other robustness factors have to come in play then as 51% attack by design is way more expensive in PoS -and impractical- than it's with PoW.

8) REFERENCES

Normative references

I. S. Trimborn; W. K. Härdle (2015), CRIX an Index for blockchain based Currencies Retrieved 2017-10-21

II. Tai Zen; Leon Fu Dot Com (2017) TaiFu™ 30 Cryptocurrency Market Index a market capitalization weighted index of the largest 30 cryptocurrencies for that day. Retrieved 2017-10-21

III. Bletchley Indexes (2017), Bletchley Indexes Family Retrieved 2017-10-22

IV. SCI (2017): Smith + Crown Index Retrieved 2017-10-21

V. Crypto30 (2017) The CAMCrypto30 an open, published, rules-based index of the top 30 crypto currencies (CCs) by market capitalization. Retrieved 2018-01-25

VI. Lawnmower Blockchain Index (2015) LBI Lawnmower Blockchain Index: selected market capitalization weighted crypto index . Retrieved 2017-10-09

VII. D Schwartzkopff; L. Schwartzkopff; R. Botha; M. Finlayson; F. Cronje. (2017) C20 - Crypto20: Tokenized Crypto Index Fund: Whitepaper Retrieved 2017-12-15

VIII. CCX20 (2017), Buchman Crypto 30 Index 20% capped market capitalization of 30 largest cryptocurrencies. Updated 2018-02-10

IX. Bit20 (2017): 10% capped index fund by market capitalization Retrieved 2017-10-06

X. I. Rivin; C. Scevola; R. Davis (2017), CCI30: Smoothed market capitalization weighted of top 30 crypt currencies, CCI30 weigh each component proportionally to the square root of its market capitalization Retrieved 2017-10-26

XI. ICONOMI (2016), DAA a tokenized digital assets arrays™ of cryptos using Ethereum smart contracts. Retrieved 2017-10-26

XII. A. Antonopoulos (2014), Mastering Bitcoin Programming the Open Blockchain 2nd Edition, O'Reilly, pp 254 - 255 via google books

XIII. BitcoinCharts (2017) Bitcoincharts Bitcoin Network Retrieved 2017-10-12

XIV. Top 500 (2017) Performance Development Retrieved 2017-10-11

XV. CryptoCompare (2017) Bitcoin Mining Profitability, and Ethereum Mining Profitability, Retrieved 2018-02-22

XVI. G. Hileman; M. Rauchs (2017) Global Cryptocurrency Benchmarking Study, Cambridge centre for Alternative Finance

XVII. M. Rosenfel (2011). Analysis of Bitcoin Pooled Mining Reward Systems

XVIII. I. Giechaskiel; C. Cremers; K. B. Rasmussen (2016), On Bitcoin Security in the Presence of Broken Crypto Primitives

Informative references

I. E. Heilman; A. Kendler (2015) Eclipse Attacks on Bitcoin's Peer-to-Peer Network
II. Mario Dian (2017), Cost of a 51% Attack and Security of Bitcoin, Monero, Litecoin and other Cryptocurrencies
III. Github Crypto Index Fund: A DIY crypto index fund based on Google spreadsheet and Coinmarketcap APIs
IV. The Flipside (2017) Crypto GitHub Index Tracks cryptocurrencies with a GitHub repository
V. Y. Gilad; R. Hemo; S. Micali; G. Vlachos; N. Zeldovich (2017), Algorand Scaling Byzantine Agreements for Cryptocurrencies, MIT CSAIL
VI. N. Tomaino (2017) Antifragile Cryptoeconomic Systems, The Control via Medium
VII. They Crypto Coffee Index (2017), is based on the average price of coffee, the average barista hourly wage, the block speed of the cryptocurrency and transaction fees associated with the particular crypto.
VIII. Raulo (2011), Optimal pool abuse strategy
IX. CoinGecko (2017), Community and Developer statistics.

