UNIVERSITY *of* NICOSIA

MSc in Digital Currency

Introduction to Digital Currencies

DFIN-511

Introduction to Digital Currencies

Session 7: Alternatives to Bitcoin

UNIVERSITY of NICOSIA

Session Objectives

- 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” (with about 50% of the total space market capitalization) 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 Session 7

- Why alternative currencies?
- Indicative alternatives
- Common characteristics
- Criteria for categorization
- KPIs for assessing digital currencies
- Permissioned Ledgers and Private Blockchains
- Conclusions
- Further Reading

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 (approximately 135GB) – and will only become larger, as Bitcoin use becomes more widespread.
- The process of mining is power intensive, which may be argued is with a disproportionate benefit towards the network, unless this is mutualized to many more transactions.
- The nature of a predetermined, and eventually deflating monetary base as coins are irrecoverably lost, may also be among the dissuading factors of some using it.

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 and MaidSafe) 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
  - Adding more functions like smart contracts
  - Improving fungibility and the privacy characteristics of the currency itself
  - 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

Indicative alternatives

Indicative alternatives

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

- The so called “market cap” (available supply*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, availability of coins in the market, 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	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$76,154,665,333	$4584.12	16,612,712 BTC	$1,461,000,000	2.94%	
2	Ethereum	$28,964,571,475	$304.82	95,021,575 ETH	$370,567,000	-1.97%	
3	Ripple	$10,314,005,613	$0.267222	38,597,142,499 XRP *	$687,715,000	10.47%	
4	Bitcoin Cash	$5,651,943,611	$338.89	16,677,763 BCH	$250,021,000	-5.95%	
5	Litecoin	$2,767,693,504	$51.93	53,296,107 LTC	$120,041,000	-0.93%	
6	Dash	$2,265,476,933	$297.68	7,610,521 DASH	$43,132,400	-4.94%	
7	NEM	$1,781,910,000	$0.197990	8,999,999,999 XEM *	$6,300,300	-5.35%	
8	NEO	$1,522,790,000	$30.46	50,000,000 NEO *	$114,108,000	-15.60%	
9	IOTA	$1,358,809,513	$0.488863	2,779,530,283 MIOTA *	$9,196,220	-8.36%	
10	Monero	$1,344,081,794	$88.46	15,193,734 XMR	$32,135,800	-3.26%	

source: coinmarketcap.com, as of October 2017

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 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 Ethereum, Monero, NXT or Ripple).

- 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), it is used more as computational fuel than a scarce currency:
  - 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 (100), (b) Szabo (1012), (c) Finney (1015), to (d) Ether (108), 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 without the UTXO basis we saw in Bitcoin. 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.
- Applications on Ethereum have been dubbed as Dapps (decentralized applcations)

Ethereum, progress so far

- Ethereum is so far, one of the most highly crowdfunded project globally, gathering a staggering 31,529.49449551 BTC by September 3rd 2014 (address). Total amount of Bitcoins received as of October 2017 is 31,549.8865212 BTC

- To perform everything the team is poised for, in a scalable and secure manner is a very tall order in itself. Several implementations of the Ethereum VM already exist, including C++, Go, Java, Python, Javascript, Haskell bkirwi& jamshidh , Node, .NET

- Homestead is the second release of the Ethereum project, moving beyond developers and to the mainstream, after the successful hard fork towards it. This is not to be confused with the DAO sustained hard fork which happened later, and resulted in two version of the protocol and two chains (ETH and ETC).

- 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.

The world computer?

- While Frontier allowed only for command line, the first production release of Ethereum called Homestead was recently released via a hard fork of the blockchain, and it allows users to build more on the platform. More information on the improvements of Homestead can be found here
- A private version of the Ethereum network served as the platform for the first major test conducted by blockchain consortium startup R3CEV in January, 2016, with the trial uniting 11 major banks in a high-profile proof-of-concept. Several proof of concept decentralized Applications (dapps) are available here.
- More resources and use cases are springing daily, making the Ethereum blockchain grow far faster than Bitcoin's ever has. In July 2017, it surpassed the Bitcoin blockchain by 40%, although some differences apply (state transitions, each implementation can choose how to store data, etc).
- Several very novel approaches are being implemented in Ethereum, including an improved version of the GHOST protocol to decrease block times, and the transition to a Proof of Stake (detailed later in this session) called Casper. We can expect to see more interaction with the Bitcoin ecosystem as wallet building, processing and more exchanges adding the tradeable underlying token in the future.
- In Feb 2017, a consortium of large companies including JPMorgan, Intel, Microsoft And Others formed the Enterprise Ethereum Alliance, which aims at creating a standard version of the Ethereum software that businesses around the world can use to track data and financial contracts.

The DAO hack and the ensuing fallout

- "The DAO" (Decentralized Autonomous Organization) had a formidable calling, to create the first decentralized crowdfunding platform, a place where investors would have proportional decision making ability on the investment of funds which a decentralized organization held. At its height it gathered about $160 million (at that time), and became the largest crowdfunded project ever.
- Despite criticism on the "too much, too fast, too early" nature of the project while it was starting, it went on, and on Friday June 17th 2016, an attacker syphoned about $50 million worth of the native tokens away. The exploit used was suggested as an attack vector before, and was even, reportedly, fixed.
- The proposed solution by the ETH community was a hardfork to remove the funds from the attacker. This caused a split in the community as not everyone was in favor of "bailing out" the DAO since it was a construct on ETH and not an ETH vulnerability itself. This led to a hard fork and the creation of two Ethereum blockchains. The majority one (retained the Ethereum name) and the minority one was named Ethereum Classic. A comparison at the current status of each chain can be found here.
  - Some further reading :

    https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/

    http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/

Monero, a short introduction

- Monero launched on April 2014 as a fork of Bytecoin. Bytecoin was an obscure cryptocurrency that, while having pioneered a novel way to achieve privacy, was plagued with a shady history and an unfair launch. As a result, the community forked the code of Bytecoin and began a long, multi-year project of cleaning it up, documenting it, and getting the fundamental aspects of it right.
- Monero focuses on providing strong privacy by default while offering optional transparency, allowing its users to selectively disclose their transactional history to selected parties. Privacy is inherent to the protocol and requires no additional steps (interactivity) from the user. As a result, fungibility is greatly improved as well.
- Monero's architecture provides a clear separation of the node functionality and the wallet. Originally having just a command line wallet, which was deemed too difficult for non-technical users to use. The second beta of Monero's Graphical User Interface (GUI) was released in late March 2017.
- Apart from its novel privacy features, Monero offers several improvements as compared to Bitcoin, both in its core cryptography (like using the ECDSA Curve25519 made by renowned cryptographer Daniel J. Bernstein and Schnorr signatures) as well as its interesting economic aspects, such as having a dynamic block size and fee system, and a constant tail emission of coins corresponding to a yearly inflation rate of around 1%.

Monero, Privacy and Fungibility

- In Bitcoin, transactions are traceable as the transaction graph is visible in the blockchain; sender and recipient addresses as well as transaction amounts are visible. This makes Bitcoin vulnerable to coin tainting and susceptible to blockchain analysis, thus potentially significantly reducing its fungibility and usefulness as digital cash (which should be indiscernible from any other coin). Various techniques have been proposed and utilized to improve Bitcoin's privacy, however they either suffer from having to trust centralized services (coin mixers) of dubious quality and legal status, or from requiring manual user intervention and coordination (such as CoinJoin).
- Providing privacy and fungibility by default is considered a core tenet of the Monero project. Monero obscures the transaction graph and hides transaction amounts by a combination of Ring Signatures and Confidential Transactions, and hides user addresses via the use of Stealth Addresses.

Monero, Ring Signatures

- Monero originally used two techniques to make blockchain analysis difficult: Ring signatures and Stealth Addresses.

"A ring signature is a type of group signature that makes use of your account keys and a number of public keys (also known as outputs) pulled from the blockchain using a triangular distribution method…In a "ring" of possible signers, all ring members are equal and valid. There is no way an outside observer can tell which of the possible signers in a signature group belongs to your account similar in function to a bank account, contains all of your sent and received transactions"
Source: https://getmonero.org/resources/moneropedia/ringsignatures.html

- Ring Signatures obfuscate the transaction graph by associating each transaction input to not just one but many possible and equiprobable outputs. This number of possible outputs is called the Ring Size of the transaction; the minimum Ring Size is currently 2, soon to be raised to at least 4. This process is constant and no manual user intervention is needed.
- Monero also hides recipient addresses by using Stealth Addresses. While the recipient can always give the same address to every sender, this address is used to generate a different, one-time address to use each time a transaction is made. Thus, the recipient's address never appears on the blockchain, and transactions are unlinkable, as nobody can prove that two transactions have the same recipient.
- Originally, transaction amounts were visible in Monero's blockchain. However, in January 2017 a hard fork was performed that upgraded the Monero protocol to utilise a new scheme, Ring Confidential Transactions, that combines Ring Signatures with Gregory Maxwell's "Confidential Transactions" scheme. This evolution allowed the obfuscation of the transaction amounts as well, which means that Monero's blockchain is opaque at this point.

