



UNIVERSITY OF NICOSIA
ΠΑΝΕΠΙΣΤΗΜΙΟ ΛΕΥΚΩΣΙΑΣ

DFIN-511

Introduction to Digital Currencies

Session 7

Alternatives to Bitcoin

Objectives of Session 7

- Provide an overview of some popular alternative currencies
- Devise categorization criteria for most popular alt-coins
- Summarize KPIs to keep in mind when assessing alternative digital currencies



As mentioned in Session 6, boundaries between concepts are not always 100% clear in an area of constant innovation. Bitcoin might be the “king” but there are alternative digital currencies that represent a different way of thinking.

In the following pages, we aim to build a framework for the reader to better understand the notions behind cryptocurrencies that are being developed, other than Bitcoin. This session is devoted to them since they certainly deserve our attention.

Agenda

1. Why alternative currencies?
2. Indicative alternatives
3. Common characteristics
4. Criteria for categorization
5. KPIs for assessing digital currencies
6. Conclusions
7. Self-Assessment Exercises and Further Reading

1. Why alternative currencies?

Why alternative currencies?

Bitcoin is the first application of a technology that paves the way forward, revealing an opportunity for innovation that was not apparent before.

Bitcoin is wholly open source, so every element of it can be tweaked, modified, altered and tested for potentially improved iterations, just like evolution.

Bitcoin's blockchain has grown large (currently slightly over 34GB) – and will only become larger, as Bitcoin use becomes more widespread.

The process of mining is very power intensive, which may be argued is with a disproportionate benefit towards the network.

The nature of a predetermined, and eventually deflating monetary base as coins are irrecoverably lost, dissuades some from using it. Excessive hoarding is also said to be doing the same.

Why alternative currencies?

The freedom to try out every possible solution has driven many to spawn their own “**alt – coins**”, with their own rules and their own networks. Some older concepts (like Ripple) have been augmented by the innovation of the blockchain and have developed in their own right.

While some are merely small modifications of the Bitcoin protocol and have limited audiences, others are interesting sources of innovation. The differences derive from changes in the basis of each coin’s philosophy which are achieved in a variety of ways, such as:

- Altering the issuance method to less energy intensive processes
- Altering the monetary supply and issuance rate
- Altering the hashing algorithms or other parameters
- Introducing other concepts such as demurrage to increase the velocity of money

2. Indicative alternatives

Indicative alternatives

Bitcoin may be the king, but several alt-coins have seen some attention :






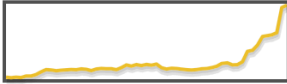

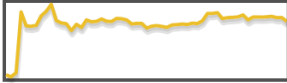

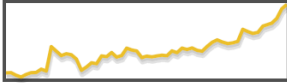



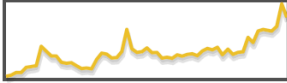

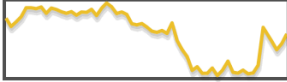

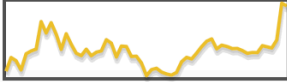
568 Currencies / 55 Assets / 1770 Markets

source: coinmarketcap.com as of May, 2015

The so called “market cap” (available supply X current exchange rate) for each coin, is at best a vague indicator of each coins’ prowess. Several other important factors are harder to quantify and are not usually considered in tandem (user base, merchants accepting, exchanges trading each coin, active development taking place, etc).

Even if we assume, (through the Efficient Market Hypothesis), that these elements are already “baked” in the exchange rate of each coin, there is still a degree of subjectivity surrounding valuation and the final exchange rates, like in the conventional world.






Indicative alternatives






#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$ 3,352,091,607	\$ 235.86	14,212,450 BTC	\$ 15,023,500	-0.65 %	
2	 Ripple	\$ 275,982,806	\$ 0.008649	31,908,551,587 XRP *	\$ 1,634,690	18.13 %	
3	 Litecoin	\$ 71,809,988	\$ 1.82	39,432,854 LTC	\$ 1,370,960	-1.20 %	
4	 BitShares	\$ 20,952,427	\$ 0.008341	2,511,953,117 BTS *	\$ 264,895	16.41 %	
5	 Dogecoin	\$ 19,519,358	\$ 0.000196	99,588,051,522 DOGE	\$ 848,239	7.68 %	
6	 Stellar	\$ 18,089,867	\$ 0.003740	4,837,354,256 STR *	\$ 115,466	10.97 %	
7	 Dash	\$ 15,062,032	\$ 2.79	5,407,784 DASH	\$ 70,156	5.84 %	
8	 Nxt	\$ 12,953,262	\$ 0.012953	999,997,096 NXT *	\$ 165,421	10.69 %	






source: coinmarketcap.com,
as of May 2015

Indicative alternatives

Some more players and their market caps...

1	 Bitcoin	\$ 3,352,091,607
2	 Ripple	\$ 275,982,806
3	 Litecoin	\$ 71,809,988
4	 BitShares	\$ 20,952,427
5	 Dogecoin	\$ 19,519,358

6	 Stellar	\$ 18,089,867
7	 Dash	\$ 15,062,032
8	 Nxt	\$ 12,953,262
9	 BanxShares	\$ 8,289,356
10	 MaidSafeCoin	\$ 7,803,995

11	 Peercoin	\$ 7,351,425
12	 Bytecoin	\$ 4,795,221
13	 Namecoin	\$ 3,935,313
14	 Monero	\$ 3,580,960
15	 FairCoin	\$ 3,404,161

source: coinmarketcap.com,
as of May 2015

A coin by any other name

In the previous session we briefly discussed meta-coins; in this session we are touching up on alt-coins.

Any means of exchange that is based on the design concepts of Bitcoin, yet with differences or enhancements in its implementation, could be considered to be an “*alt-coin*”.

An alt-coin is in many cases considered a software “*fork*” of the Bitcoin code (not a blockchain fork that may happen in Bitcoin), with minor alterations to its characteristics. Using the original open source software with a number of modifications, these new coins have different properties and create their own blockchains, which are unrelated to the Bitcoin blockchain. Some designs start from the ground up, with new code and additionally confer other characteristics to the functionality of the coins themselves (like NXT or Ripple) so the network itself is not an alt-coin.

Their market cap is only one possible indicator of their prowess in the market, and is usually not meant to be directly comparable between different coins.