9) ANNEX I - TRANSACTION VOLUME WEIGHTED MODEL C

Blockchain cryptocurrencies record all validated transactions grouped into blocks, each cryptographically linked to predecessor transactions down to the genesis block, thereby creating a “chain of blocks” or “blockchain”, the mining sector is responsible for confirming transactions and securing the global record of all transaction and transaction fees, representing a portion of mining revenues, and projected to constitute nearly 10% of total mining revenues by the end of 2017 - G. Hileman; M. Rauchs (2017)

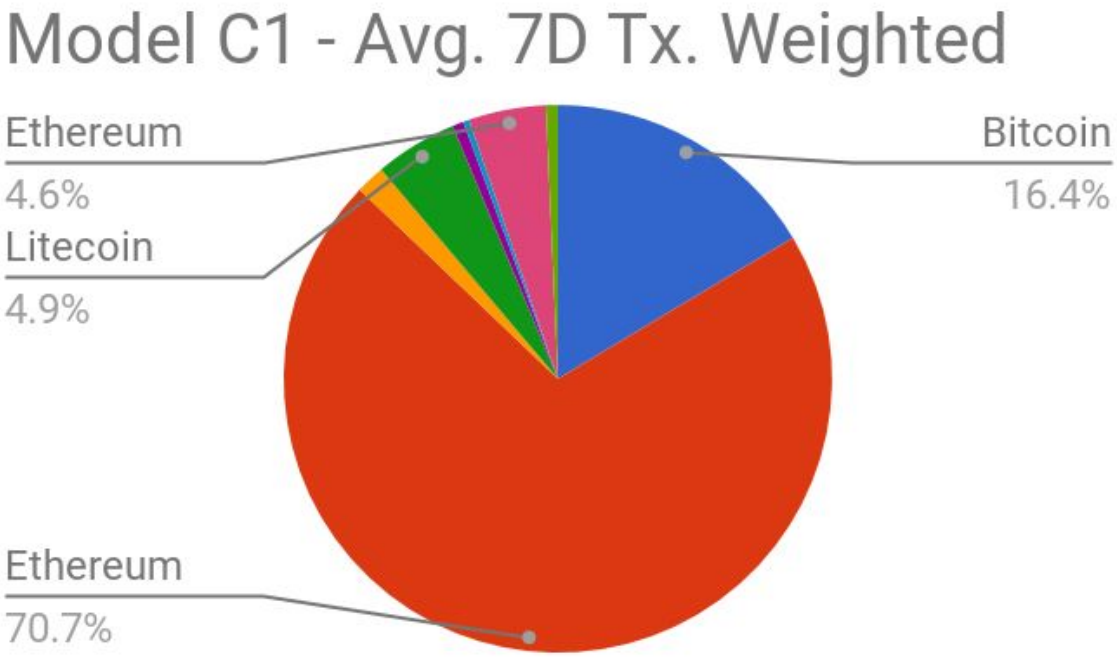
Transaction Volume (*both transaction volume in USD-value and transaction volume measured by the number of transactions*) as a utility and user adoption indicator factor, and beyond the store of value but as transactional money with broader utility, we simulate an index transactional volume-weighted for comparison.

When comparing the average number of daily on-chain transactions performed on each cryptocurrency network, Ethereum and Bitcoin are by far the most widely used, followed -and by considerably distant- third-place Ethereum Classic, Litecoin and others.