Monero, other distinguishing features

- Monero is a relatively young project. Having a completely different code base than Bitcoin enhances the diversity of the system, but significantly increases the difficulty of integrating Monero into services that have already implemented Bitcoin integrations.
- Monero offers a dynamic block size (one of the developers discusses their interesting approach here) and a dynamic fee system, in effect making the system more robust by automating basic parameters of the system, as well as providing a more flexible cryptocurrency protocol.
- Monero is currently upgraded regularly by scheduled hard forks, which makes it able to evolve and adapt quickly at its current stage. However, hard forks come with their own disadvantages as well, and this matter will be regularly revisited as Monero's user base grows and requires more stability and longer support periods.
- Monero is closely related to the Kovri project, which implements an I2P client in C++. Once it is production-ready and integrated into Monero, Kovri will also help obfuscate user and node IP addresses, making it less susceptible to network metadata analysis.
- Monero transactions are an order of magnitude larger than Bitcoin's, which makes it significantly less scalable on-chain and accelerates the need for off-chain solutions such as Lightning Network or Sharding.

Monero

- Monero is still a young currency (and mostly under the radar so far) but one that's trying to solve a very major problem that is needed for a decentralized digital currency to be widely used. Here's an interesting early discussion on the topic with Satoshi Nakamoto discussing the potential of Ring Signatures : https://bitcointalk.org/index.php?topic=770.msg9074#msg9074
- We shouldn't be making the mistake of saying that we don't need increased privacy because we have nothing to hide. This is a slippery slope to saying we don't need free speech because we may have nothing to say, or the equivalent of permanently removing the shutters/blinds from our house. Fungibility and privacy are important enough topics for Bitcoin as well, since they took the central stage at the recent Scaling Bitcoin conference in Milan. It's a tricky problem and one that involves complicated cryptographic schemes that are understood by few (so far), and are not very accessible to the average user, without a practical way to hide the complexity.
- You can read more about it, and its features in more detail here : https://getmonero.org/home

Bitcoin Cash

- On August 1, 2017, bitcoin went through a hard fork which gave birth to Bitcoin Cash (BCH). Records of existing transaction were kept secure

- Differences with Bitcoin:
  - The blocksize is 8 MB. More transactions in a block can generate more transaction fees for miners. Approximately 2 million transaction per day can be processed compared to 250k transactions which Bitcoin allows.
  - No segwit activation.
  - No “replace by fee” feature.
  - It will enhance replay and wipeout protection.
  - It offers a way to adjust the proof-of-work difficulty quicker than the 2016 block difficulty adjustment interval of Bitcoin.

- Anyone with the possession of Bitcoins at the time of the hard fork, got the equal amount of coins in Bitcoin Cash. This was applicable provided that users did not have their Bitcoins in exchanges and were in possession of their private keys at the time of the hard fork.

Bitcoin Cash

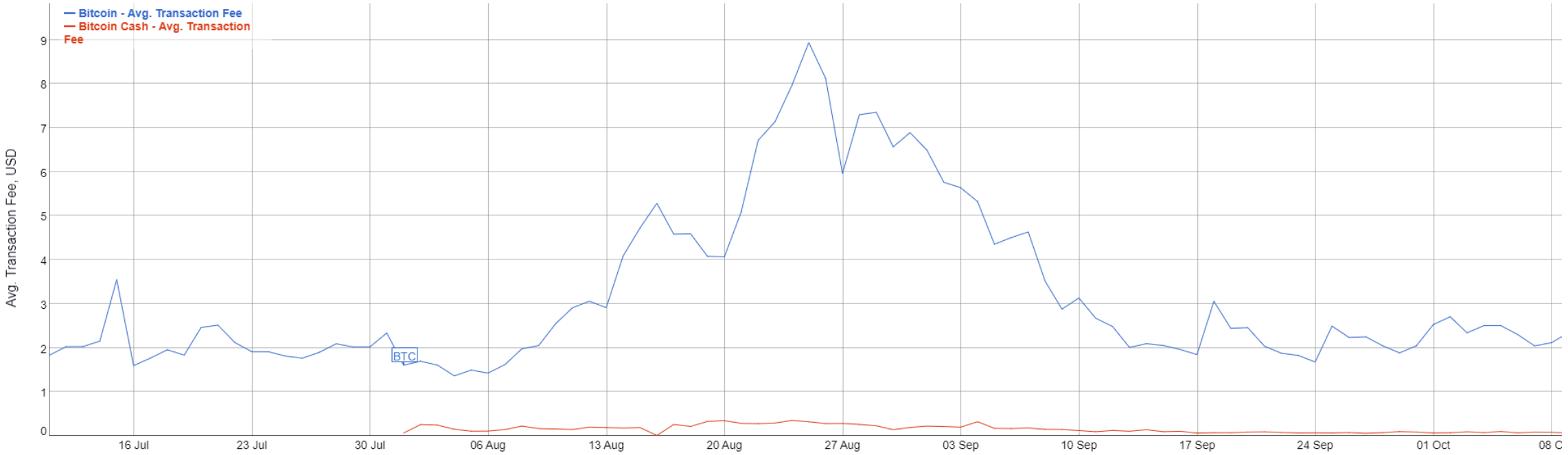
- BCH is currently (October 9, 2017) traded at $339, which makes it the second most expensive cryptocurrency behind BTC, even though it faced a significant drop in value from $914 (August 19)

How does Bitcoin Cash prevent replay attacks?

- A replay attack occurs when data are maliciously repeated or delayed in multiple locations.
- In the case of a blockchain, an example would be a transaction that happens on the Bitcoin blockchain and repeated on the Bitcoin Cash blockchain. E.g. Andreas sends 1 BTC to Antonis, as well as 1 BCH, even though this was not his intention.

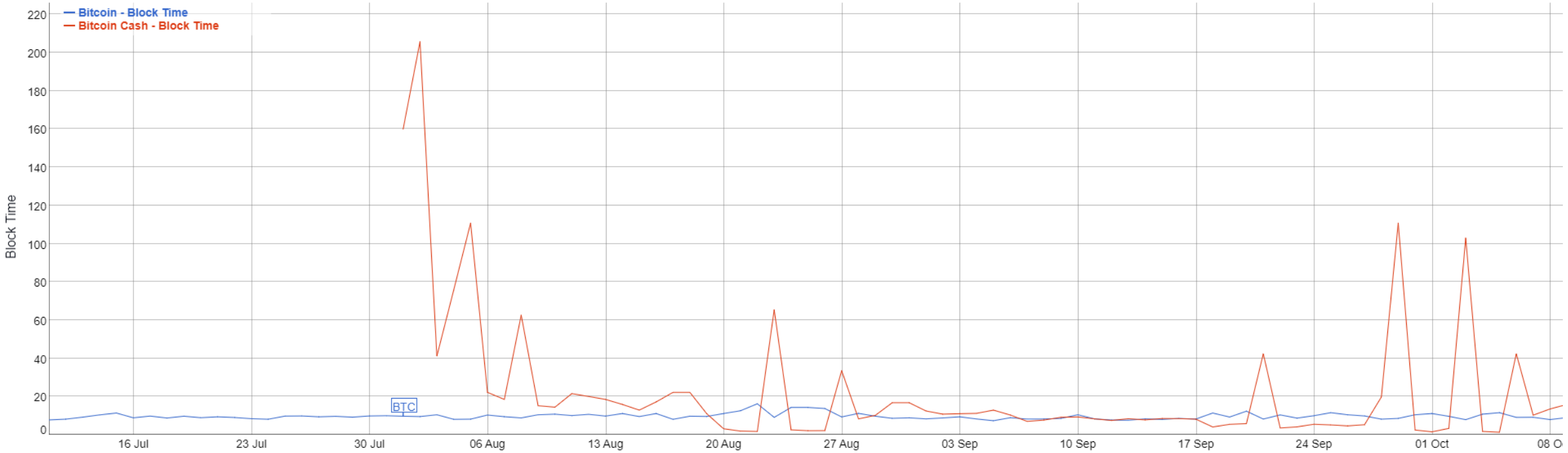
- Bitcoin Cash achieves this by (Source: https://blockgeeks.com/guides/what-is-bitcoin-cash/):
  - *Using a redefined sighash algorithm. This sighash algorithm is only used when the sighash flag has bit 6 set. These transactions would be invalid on the non-UAHF chain as the different sighashing algorithm will result in invalid transactions.*
  - *Using OP_RETURN output which has the string "Bitcoin: A Peer-to-Peer Electronic Cash System" as data. Any transaction which contains this string will be considered invalid by bitcoin cash nodes until the 530,000th block. Basically, before that block you can split your coins by transacting on the non-UAHF chain first with the OP_RETURN output, and then transacting on the UAHF chain second.*

Bitcoin vs Bitcoin Cash Average Transaction Fees



Source: https://bitinfocharts.com/

Bitcoin vs Bitcoin Cash Block Time



Source: https://bitinfocharts.com/

Initial Coin Offerings (ICOs)

- ICO is a method of raising funds used by cryptocurrency/blockchain-based startups. The new cryptocurrency created by the startup is sold to parties willing to invest in the project, in exchange usually for Bitcoin or Ethereum.
- The new cryptocurrency is expected to be used in the applications of startups. If the project succeeds, the investors gain accordingly as the new cryptocurrency appreciates in value.
- ICOs can bypass complex regulatory requirements required by banks and official authorities in traditional capital raising processes e.g. IPOs
- Investors actually receive tokens which are then listed and traded on private exchanges (the equivalent of NASDAQ for tokens)
- Ethereum is an example of a successful ICO project

The ICO Process

- Startup companies publish a whitepaper stating what the project is about, the goal of the project, the amount of funds needed to kick start the venture and how many tokens the pioneers of the project will keep in their possession
- Additional provided information include the cryptocurrency accepted and for how long the ICO campaign will run for
- Believers of the startup's project buy an amount of the tokens offered usually in Bitcoin or Ether, similar to shares of a company sold to investors in an Initial Public Offering (IPO)
- There is a possibility that the funds raised do not meet the minimum target funds set beforehand. In such a case, the funds are returned to the investors and the ICO is considered unsuccessful
- TokenMarket is a website you may want to visit regularly in order to stay up to date regarding upcoming ICOs
- Anyone who wants to participate should evaluate the project beforehand in order to draw a fair conclusion regarding its potential.