Ethereum

Ethereum is a a hybrid meta/alt-coin (studied in Session 6) that attempts to build, in their own words, “*a revolutionary new platform for applications*”, targeting anything from *voting to financial exchanges*, to *smart property*, and most importantly, *decentralized autonomous organizations*. Even though the currency used in the network is an alt-coin (ether), the protocol goes beyond that simple exchange of currency to provide :

- A standardized foundation platform (i.e. the enhanced Ethereum programming abstractions, protocol and network)
- A programming language to facilitate the creation of distributed applications by anyone
- Its own currency or *cryptofuel* – the “*Ether*” – with subdenominations / multipliers ranging from: (a) *Wei* (10^0), (b) *Szabo* (10^{12}), (c) *Finney* (10^{15}), to (d) *Ether* (10^8), used for paying transaction fees



Source: ethereum.org

Ethereum is based on the concept of *self-executing smart contracts* (Session 6), software contracts that execute specific instructions upon interacting with them through transactions.

Ethereum – in detail

Ethereum approaches the existing Bitcoin infrastructure as a “*state machine*”, where transactions (which store *messages*) serve as “*state transitions*” between Ethereum accounts.

There are *two types* of Ethereum accounts:

- **Externally-owned accounts** – used for sending *messages*, and do not contain code
- **Contract accounts** – used for executing a specific *contract code* upon receiving a *message*

An **Ethereum account** consists of:

- **An Ether balance** – used for paying transaction fees
- **A contract code** – used by contract accounts to implement application logic
- **Storage** – used by **contract accounts** for retrieving or storing information accordingly as their code executes, otherwise it is empty
- **A nonce** – used for ensuring that transactions are only processed once

Ethereum messages serve as “*functions*” and have the following characteristics:

- They can be created by an external entity or a contract
- They can contain data
- They can only receive responses from *contract accounts*

Ethereum – in detail

Finally, **Transactions** in Ethereum are viewed as “*signed data packages*” and contain:

- **A message** to be sent from an *externally-owned account*
- **A Sender signature** – which indicates the sender of the message
- **A Receiver address** – which indicates the receiver of the message
- **An Ether amount** – which indicates the amount of Ether to send
- **Data** – which encapsulates the data to be sent
- **A Start Gas field** – which limits the number of computational steps over which a contract code will execute
- **A Gas Price field** – which is the fee that will be paid to a miner at each computational step

To achieve its goals, Ethereum defines its own logic for state transitions processing and code execution, whose details are beyond the scope of this Session.

Due to the vast applications it enables, Ethereum has been described as, “*Bitcoin on steroids*”.

Ethereum, progress so far

Ethereum is so far, the third most highly crowdfunded project globally, gathering a staggering 31,529.49449551 BTC by September 3rd 2014 ([address](#)).

Even though the road is still long for a functional prototype that can perform everything the team is poised for, several proof of concept clients are available in their [GitHub repository](#).

One of the very important concepts that Ethereum attempts to achieve is a level of being “**Turing Complete**”. ([Definition](#)) So far, the explanation [given](#) by the Ethereum team is that they are attempting to make a quasi-Turing-complete system. The cost of each step of these recursive processes or loops is the fuel of the system (ether) as a fee.

3. Common characteristics

Common characteristics

All different digital currencies have some common characteristics:

- They rely on cryptographic hash functions and asymmetric cryptography
- Most are designed to gradually introduce new coins into circulation
- All have a specific rate of issuance which may or may not be capped towards an ultimate number. Some are based on a pre-programmed supply, response to demand or response to their use.

In the following pages, we will be exploring their differences, categorizing them into groups using different criteria and conclude with KPIs (Key Performance Indicators) that are important to keep in mind when assessing crypto-currencies.

4. Criteria for categorization

Criteria for categorization

Let us now explore
the core differences
between most
decentralized digital
currencies:



Criteria for categorization

Let's begin with the basic elements of the consensus and incentive method used:



Proof of work / stake / resources / ...

There are different methods / concepts behind the process though which one can provide proof to the network of working “*with the system*” and not “*against it*”. The tradeoff between something of value (energy, time or other resource) to empower the network, aids to ascertain which participants are acting “rationally” and which are not. The incentive for this is usually earning new coins and/or transaction fees.

Proof of work - mining is required to gain coins, which usually is hash or script based

Proof of stake - coins are earned as a reward for displaying ownership

Proof of resources – recognition of contribution of resources to the network

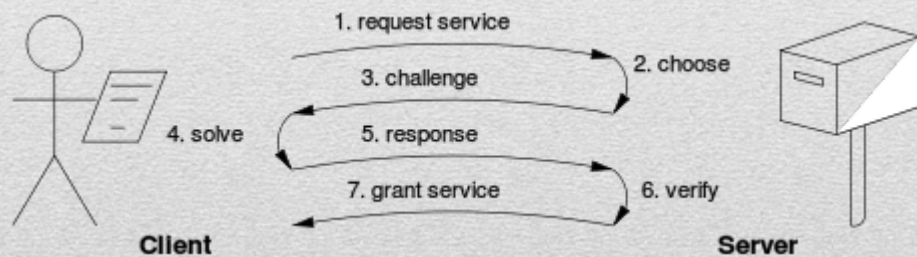
Proof of burn – “*bootstrapping one cryptocurrency off of another*”

Proof of work (PoW)

Proof of Work (PoW) - One party (the **prover**) presents the result of a computation hard to **compute**, but easy to **verify** and by verifying the solution anyone else can be **sure** that the prover performed a certain amount of computational work to generate the result.

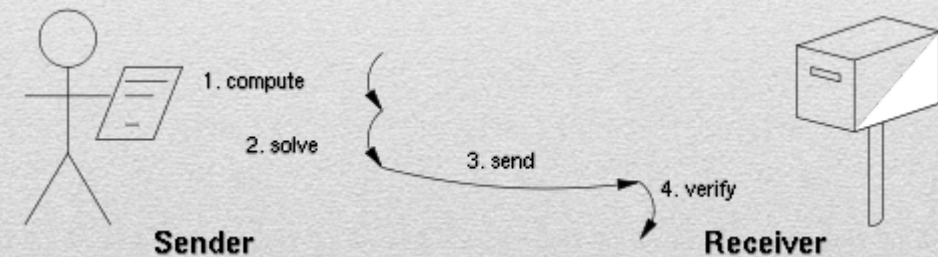
2 classes of PoW protocols:

challenge-response



VS

solution-verification



PoW - Algorithm used for verification / mining

- Secure Hash Algorithm - SHA-256 (e.g. Bitcoin)
- scrypt algorithm (e.g. Litecoin)
- Hybrid and CPU-only algorithms (e.g. PrimeCoin)
- X11 algorithm (e.g. Dash)

PoW - Algorithm used for verification / mining

Examples of coins using Secure Hash Algorithm - SHA-256 :



Namecoin – Peercoin

```
SHA256("hello") = 2cf24dba...  
SHA256("Hello") = 185f8db3...  
SHA256("Hello.") = 2d8bd7d9...
```

SHA-256 is an asymmetric hash function for which it is easy to calculate an output given an input but impossible to do the reverse. The representation of a SHA-256 output is a series of 64 hexadecimal digits – letters and numbers in the set {0123456789abcdef}. For example, the first digits of the hashes are depicted above.