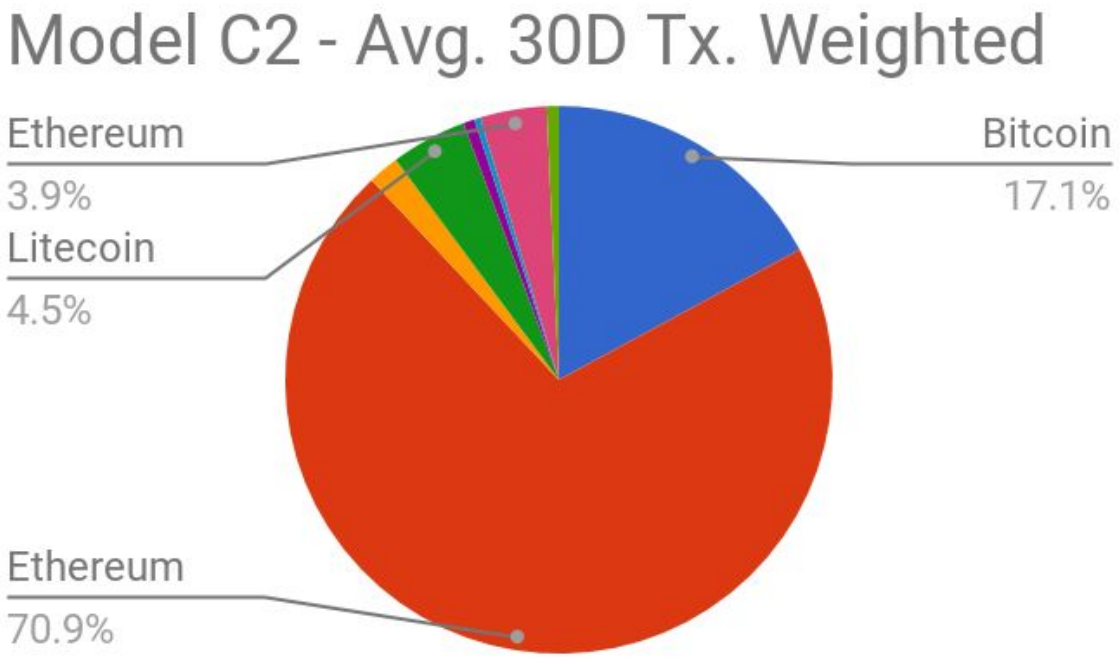
We cannot assert and sustain that the transaction volume are isolatedly the main factors on the indication of a particular crypto utility progress and user adoption; the study of isolated variables, inductively, allows us, however, to understand findings more widely, another conjugated indicator on the same class is the so-called “active wallets”, wallets or addresses that transact with n frequency, but because of 1) the ambiguousness of the term “Active” and its definition 2) Technical limitations in gathering the relevant data we limited the study here to the transaction volume by number of transaction recorded on-chain only[6]

[6] Bitcoin transaction data available at blockchain.info, Ethereum transaction data available at: Etherscan.io; DASH transaction data available at: CryptoID, Monero transaction data available at: MoneroBlocks.info; Litecoin transaction data available at: CryptoID, aggregated transactions data available at: bitInfoCharts (All Retrieved: 2018-02-22).