China ban

- In September 2017, the People's Bank of China officially banned ICOs, labelling it as *"illegal and disruptive to economic and financial stability"*. Warnings have also been issued earlier in 2017, urging the compliance of bitcoin exchanges with *"relevant laws and regulations"*.
- China's central bank banned tokens usage as a currency and forbid banks of offering services related to ICOs. Already established ICOs were also penalized.
- The result of this statement was the fluctuation of bitcoin and ether during the following days and a significant sign that more regulations on cryptocurrencies are coming ahead.

Common characteristics

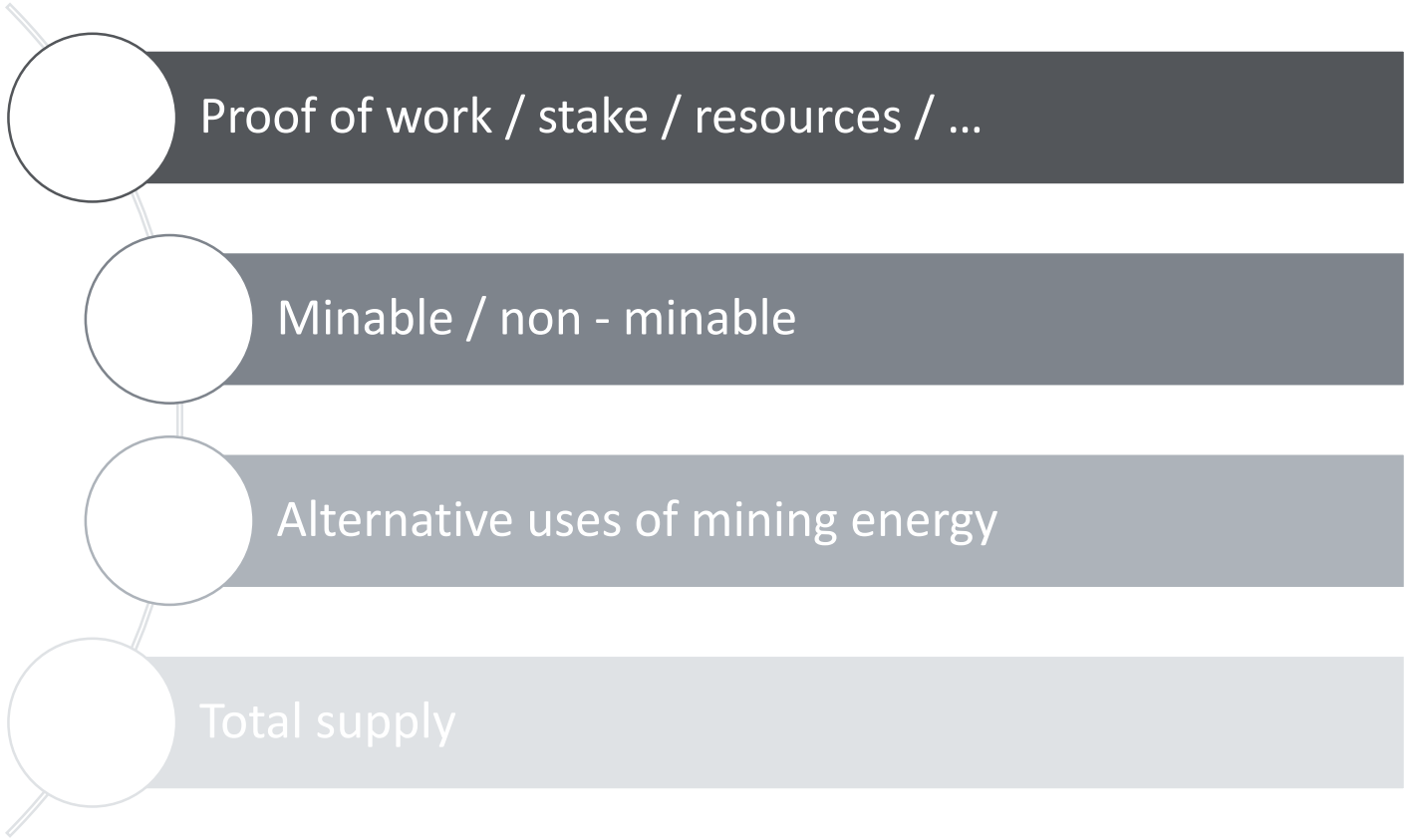
Common characteristics

- 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.

Criteria for categorization

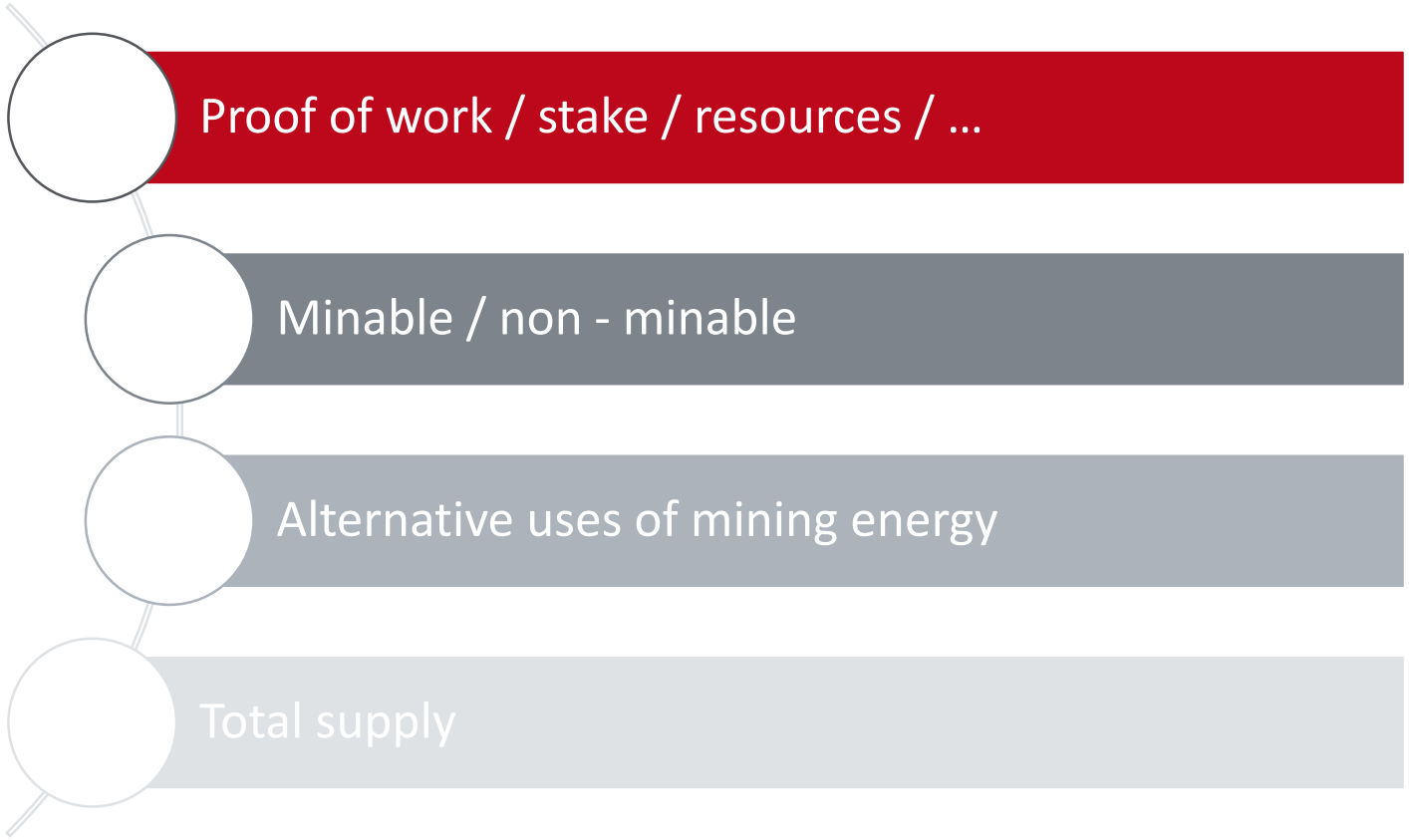
Criteria for categorization

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 through 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.