PoW - Algorithm used for verification / mining

Examples of coins using Secure Hash Algorithm - SHA-256 :



Namecoin – Peercoin

```
SHA256("hello") = 2cf24dba...  
SHA256("Hello") = 185f8db3...  
SHA256("Hello.") = 2d8bd7d9...
```

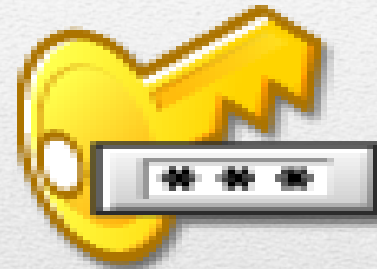
SHA-256 is designed so that even tiny changes in the input can dramatically change the output. In order to find the first digit of an input whose SHA -256 starts with '0' we need on average 16 attempts. Accordingly, to find "00" we need $16^2=256$ attempts, and so forth.

PoW - Algorithm used for verification / mining

Examples of coins using the script algorithm:



Litecoin – Novacoin – Worldcoin – Feathercoin



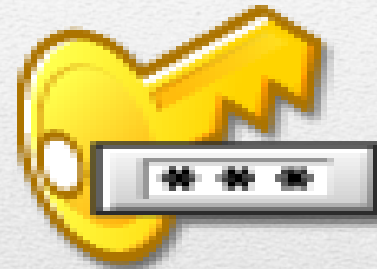
The script algorithm uses a password-based key derivation function, designed to hinder brute-forcing by raising the demands on the algorithm in term of resources (e.g. memory). Time–memory tradeoffs need to be taken into consideration when mining for such coins. script mining is memory intensive, which makes it harder to massively parallelize and centralize with Application Specific Integrated Circuit (ASIC) technology.

PoW - Algorithm used for verification / mining

Examples of coins using the X11 algorithm:



Dash



The X11 chained hashing algorithm is a PoW algorithm that uses 11 different hashing functions to calculate the block header. The X11 algorithm was intended to be ASIC resistant so as to keep mining CPU- and GPU- friendly.

Proof of Stake (PoS)

Proof of Stake (PoS) – Instead of performing the task of solving difficult mathematical algorithmic problems (i.e. mining for coins), a proof of stake scheme implies that the owner of coins can earn coins by just proving that she owns a certain amount of coins.

There are 2 main approaches taken in PoS implementations:

Cunicula's Implementation of Mixed Proof-of-Work and Proof-of-Stake

This suggestion is of a mixed Proof-of-Work / Proof-of-Stake system.

Meni's implementation

This proposal is for a proof-of-work (PoW) skeleton on which occasional checkpoints set by stakeholders are placed. In one variant, double-spending is prevented by waiting for a transaction to be included in a checkpoint; the variant described here uses cementing to prevent double-spending, and checkpoints to resolve cementing conflicts.

source : https://en.bitcoin.it/wiki/Proof_of_Stake/

Proof of Stake (PoS)

Proof of stake - first appearance of this concept:

QuantumMechanic
Member
●●



Proof of stake instead of proof of work

July 11, 2011, 04:12:45 AM

#1

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys.

Activity: 110

PoS : the ..other side of the coin

Could Peercoin and "Proof-of-Stake" Turn Bitcoin Into The Myspace of Cryptocurrency?

JANUARY 19, 2014 BY SHANE DARK | FOLLOW US ON TWITTER [HERE](#)

source : cointrader.org/peercoin-proof-of-stake-and-bitcoin/



Gavin Andresen

@gavinandresen



Follow

@mariobo03 I think proof-of-stake is hard-coded 'the rich get richer' and is deeply unfair.

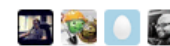
↩ Reply ↻ Retweet ★ Favorite ⋮ More

4

RETWEETS

1

FAVORITE



5:32 AM - 10 Jan 2014

PoS - Algorithm used for verification / mining

Examples of coins using PoS algorithms:



Nxt

the first 100% PoS currency.

Coins are earned solely by charging transaction fees.



Examples of Coins using Hybrid Algorithms

Examples of coins using Hybrid algorithm:



Peercoin (PPC)

Hybrid Proof of Work / Proof of Stake coin;
“The ratio of newly produced coins shifts to favor ones produced via Proof-Of-Stake minting”

Examples of Coins using Hybrid Algorithms

Examples of coins using Hybrid algorithm:



Securecoin

Multiple Algorithms:

Grøstl, Skein, BLAKE, BLUE MIDNIGHT WISH, JH, SHA-3



Examples of Coins using Hybrid Algorithms

Examples of coins using Hybrid algorithm:



Quark coin (QRK)

“Super secure” hashing:

9 rounds of hashing from 6 hashing functions

3 rounds apply a random hashing function.

Examples of Coins using Hybrid Algorithms

Examples of coins using Hybrid algorithm:



Yacoin (YAC)

Hybrid Proof of Work / Proof of Stake;
Proof of Work – Script, but
N parameter of Script increases over time