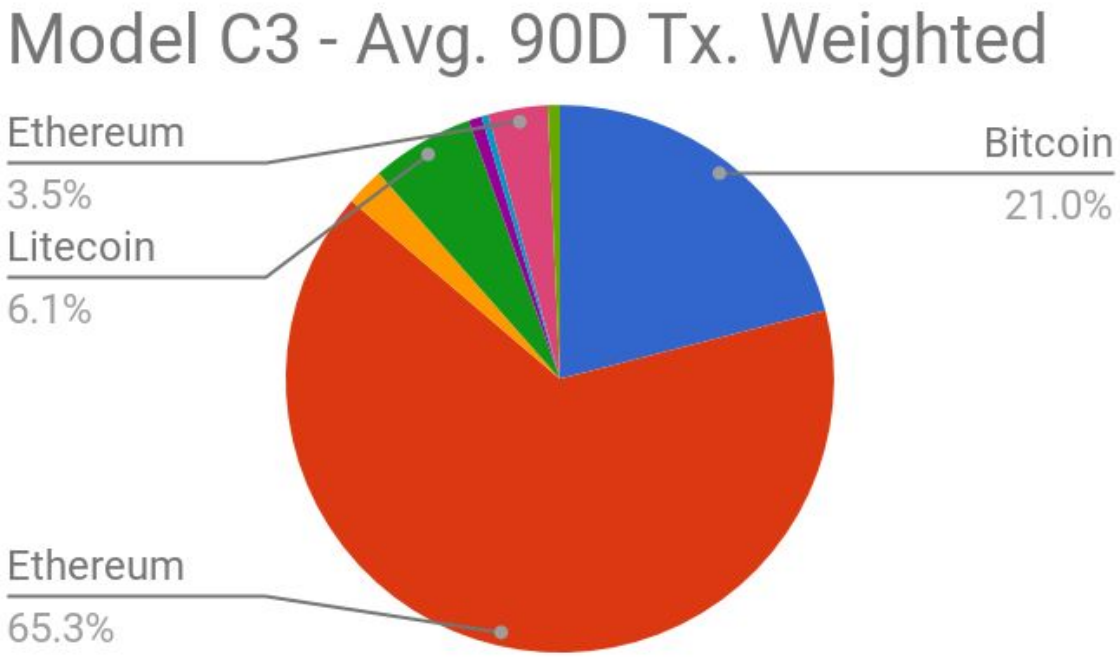
	Market Cap	% of Marketcap	Transaction Vol.	Tx Vol. Avg.	Index % - Model C1
2018-02-22		*vs. Total Crypto*	*Tx 1 Day*	*avg. 7 days*	*Avg 7day Tx . Weighted*
Bitcoin	$167,718,371,080	41.83%	185,045.00	184,522.00	16.40%
Ethereum	$73,666,238,524	18.37%	733,084.00	795,990.00	70.74%
Bitcoin Cash	$18,301,236,553	4.56%	17,589.00	19,228.00	1.71%
Litecoin	$10,263,353,772	2.56%	41,534.00	54,940.00	4.88%
Dash	$4,095,322,437	1.02%	6,633.00	7,432.00	0.66%
Monero	$4,941,283,788	1.23%	3,319.00	3,986.00	0.35%
Ethereum Classic	$2,400,823,509	0.60%	49,971.00	51,258.00	4.56%
Zcash	$1,173,510,334	0.29%	6,589.00	7,886.00	0.70%



	Market Cap	% of Marketcap	Transaction Vol.	Tx Vol. Avg.	Index % - Model C2
2018-02-22		*% of Marketcap*	*Tx 1 Day*	*avg 30 day*	*Avg 30day Tx . Weighted*
Bitcoin	$167,718,371,080	41.83%	185,045.00	199,798.00	17.11%
Ethereum	$73,666,238,524	18.37%	733,084.00	827,983.00	70.90%
Bitcoin Cash	$18,301,236,553	4.56%	17,589.00	21,460.00	1.84%
Litecoin	$10,263,353,772	2.56%	41,534.00	52,445.00	4.49%
Dash	$4,095,322,437	1.02%	6,633.00	7,815.00	0.67%
Monero	$4,941,283,788	1.23%	3,319.00	4,231.00	0.36%
Ethereum Classic	$2,400,823,509	0.60%	49,971.00	45,767.00	3.92%
Zcash	$1,173,510,334	0.29%	6,589.00	8,369.00	0.72%