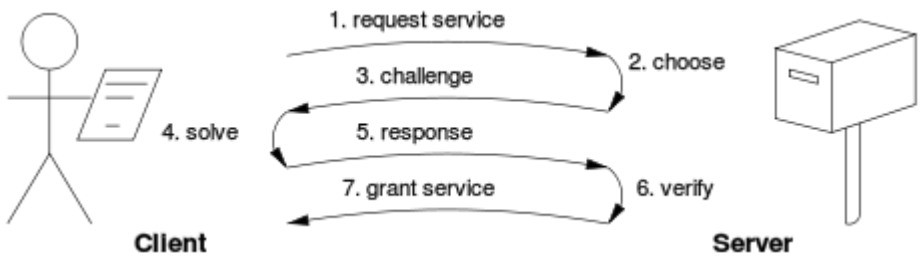
  - Proof of work - mining is required to gain coins, which usually is hash or scrypt based
  - Proof of stake - coins are earned in an order, as a reward for displaying ownership
  - Proof of resources – recognition of contribution of resources to the network
  - Proof of burn – *"bootstrapping one cryptocurrency off of another"*

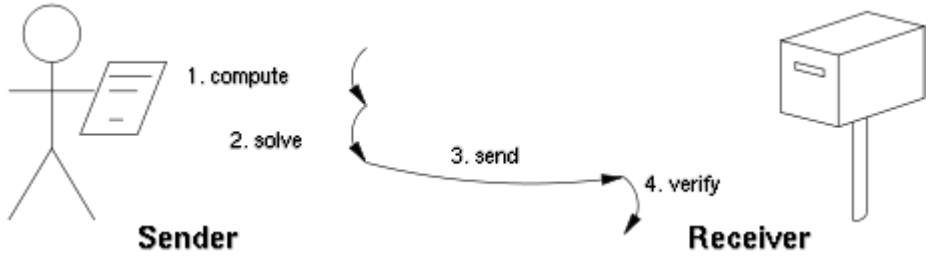
Proof of work (PoW)

- **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 and variations –
  - SHA-256 (Bitcoin)
  - Keccak_256 and Keccak_512 (non standard SHA3 used by Ethereum)
- scrypt algorithm (e.g. Litecoin)
- Hybrid and CPU-only algorithms (e.g. PrimeCoin)
- X11 algorithm (e.g. Dash)
- CryptoNight (e.g. Monero, other Cryptonote coins)

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 the scrypt algorithm:

Litecoin – Novacoin – Worldcoin – Feathercoin

- The scrypt 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. Scrypt 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, 3 if we include iterations of Casper as it may be used in Ethereum:

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.

Proof of Stake (PoS)

- **Proof of stake** - first appearance as a concept:

QuantumMechanic
Member

Activity: 110

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:

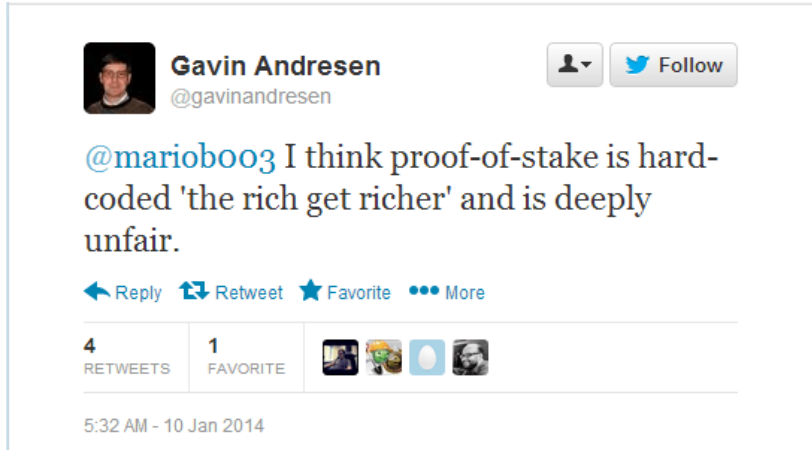
I'm wondering if as bitcoins become more widely distributed, whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources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

- **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/



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

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”

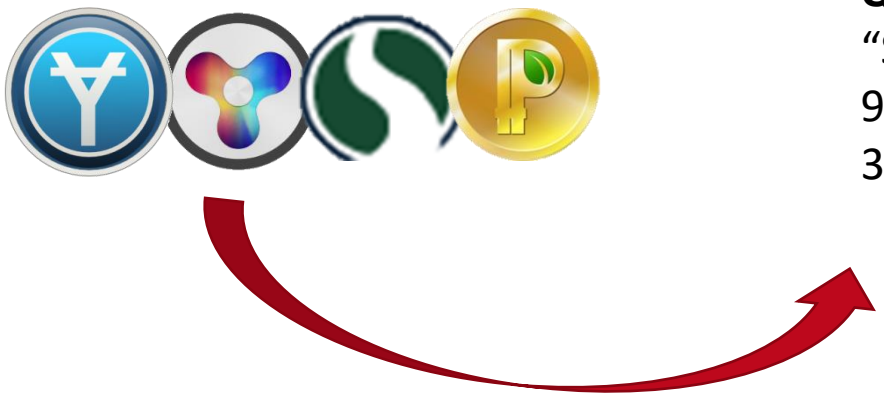
Examples of Coins using Hybrid Algorithms

- Examples of coins using Hybrid algorithm:

Securecoin (cap under 200BTC)
Multiple Algorithms:
Grøstl, Skein, BLAKE, BLUE MIDNIGHT WISH,
JH, SHA-3

Examples of Coins using Hybrid Algorithms

- Examples of coins using Hybrid algorithm:



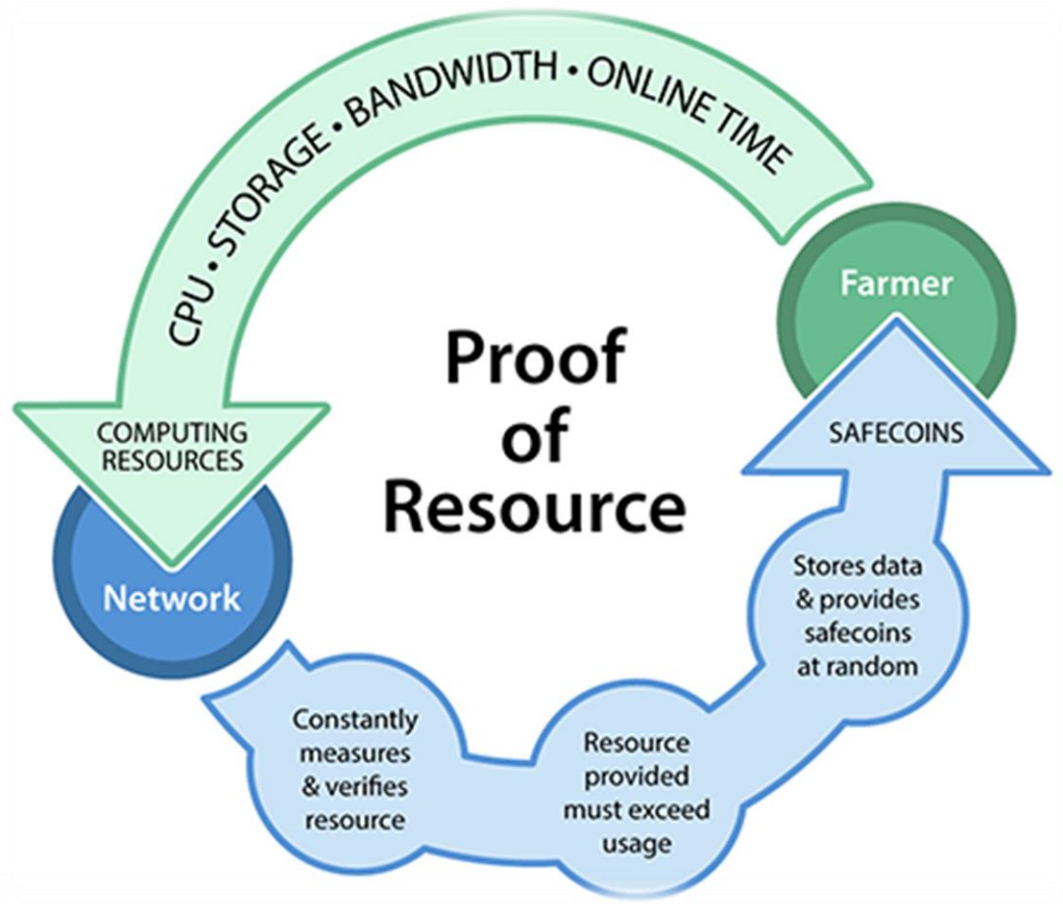
Quark coin (QRK) (Cap at 500BTC)
"Super secure" hashing:
9 rounds of hashing from 6 hashing functions
3 rounds apply a random hashing function.

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.