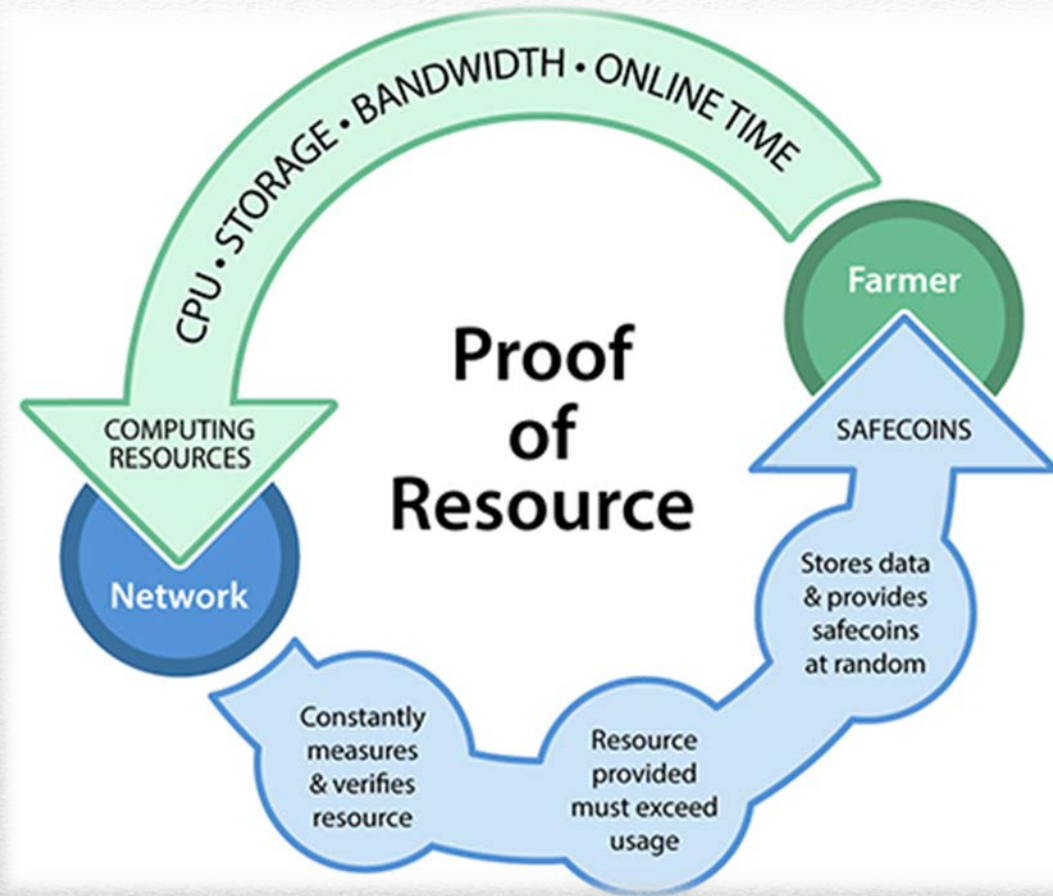


Proof of Resources (PoR)

This scheme is based on the notion that end users can earn coins by contributing to the network, more resources than those they use to mine coins for themselves. These users are called “farmers” and they receive this reward for maintaining / supporting the network.

This concept has not been extensively discussed or adopted; the main idea is depicted in the diagram on the right, but it could be the spur for significant innovation.

The main effort to apply POR is currently applied by the [Maidsafe](#) project, in a venture to create nothing less, than a fully decentralized Internet !



http://en.bitcoinwiki.org/Safecoin#End_Users_Proof_of_Resource

PoR - Algorithm used for verification / mining

Examples of coins using PoR algorithms:



SAFE (Secure Access For Everyone)

End users can farm (or earn) safecoins by providing Proof of Resource (PoR). Resources can be bandwidth or disk space, in an attempt to further decentralize the internet.



Proof of Burn (PoB)

The idea is that miners should show proof that they *burned* some coins - that is, sent them to a verifiably unspendable address. This is expensive from the miners' individual point of view, just like proof of work; but it consumes no resources other than the burned underlying asset. To date, all proof of burn cryptocurrencies work by burning proof-of-work-mined cryptocurrencies, so the ultimate source of scarcity remains the proof-of-work-mined "*fuel*".

https://en.bitcoin.it/wiki/Proof_of_burn

There is a significant discussion on the subject in the Bitcoin forum at bitcointalk.org.

PoB - Algorithm used for verification / mining

Examples of coins using PoB algorithms:



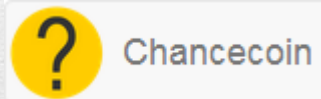
Counterparty

"Proof of burn" is also used by CounterParty, a meta-coin that sits on top of the Bitcoin blockchain (as already discussed in Session 6).



PoB - Algorithm used for verification / mining

Examples of coins using PoB algorithms:



CHA

Chancecoin is a protocol, a coin and a client, created upon the Bitcoin blockchain, for gambling like on online casinos. Coins are created by burning Bitcoins in a certain period of time (*"proof-of-burn"* period).

<https://bitcointalk.org/index.php?topic=528023.0>

<http://bitcoin.stackexchange.com/questions/24187/what-is-proof-of-burn>

Criteria for categorization

Let us now explore
how new coins are
introduced in the
systems and how
rewards for
processors work:



Pre-mined / Merged mining

Some currencies are *pre-mined*, which means that coins are mined from the creator of the cryptocurrency before it is actually released to the public. They can then sell them to the public, thus increase the supply of coins leading the crypto-currency to deflation.

"There's a term for them in the community," says Freidenbach in an [interview](#) in The Guardian. "They call them 'scamcoins' because they're obviously there to commit fraud." - ([link](#) for the term)

Joint / merged mining refers to the practice of creating hashes and submitting them to more than one blockchains, i.e. mining for Bitcoin and Namecoin at the same time (or Sidechains). No intersection of data takes place; for merged mining to take place, we only need to run two clients simultaneously and submit hashes created by your miner to both networks.

Running more than one clients is of course resource consuming; disc space and memory are more occupied and bandwidth is also necessary. Moreover, the pair or group of currencies that we need to choose for merged mining has to be on the same difficulty level, otherwise you produce hashes that are proper for one network each time, providing you with less opportunities for synergies.

Ripple

Ripple is a case of a project that begun before Bitcoin (2004), but truly came to fruition after the technology of Bitcoin was invented.

Ripple resembles a digital version of the ancient [Hawala](#) system, a form of social remittance mechanism based on connections of parties that trust each other. This creates a network of trusted entities that can transact a very large number of currencies and assets with each other. Gateways are the interface point of users with the network and they transfer assets via issuing and transferring IOUs to each other, through the shortest trust paths of the network between sender and receiver. Transfers in Ripple usually take 2-5 seconds to make. There is no mining process involved and all internally used currency (XRP) are issued centrally. In total, 100 billion XRP were created, 80 billion of which were given to Ripple Labs to manage and distribute to users. The co-founders kept the other 20 billion.

News of Ripple co founder's intention to sell off his [holdings](#), spurred speculative pressures on the exchange rate of XRP in May 2014. Since then, they have announced [\\$28 million in funding](#), and are exploring a pilot [program with Western Union](#).



