

***INITIAL COIN OFFERINGS: THREATS AND
OPPORTUNITIES OF A NEW FINANCING TOOL.***

RELATORE:

Prof. Riccardo Bruno

CORRELATORE:

Prof. Alfio Torrisi

CANDIDATO:

Lorenzo Canuti

Matr. 684801

Anno Accademico 2017/2018

Foreword

The objective of this work is not to give the umpteenth description of the whole history about Bitcoin and its skyrocketing price, but rather to give a comprehensive view of its underlying technology and its implications for the upcoming future, both as a new way to conceive transactions and as a "killer application"¹ of Blockchain technology that for sure accelerated the approach to new currency frameworks and financing tools such as Initial coin offerings. In order to do so, when I will mention the term "Blockchain", I will refer to the "first distributed chain of blocks" ever made² by the Bitcoin founder Satoshi Nakamoto, to distinguish it from the very first conception of the term "chain of blocks"³ made in 1991. From now on, I will intend with Blockchain the technology over which Bitcoin has been and it's still run. Thus, being Bitcoin the first Blockchain application, we unavoidably have to analyze what factors have determined its success and made it become so popular that we can give it credit for having introduced the Blockchain to the world.

1 <https://www.techopedia.com/definition/7953/killer-application-killer-app>

2 <https://en.wikipedia.org/wiki/Blockchain#History>

3 <https://link.springer.com/article/10.1007/BF00196791>

Contents

Foreword.....	3
Chapter 1 -What is Blockchain and what are its implications?.....	6
1.1 How did we arrive to Bitcoin: technology development history.....	6
1.2 Satoshi's whitepaper: The birth of Bitcoin.....	9
1.3 Bitcoin transactions.....	10
1.3.1 Blockchain types.....	11
1.3.2 Who approves transactions?.....	12
1.3.3 How are miners rewarded?.....	15
1.4 The denationalization of money.....	16
1.5 Issues for Bitcoin.....	16
1.5.1 Mining pools.....	16
1.5.2 Electricity cost.....	17
1.5.3 Velocity of transaction.....	18
1.5.4 Money Laundering.....	19
1.6 Where does all of this started? Preconditions.....	20
1.6.1 Decreasing trust on central authorities.....	20
1.6.2 Information emerging as a new asset class.....	25
1.6.3 Privacy and transparency issue: the surveillance society.....	27
1.6.4 Financial crisis as proof of concern.....	32
1.6.5 Globalization as a decentralization enhancer.....	33
1.6.6 Millennials drive the new emerging markets.....	34
1.6.7 Trends in the use of paper money: The cashless society.....	37
1.7 Trust and Bitcoin birth.....	39
2. Chapter 2 ICO market overview.....	40
2.1 Introduction to Initial coin offerings.....	40
2.2 What is an ICO.....	40
2.3 Difference between tokens and cryptocurrencies.....	41
2.3.1 Blockchain layers.....	41
2.4 Token classification framework.....	43
2.5 ICO structure.....	45
2.5.1 Token sales structure.....	46
2.5.2. Soft cap and Hard cap.....	48
2.6 Global market growth.....	48
2.7 ICO brief history.....	53
2.7.1 The Birth of Ethereum.....	54
2.7.2 The DAO: smart contracts and hacks.....	57

2.7.3 Security offering.....	59
2.8 Ico comparison with VC.....	61
2.9 ICO comparison with IPO.....	63
2.9.1 Advantages and disadvantages of the two financing means.....	63
2.9.2 Differences with IPOs.....	66
2.9.3 Reverse ICOs.....	67
2.10. Debate in the valuation framework: a far to complete process.....	68
2.10.1 Metcalfe’s law.....	68
2.10.2. Quantitative theory of money applied to crypto.....	71
2.10.3 Network value to transaction ratio.....	71
2.11 What factors determine the success/failure of a campaign?.....	73
Chapter 3 Fundamental value for ICOs.....	74
3.1 Framework.....	74
3.1.1 ICO use case presentation: Overstock’s subsidiary tZERO.....	74
3.2 tZERO company overview.....	75
3.3 ICO structure.....	76
3.4 Valuation multiples.....	79
3.4.1 Assumptions on comparables.....	79
3.4.2 Multiple used.....	80
3.4.3 Detecting overvaluation with NVT ratio.....	82
3.5 ICO announcement and stock value.....	83
3.6 Bubble to burst? Comparison with dotcom bubble.....	85
Conclusions.....	88
Bibliography.....	94
Sitography.....	94
Resume.....	98
Overview.....	98
Chapter 1.....	99
Chapter 2.....	101
Chapter 3.....	105
Conclusion.....	106

Chapter 1 -What is Blockchain and what are its implications?