PoR - Algorithm used for verification / mining

- Examples of coins using PoR algorithms:

safecoin

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.

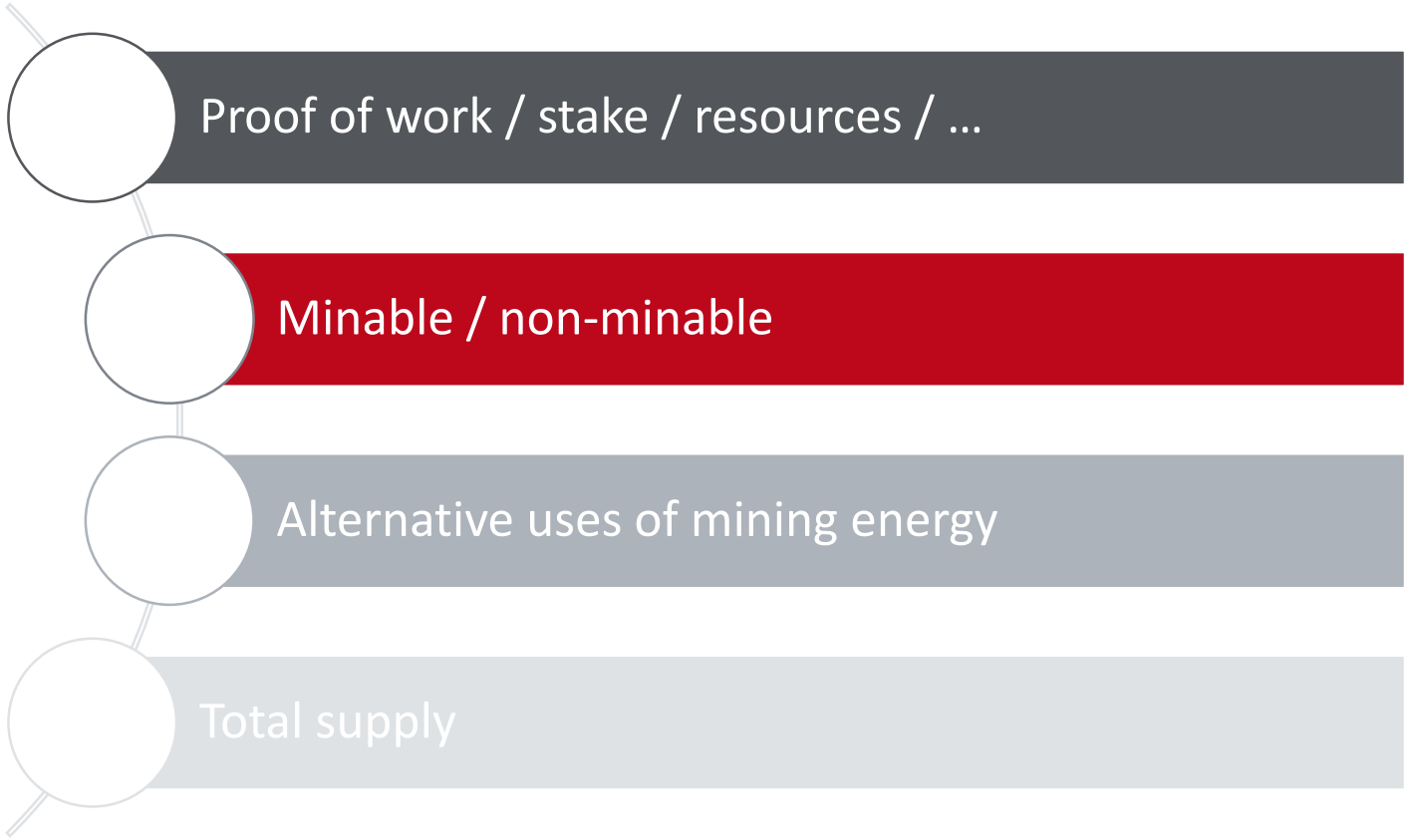
PoB - Algorithm used for verification / mining

- 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).

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.

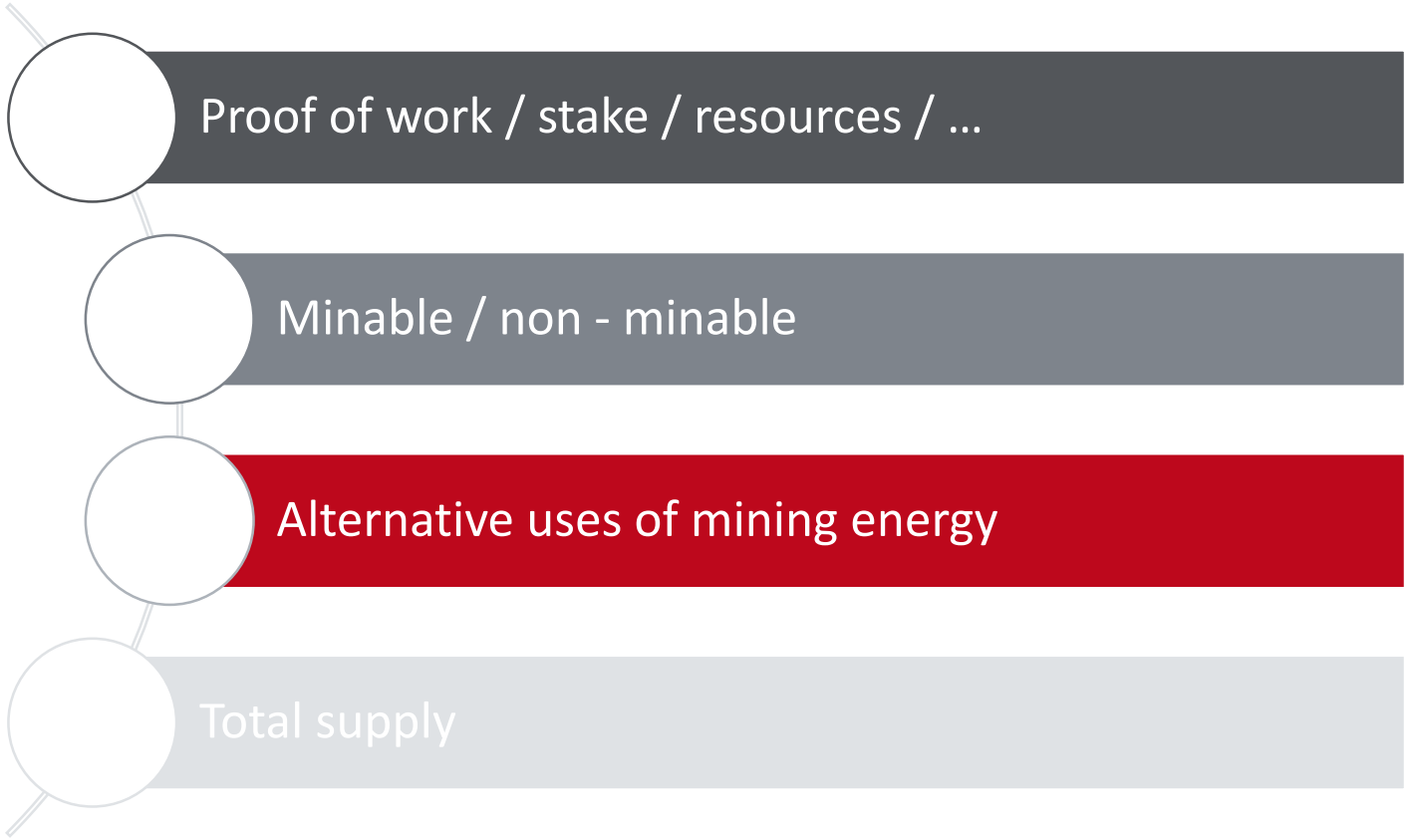
http://bitcoin.stackexchange.com/questions/273/how-does-merged-mining-work

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 and significant funding and several pilot projects with various banks.