Criteria for categorization

Can the mining effort be productive for other things as well?



Alternative uses of mining energy

Mining as a process requires the expenditure of significant energy. While the investment of “*work*” is an imperative for the success of the PoW systems, alternatives have been suggested, that could provide additional usability to this work produced.

Smart algorithms aim to use this energy effectively e.g. produce and store prime numbers.
Example :



Miners solving arbitrary hash functions, use their processing power to discover new Cunningham chains (prime numbers), a mathematically valuable function.

Prime numbers are thought to have applications in curing diseases like Alzheimer's and possibly even finding alien life. Thus, Primecoin offers a form of academic utility and turns researchers' attention to modern mining applications that go far beyond just mining cryptocurrencies.

Criteria for categorization

Let us now explore the significance that total supply and new coin introduction rate may have:



Total Supply

The total supply of bitcoins and the reason it was arbitrarily set at 21,000,000, has given fuel for much discussion in the Bitcoin community. In the true spirit of open source, this has led to a large number of coins arguing over increased scarcity (less total number of coins) or artificial abundance (many more total number of coins).

Other characteristics are often the ground for experimentation. These include:

- The rate of issuance until the total supply
- The issuance rate according to issuance method (for hybrid PoS/PoW coins), and
- Whether there will ever be a total supply, or will it be ever increasing (inflationary)

5. KPIs for assessing digital currencies

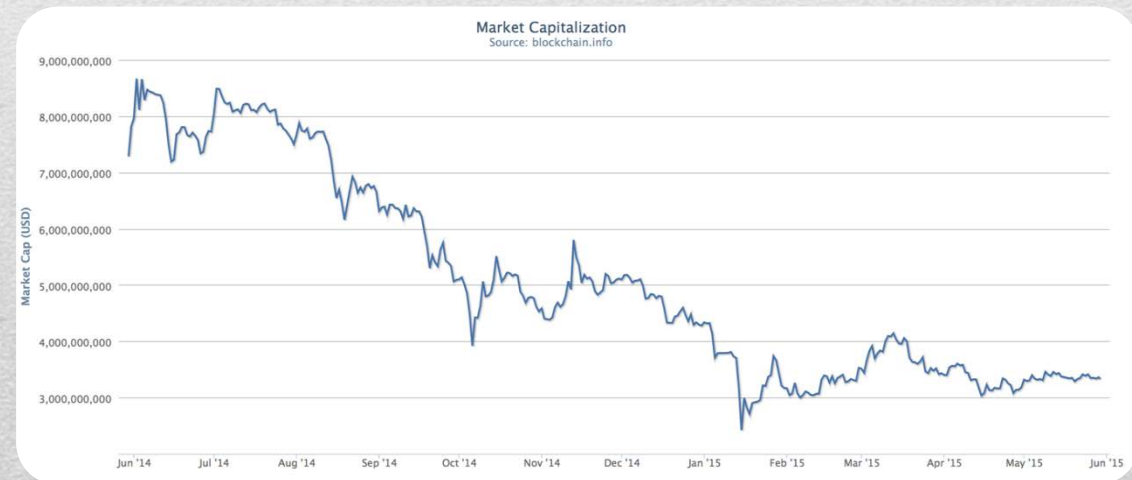
KPIs for assessing digital currencies

This section is devoted to providing the reader with the most important Key Performance Indicators (KPIs) to have in mind when evaluating digital currencies.

Market capitalization: This metric refers to the aggregated value of a coin and its penetration “in the market” of digital currencies. This is a metric that gives us a snapshot, an indication for the present state of each coin compared to major conventional currencies. This reflects a momentarily impression and provides information for the history.

With regards to market capitalization of all coins you can visit

coinmarketcap.com, whereas you can see the Bitcoin market capitalization at: blockchain.info/charts/market-cap

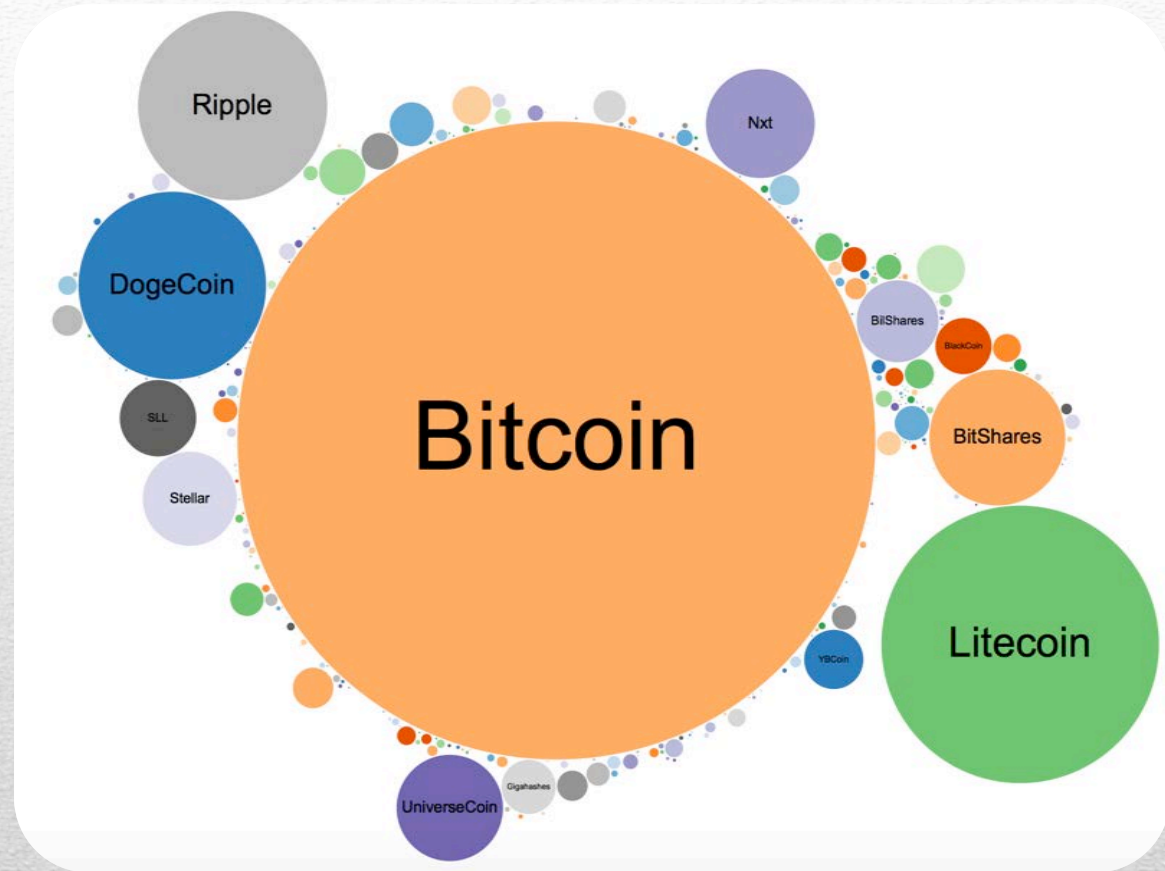


KPIs for assessing digital currencies

Trading volume: This metric expresses the total number of transactions taking place with the use of a particular currency. This volume is measured in BTC for the following chart.