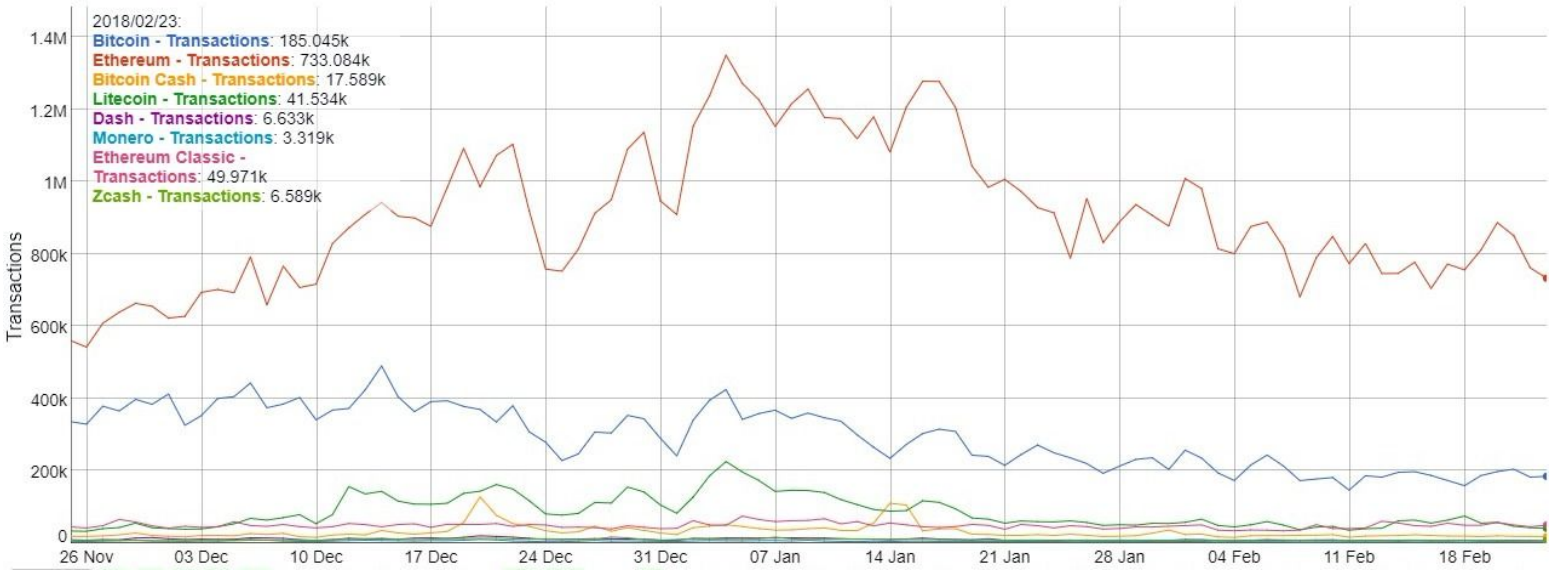


	Market Cap	% of Marketcap	Transaction Vol.	Tx Vol. Avg.	Index % - Model C3
2018-02-22		*vs. Total Crypto*	*Tx 1 Day*	*avg. 90 days*	*Avg 90day Tx . Weighted*
Bitcoin	$167,718,371,080	41.83%	185,045.00	292,977.00	20.99%
Ethereum	$73,666,238,524	18.37%	733,084.00	911,125.00	65.27%
Bitcoin Cash	$18,301,236,553	4.56%	17,589.00	31,570.00	2.26%
Litecoin	$10,263,353,772	2.56%	41,534.00	85,048.00	6.09%
Dash	$4,095,322,437	1.02%	6,633.00	10,779.00	0.77%
Monero	$4,941,283,788	1.23%	3,319.00	5,730.00	0.41%
Ethereum Classic	$2,400,823,509	0.60%	49,971.00	48,974.00	3.51%
Zcash	$1,173,510,334	0.29%	6,589.00	9,799.00	0.70%



Bitcoin vs. Ethereum Transactions volume 2017-2018

BTC vs. ETH, BCH, LTC, DASH, XMR, ETC, ZEC Transactions volume - 1Q2018



10) ANNEX II - CRYPTOCURRENCY ANTIFRAGILITY INDEX

Arguably all open-source blockchains are anti-fragile by design as result of the repeated exposure to stress, presenting mainly by having the (1) source open and (2) financial incentive, it doesn't just resist attack but actually benefits from it, every day it becomes harder and harder to disrupt blockchain

An “antifragility” weighted index, which would measure the property of cryptoasset network that increases in capability, resilience, or robustness as a result of stressors, shocks, volatility, noise, mistakes, faults, attacks, or failures

A system can become antifragile, since, it grows stronger from each successive stressor, disturbance, and failure,

In such a model each attack *or attempt* (including fork or security flaw) needs quantifiable metrics or scale value, It would be quite interesting to explore in further details, Antifragility as different flavor addition to Index family