Criteria for categorization

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



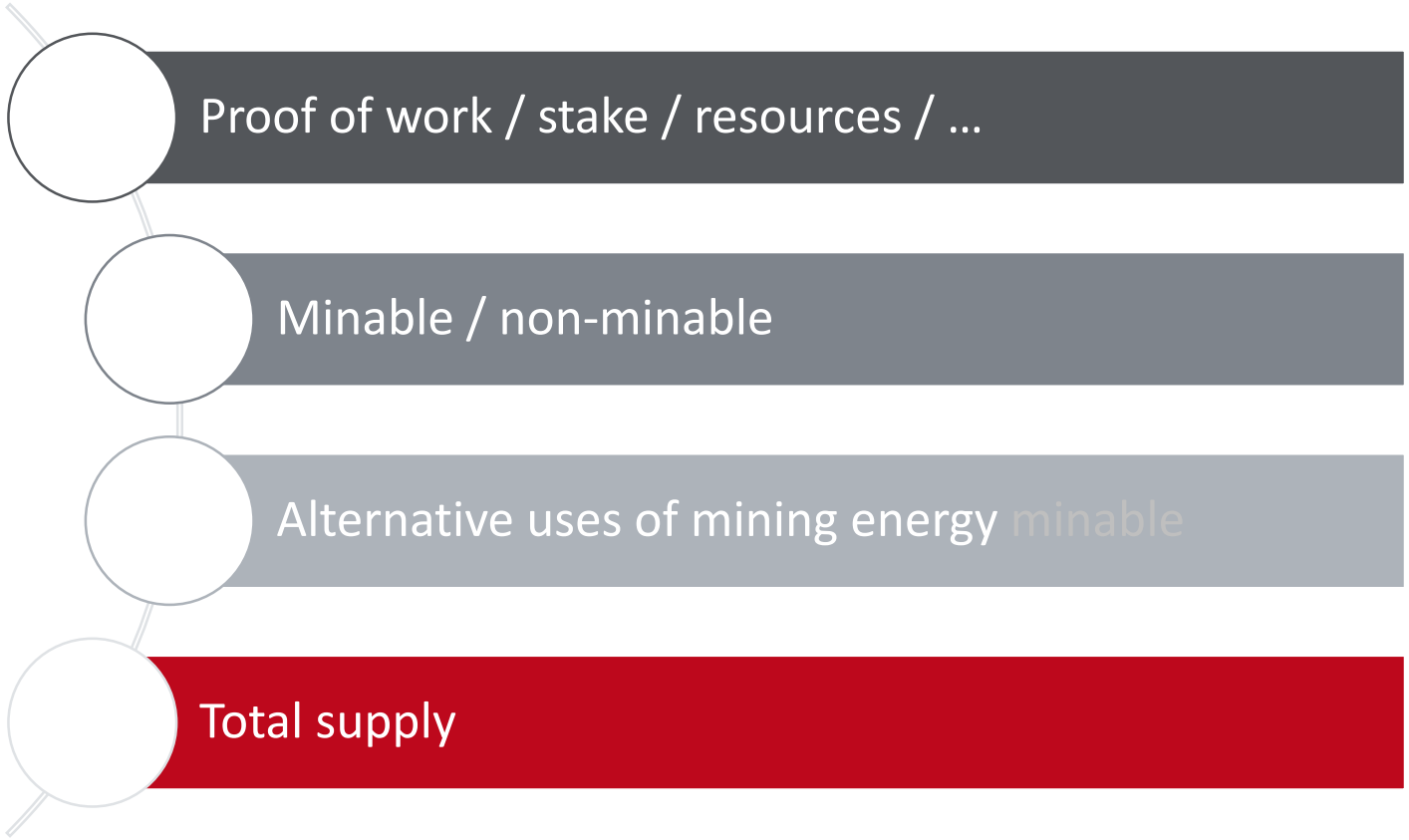
Alternative uses of mining energy

- 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 or tail emissions)

KPIs for assessing digital currencies

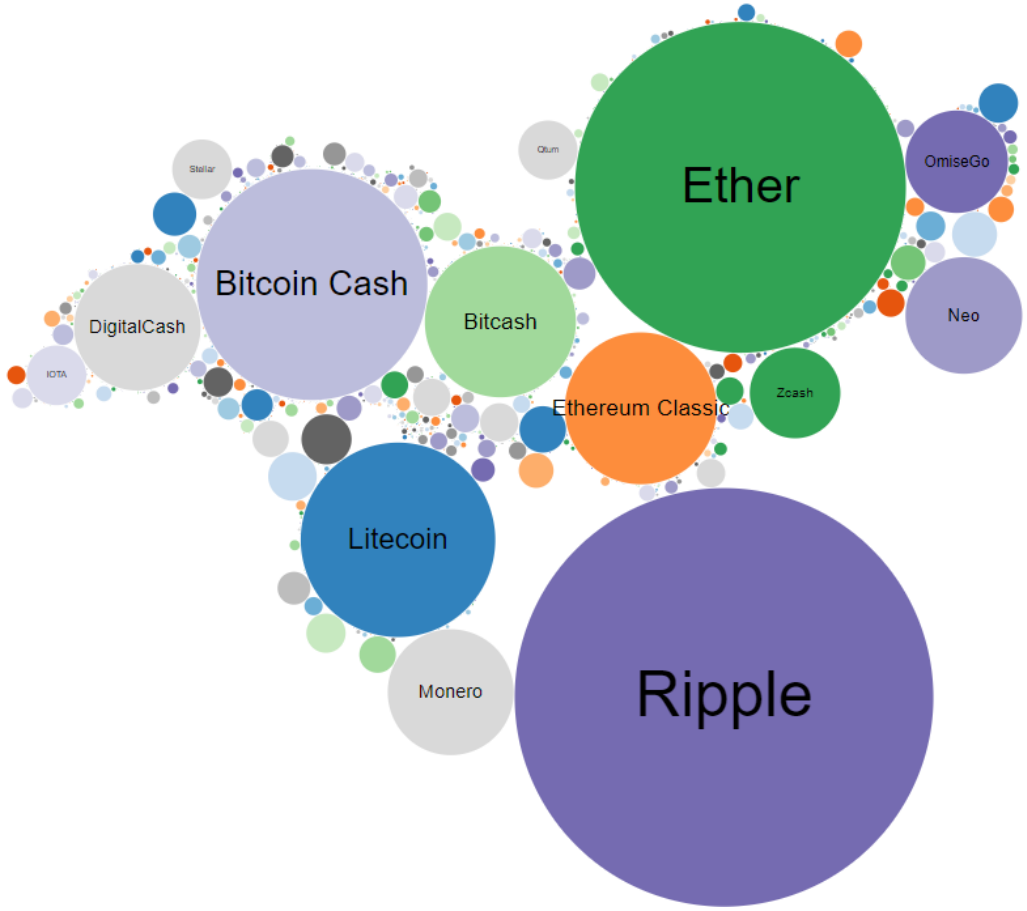
Subtitle (optional)

KPIs for assessing digital currencies

- This section is devoted to providing the reader with suggestions on 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 http://www.coinmarketcap.com, whereas you can see the Bitcoin market capitalization at: blockchain.info/charts/market-cap

KPIs for assessing digital currencies

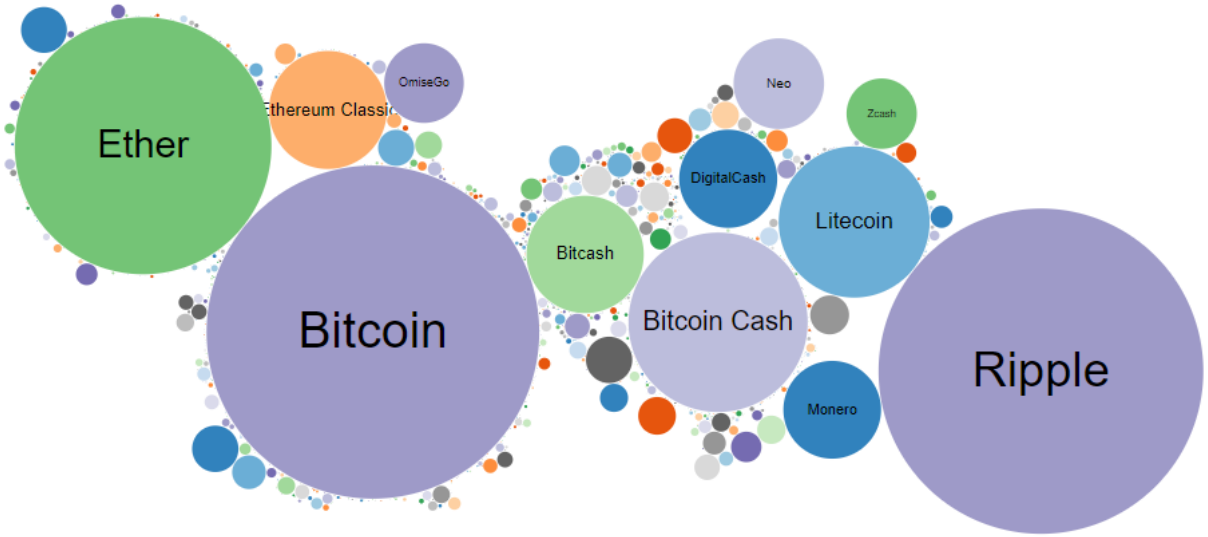
- **Trading volume:** This metric expresses the total number of transactions taking place with the use of a particular currency. This volume is measured in BTC for the following chart.
- Again, a metric that depicts the **as-is** situation of a particular day and changes in time (very often in fact…)
- This graph depicts the total trading volume sum of all exchanges in digital currencies for October 9, 2017 **excluding Bitcoin**



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

Trading Volume

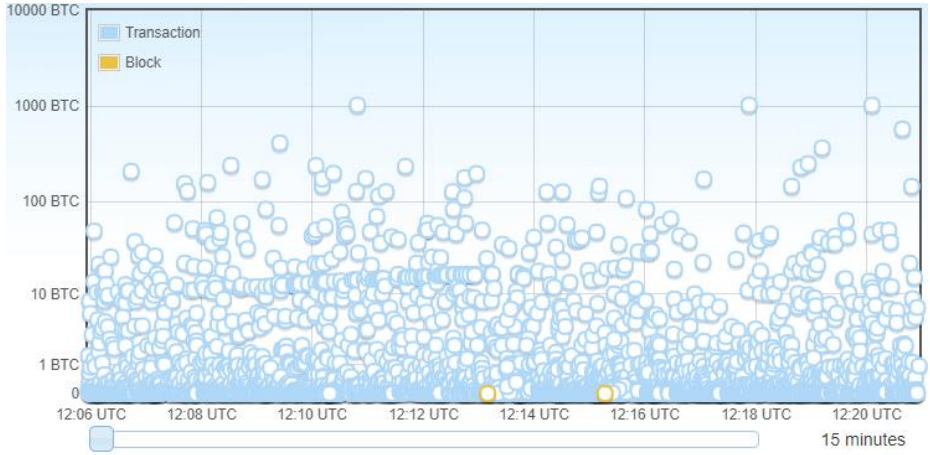
- This graph depicts the total trading volume sum of all exchanges in digital currency for October 9, 2017 including all data available.