Again, a metric that depicts the as-is situation of a particular day and changes in time.

The graphs depict the total trading volume sum of all exchanges in digital currency for one day of May, 2015.



Source : <http://www.cryptocoincharts.info/coins/graphicalComparison>

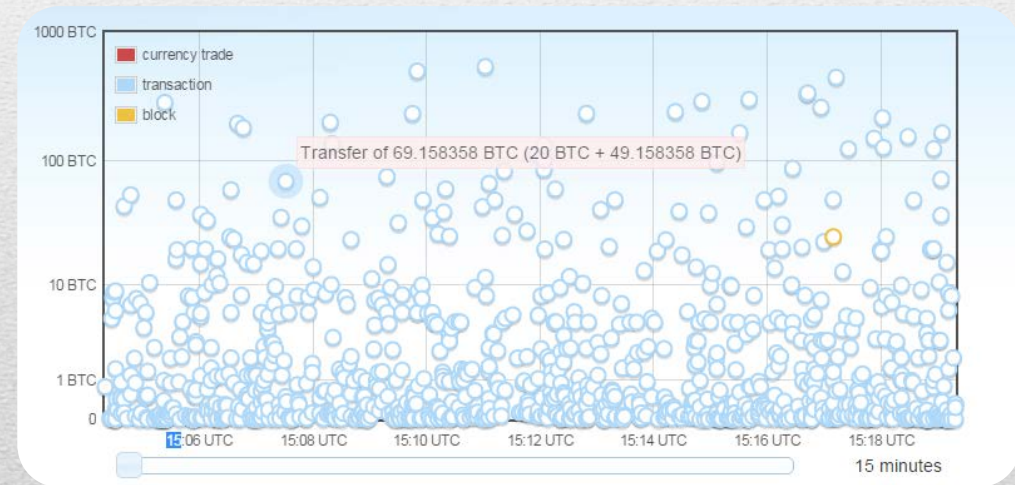
KPIs for assessing digital currencies

Transaction volume, by number of transactions and currency amount

Another way of drawing insights from the dynamics of each network is the number of transactions happening over time, as well as the amount of coins that are involved in them.

bitcoinmonitor.com is an online monitoring tool that visualizes the activity on the Bitcoin network in real time.

In this bubble graph we can see the transactions happening in real time, correlated with their size, i.e. amount transferred – measured in a logarithmic scale.



We can also refer to the absolute [number of daily transactions](#) or the [daily transaction volume](#) as provided by blockchain.info.

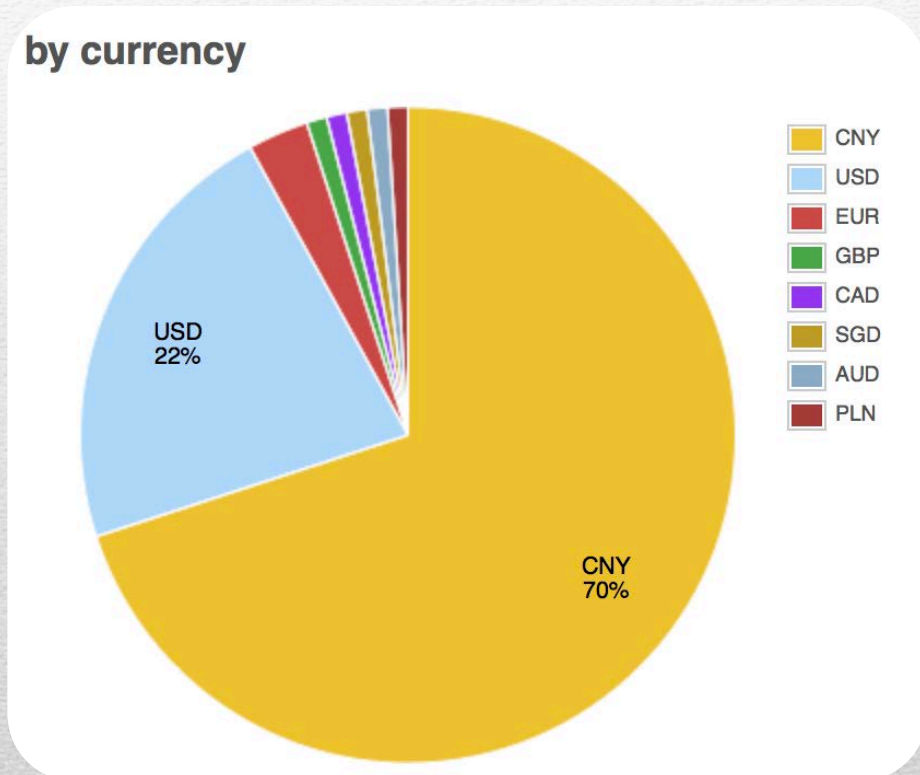
KPIs for assessing digital currencies

Exchange rate: Another important measure to consider is the exchange rate of a coin with fiat currencies.

The pie on the left shows the exchange volume distribution of Bitcoin in the last few days.

Moreover, we have to consider that there are multiple exchanges, each one maintaining a slightly different exchange rate.

bitcoincharts.com can provide us with a platform with rich information, aggregated or not, about the way differences in prices of bitcoin develop in time and for every currency in every exchange center.



Source: bitcoincharts.com/charts/volumepie

KPIs for assessing digital currencies

Average confirmation time: What is also important to know for a digital currency is the average time frame within which a confirmation is attained (block times).

Litecoin came out as a faster alternative to Bitcoin, with block times in the range of 2.5 minutes. The initial choice of 10 minute blocks aimed for a full propagation of every new block and every transaction through every node. Most other altcoins have toyed with the confirmation time, as a key differentiator, bringing it down to a few seconds.

Decreasing block times has been argued to create a higher probability of orphan blocks in their respective blockchains, and a perhaps unfair disadvantage to miners that are late to receive new blocks.

A review of the arguments for and against different confirmation times can be found [here](#).

KPIs for assessing digital currencies

Network hash rate: This metric refers to the measuring unit of the processing power of the network and can give us an indication of the current status of the difficulty in the mining process.

Difficulty refers to how easy it is to generate a SHA-256 hash for a candidate block, that is in accordance with the requisites defined by the current difficulty.

The graph on the right shows the way the hash rate of the network has performed in the last **2 months**. Despite fluctuations, we can see that there is an increasing trend.

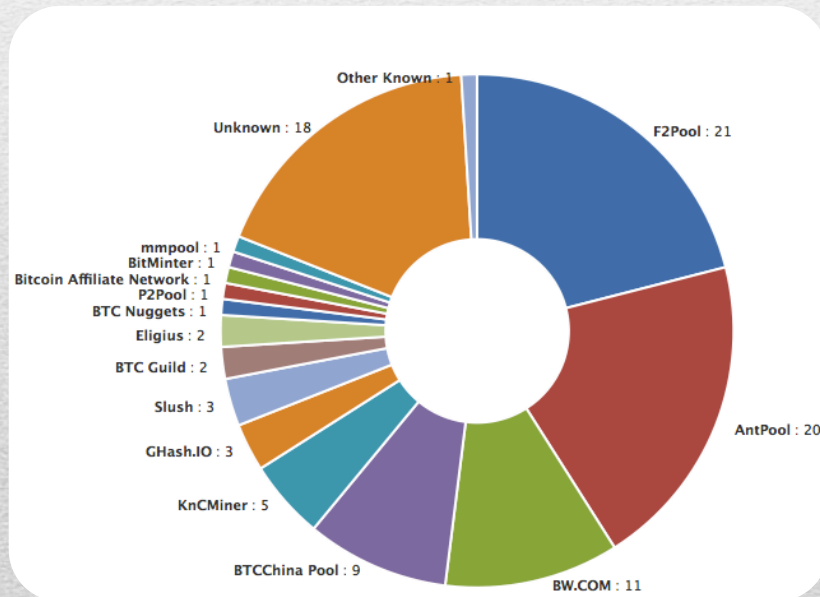
Regarding the way that this metric is calculated, there is an interesting discussion analyzing the above on bitcointalk.org.



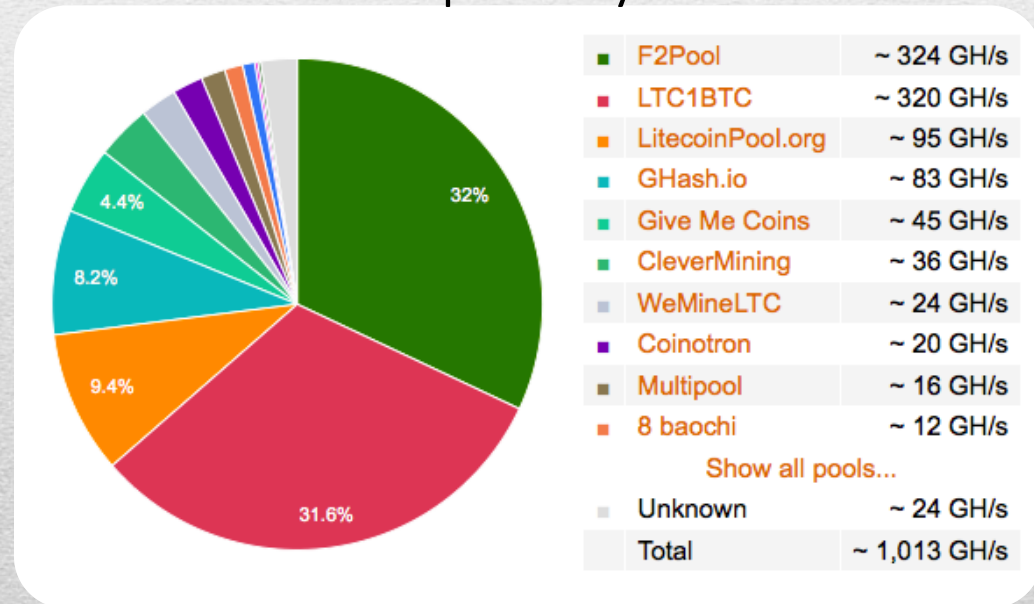
KPIs for assessing digital currencies

Hash rate distribution: A pie graph like the ones below shows the most popular mining pools and their contribution to the whole network at a single point in time.

This metric, again, is just a static picture and should be used as a quick indication of the attractiveness of different mining pools. For instance, below we can see the distribution of hash rate among different pools recently, for Bitcoin and litecoin respectively.



Source: blockchain.info/pools

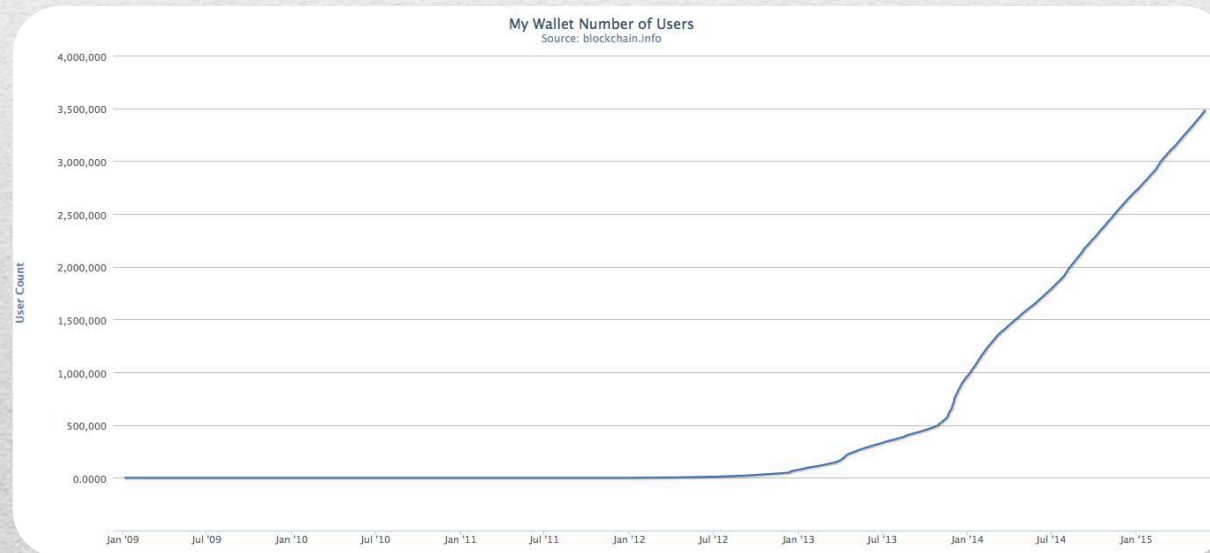


Source: litecoinpool.org/pools

KPIs for assessing digital currencies

Arguably though, the most important indicator of any currency with the characteristics of an international, borderless and voluntary is **user** and **merchant** acceptance and adoption.