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

KPIs for assessing digital currencies

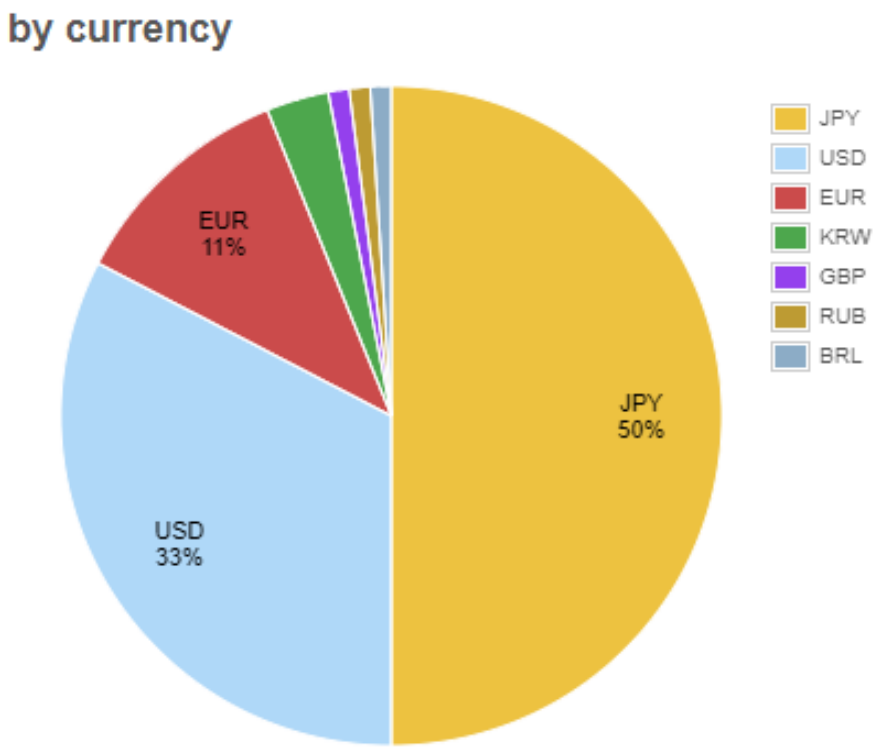
- **Transaction volume, by number of transactions and currency amount**
  Another way of drawing insights from the dynamics of each network is the number of transactions happening over time, as well as the amount of coins that are involved in them.
- bitcoinmonitor.com is an online monitoring tool that 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.
- Before choosing the exchange rate and volumes traded as an indication make sure to know the conditions under which said volume is produced.

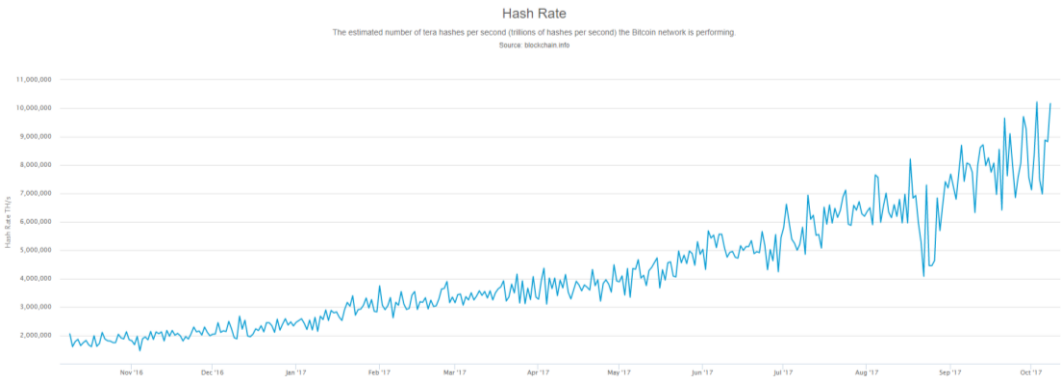


KPIs for assessing digital currencies

- **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, and even Ethereum has a blocktime of about 33 seconds currently.
- Decreasing block times has been argued to create a higher probability of orphan/stale blocks in their respective blockchains (unless something like GHOST or a variant is used like in Ethereum), 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.

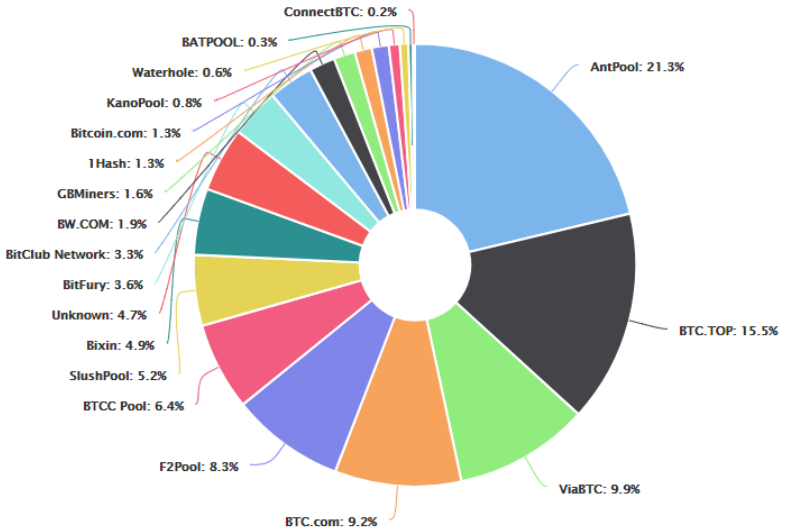
KPIs for assessing digital currencies

- **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 **year.** Despite fluctuations, we can se 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.

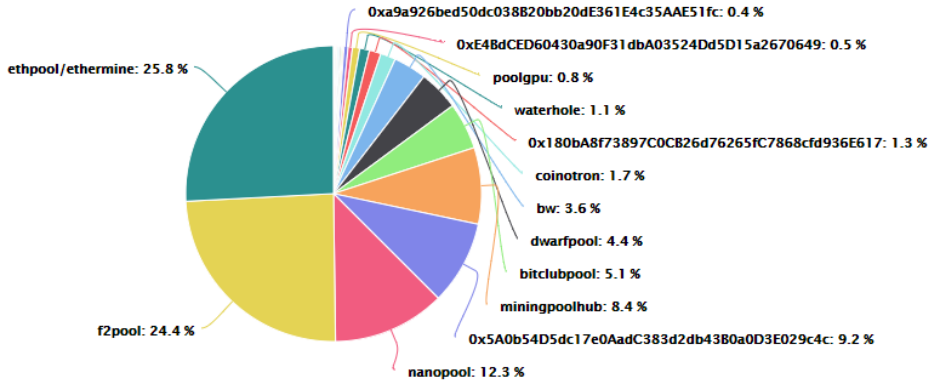


KPIs for assessing digital currencies

- **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 Ethereum respectively.



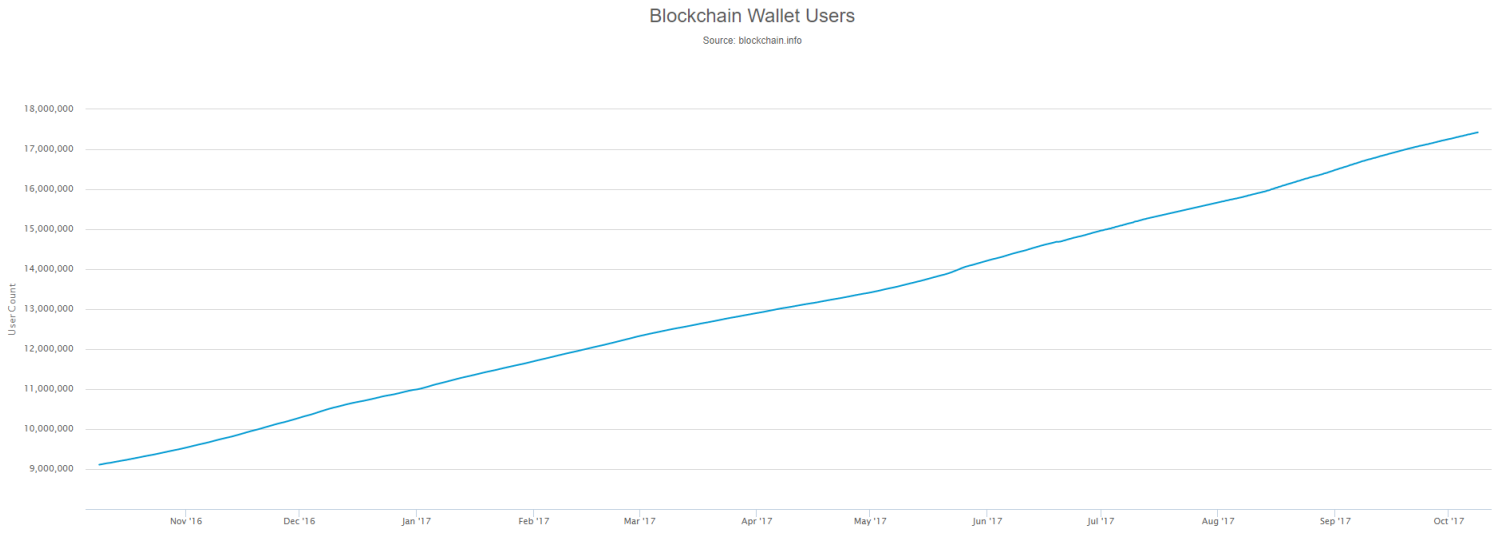
Source: https://blockchain.info/pools?timespan=4days