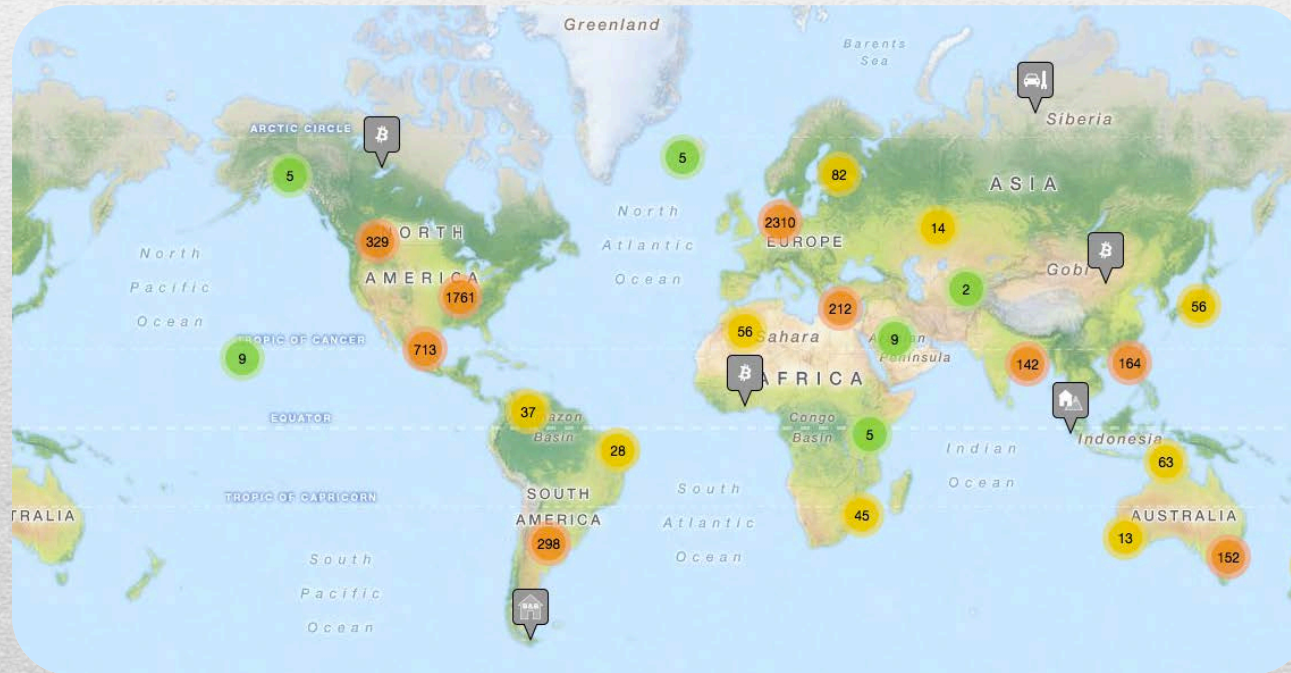
Number of Users: The number of users can only be approximated, by the number of downloads of the wallet software, when that is available, or the numbers of wallet creation from providers. Users can have any number of wallets, from any provider, so these number can never be absolute, even when not counting exchange wallets, paper wallets, brain wallets, etc.



Source: <https://blockchain.info/charts/my-wallet-n-users>

KPIs for assessing digital currencies

Merchants Acceptance: While merchant acceptance does not again provide absolute data on the adoption of a single digital currency, it is an indicator towards its wider adoption, which in turn is a comparable indicator between digital currencies. For Bitcoin, several projects list businesses accepting bitcoins including the [wiki](#) and [coinmap.org](#), which lists a large number of physical businesses accepting Bitcoin.



6. Conclusions

Conclusions

- A large number of alt-coins exist, as alternative digital currencies to Bitcoin, which at the moment holds the leading position.
- There are numerous aspects that differentiate among different alt-coins.
- We can use several criteria to categorize alt-coins in groups, such as whether they follow the “*Proof-of-work*” or “*Proof-of-stake*” scheme (or any other from the ones described) or whether they are pre-mined, minable or not.
- There are some important key factors to keep in mind when assessing one digital currency over another.

7. Self-Assessment Exercises and Further Reading

Self-Assessment Exercises

Discuss in the appropriate thread in the forums:

1. Given that Bitcoin can change by consensus if other innovative concepts come along, do we really need so many different alt-coins, especially if sidechains (session 6) are implemented?
2. We could argue that Bitcoin has a “*first mover*” advantage in the field. Is there anything to indicate that it might or might not be surpassed by alternatives like we’ve seen many times before (Netscape and Firefox, Yahoo and Google, Myspace and Facebook)?
3. What other KPIs do you find proper and helpful, with regards to assessing alt-coins?
4. Recently, Ripple has climbed significantly in market capitalization. What do you believe would happen if the market capitalization surpassed that of Bitcoin, in the next months?

Further Reading

List of crypto-currencies

https://en.bitcoin.it/wiki/List_of_alternative_cryptocurrencies

Criticism on alt-coins

<http://themisescircle.org/blog/2014/03/14/the-coming-demise-of-the-altcoins/>

<http://themisescircle.org/blog/2013/08/22/the-problem-with-altcoins/>

Interesting articles on the role and future of altcoins

<http://bitcoinmagazine.com/13150/role-future-altcoins/>

<http://bitcoinmagazine.com/11125/asics-litecoin-come/>

<http://letstalkbitcoin.com/e99-sidechain-innovation/>

Questions?



Contact Us

Email:

dc@unic-online.com

Twitter:

@MScdigital