Source: https://etherchain.org/statistics/miners

KPIs for assessing digital currencies

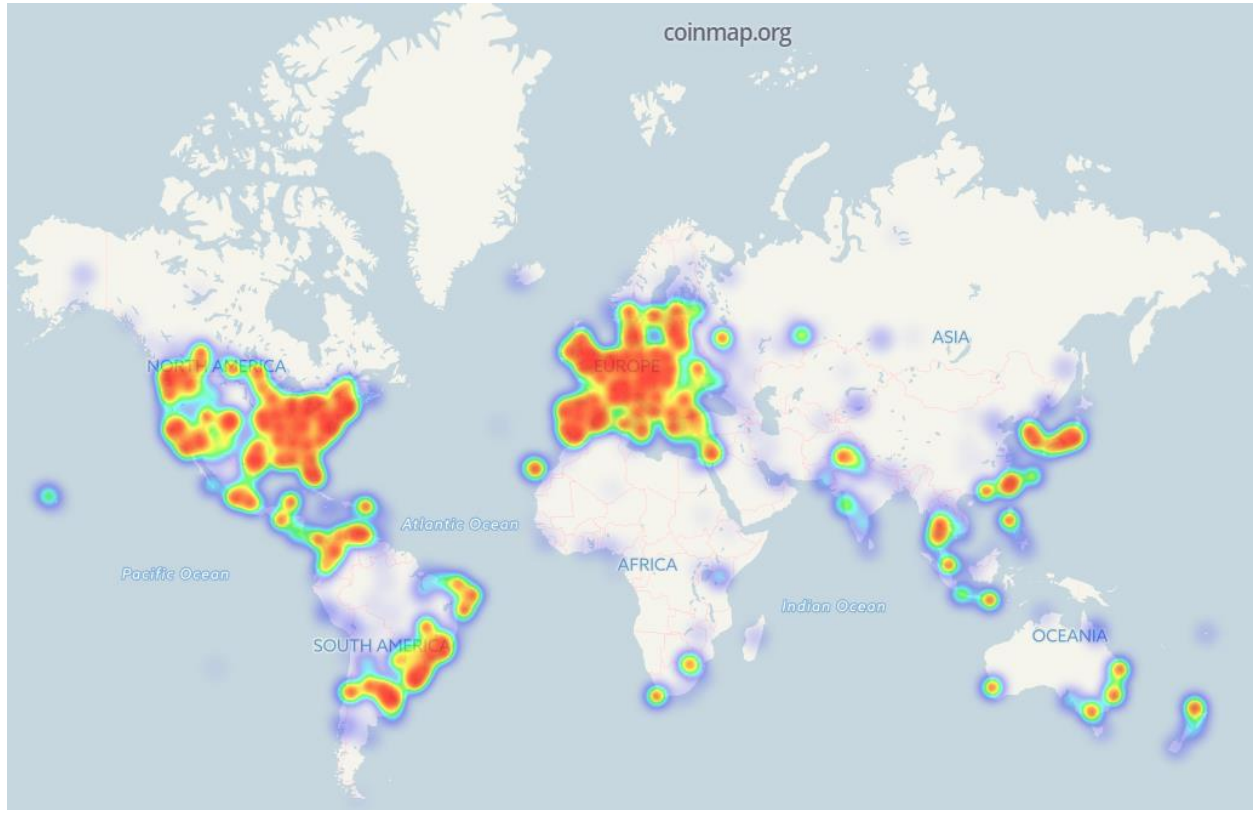
- Arguably though, the most important indicator of any currency with the characteristics of international, borderless and voluntary, is **user** and **merchant** acceptance and adoption.
- **Number of Users:** The number of users can only be approximated, by the number of downloads of the wallet software, 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, hardware 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.



Permissioned Ledgers and Private Blockchains

Private blockchains

- A new theoretical approach that is becoming increasingly popular among organizations in finance, is the concept of blockchains that are comprised of participants that are known and vetted. R3cev is such an initiative researching how to connect several banks together via a distributed ledger.
- Digital Asset Holdings is a similar venture aimed primarily at reducing settlement latency and counterparty risk for asset transference.
- These initiatives aim to use the concept of the blockchain, on some level, to decrease the inefficiencies and high costs that exist today in asset settlement and potentially even international money transfers.
- Either through the use of a syndicated participation by several organizations or private control, these blockchains will operate on different principles than what we've learned from Bitcoin's public blockchain or other cryptocurrencies, and perhaps not even use tokens as we know them.
- Most discussion around them so far (since we haven't seen a functional prototype yet), has pointed to systems for the secure communication of information or values between a finite set of authorized users, and not a public, customer facing network. Could these new ledger networks help these organizations decrease costs and increase security?

The Bit without the Coin

- While for Bitcoin, the network is inextricably tied to the token that is the means of exchange on this network, this might not be the case for these ledgers or ownership. Tokens (if they exist) might not be finite, transactions may be reversible and several other elements as we've come to know them might not need to exist (in theory) to maintain such a ledger.
- If we had a ledger shared between 10-15 trusted parties, would we have the same Byzantine General concerns as in Bitcoin, would consensus be still at a risk ?
- If there was trust, would there be fear of false participants in the network, or would Proof of Work still be needed to create a longest chain ?
- If there is no need for trust, then we might not need miner's fees, which could bring transaction costs even lower. Manual intervention could quickly fix faults in the system and transactions that were unauthorized could be reversed with relative ease, since consensus would be easier to reach.
- The lesson to keep from this field (for now), is that there is a significant effort to learn from the innovation of Bitcoin and apply it to existing systems in finance and beyond.

Issues and potential benefits

- If we take the perspective of a bank for a second, we could feel that there is a need for faster and cheaper transactions, whether for the settlement of inter bank transfers or the settlement of securities, as well as a decrease in bureaucracy and a better ability to report to regulators.
- On the other hand, there are very strict regulatory stipulations that govern their operation, and their obligations when it comes to KYC (know your customer) and AML (anti money laundering), and they are very sensitive towards both anonymity and lack of accountability. Censorship resistance and decentralized immutability is not only an undesired characteristic, but a risk towards their ongoing operation, and the eyes of their regulators.
- We examine in more detail, the potential benefits of using permissioned ledgers and private blockchains, and how they can tie into (and to which parts) of the existing financial and international settlement systems in the course **DFIN 513**, **Open Financial Systems** of the MSc.

Conclusions

Subtitle (optional)

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.
- Several businesses and banks in the finance industry are working on their own internal blockchains to replace existing functions.

Further Reading

Subtitle (optional)

Further Reading 1/2

- 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/
- On public and private blockchains :
  - https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/
  - http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf
  - http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf
- More on Ethereum and smart contract platforms:
  - https://www.linkedin.com/pulse/why-smart-contracts-make-slow-blockchains-gideon-greenspan?forceNoSplash=true
  - https://blog.ethereum.org/2015/05/24/the-business-imperative-behind-the-ethereum-vision/

Further Reading 2/2

- On Tokens and Crowdsales
  - https://medium.com/bitcorps-blog/on-tokens-and-crowdsales-309e49d9530d#.c1f8swxl7
- What Initial Coin Offerings Are, and Why VC Firms Care
  - https://hbr.org/2017/03/what-initial-coin-offerings-are-and-why-vc-firms-care
- Investor guide. Does this “cool project” truly need blockchain?
  - https://medium.com/@pavelkravchenko/investor-guide-does-this-cool-project-truly-need-blockchain-bdde70a26bfb#.sdphijbmj
- Corda and the Distributed Ledger Technology
  - https://tpbit.blogspot.gr/2017/01/corda-and-distributed-ledger-technology.html
- Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin
  - http://www.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/

Questions?

Contact us!

UNIVERSITY *of* NICOSIA

Twitter: @mscdigital
Course Support: digitalcurrency@unic.ac.cy
IT & live session support: dl.it@unic.ac.cy