1.1 How did we arrive to Bitcoin: technology development history

A brief history about the steps made in technology development is needed to understand how we arrived to Bitcoin and, as a consequence, Blockchain. One big point of departure is for sure in 9 March 1993: a man called Eric Hughes published the so called “Cypherpunk’s manifesto”⁴. Briefly speaking, Cypherpunk is a movement born with the aim to solve the privacy problem in the electronic age, age in which the rise of an impressive amount of information and transactions are continuously and increasingly connecting people, requiring the exchange of information (or at least a part of them) which could even be unnecessary for the transaction itself. We can briefly state that the exchange of information is part of what Hobbes could have included in the requirements for the so called “social contract”⁵, a non-written one in which people are voluntarily willing to give up part of their freedoms in order not to fight against each other and be protected by a centralized authority, the state, accepting its rules and obligations as a fair exchange for that protection. The issue in here is that the contract between citizens and state is based on trust, and should this latter lose this quality, citizens are “legitimately authorized” to rebel. Privacy, in this particular situation, is a part of what the state asks to at least partly manage in exchange for protection, but that requirement is not all the time necessary. Restating Hughes’ words, “privacy is necessary for an open society in an electronic age. Is not about secrecy, but rather the power to selectively reveal oneself to the world.” The explanation of this statement is that in the current state of the art, one couldn’t have even chosen whether to selectively reveal itself or not, but it had the necessity to go for the “always reveal option”, and if privacy is the issue, “encryption” is the solution proposed by the movement, which actively promotes it and works for its development. But what is encryption? Its birth is practically as long as man history, and we can briefly say that is a way to encode a message in order to let it be understood only by an interested recipient that has the “keys” to decode it⁶. The way encryption works had already been updated by Martin Hellman and Whitfield Diffie in 1976 with the invention of the so called “public key cryptography” or “asymmetric cryptography”⁷. It basically provides the user with a public and a private key (key pair), the public key can be referred to as its pseudonym and is generated as a “one time” identity to be used for the transaction,

4 https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto

5 http://www.sophia-project.org/uploads/1/3/9/5/13955288/elahi_socialcontract.pdf

6 <https://en.wikipedia.org/wiki/Encryption>

7 <https://ee.stanford.edu/~hellman/publications/24.pdf>.

while the private key is the one that is transferred to the counterparty and which uniquely allows this latter to decrypt the message. This is one of the most important improvement of the pre-existing symmetric key cryptography⁸, in which the same private key was used to both encrypt (from the sender) and decrypt (from the receiver) the message. Coming back to the Cypherpunk movement, the word “Cypherpunk” is the result of the combination of two⁹: “cypher”, which is indirectly referring to one possible mean through which encryption can be made, numbers then, and “punk” which at first glance could be a misleading word in this context, but that has to be analyzed more in deep. It’s relevant the fact that, even if that can’t come instantly, “punk” refers to a cultural movement born at the end of the 70’s, and it’s not a surprise to notice that even if the punk movement have had many different shapes in its manifestation so that one can’t group its representatives in one big class, there is a common ideal, one for all, which is the refusal of every type of social control and anti-establishment views¹⁰. If one must be precise, the real origins of the word cypherpunk is related to a punk sub-culture, known as “cyberpunk”. We can easily understand that this “desire for liberation” from the Big brother that is indeed present in the Bitcoin as one of the justifications for its birth, was already present tens of years ago, and if we just think of what is happening nowadays (while I’m writing, Cambridge Analytica scandal is being discussed¹¹) we can’t deny that is still (and for sure more) an important issue to solve. The first proof of the existence of this movement, and even the not so hidden reference to the Big brother¹² as a problem to be overcome, is related to David Chaum, which in 1982 already proposed an encryption method based on “blind signatures”¹³. Roughly speaking, it was a way to encrypt messages without any third party having the need to know the content of the message exchanged, even if mandatorily involved in the approval process. Think about a man going to notary with a closed envelope to be certified. The notary has to put the stamp on this letter to certify that this document was pre-existent and already contained at a certain date what will be read whenever is due or required. With this technology embedded, Chaum founded the first electronic money corporation ever in 1989: Digicash. Transactions validation was still done in a “traditional” manner, with a central server approving all the information. The company went bankrupt in 1998 and was sold to eCash Technologies. The failure, Chaum declared, was due to the lack of integration of a such a premature

8 <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences>

9 <https://medium.com/swlh/the-untold-history-of-bitcoin-enter-the-cypherpunks-f764dee962a1>

10 https://en.wikipedia.org/wiki/Punk_subculture#Ideologies

11 <https://www.theguardian.com/commentisfree/2018/mar/21/cambridge-analytica-facebook-data-users-profit>

12 <https://www.cs.ru.nl/~jhh/pub/secsem/chaum1985bigbrother.pdf>

13 <http://www.hit.bme.hu/~buttyan/courses/BMEVIHIM219/2009/Chaum.BlindSigForPayment.1982.PDF>

e-commerce business in a nascent market¹⁴. While DigiCash was next to bankruptcy, in 1997, Adam Back created the Hashcash “proof of work” protocol. Put simply, the proof of work protocol was a sort of “obstacle” created to deter the so called “DoS attacks” and “spam”¹⁵ and Hashcash was one of the most famous proof of work protocol at that time. The proof of work concept is to require additional work in terms of computing power to an attacker in order to let it become disadvantageous (both in economic terms and time needed) to successfully conduct such an action and prevent double-spending. The result of this protocol, is the generation of a token which “ensures” that a transaction has had a certain amount of work to be validated, the proof of work itself. Good to remember that the same concept of proof of work is a main component of Bitcoin way of working, and as you can imagine, running a protocol on an obstacle (as I mentioned before) is by itself a poor solution, more on that later. The limit of this invention was the fact that coins created with such a method could only be spent once, so that every time a user wanted to do a transaction, he had to create a new digital coin for the purpose. The next year, Wei Dai proposed B-cash¹⁶, an “anonymous and distributed electronic cash system”. It basically proposed two protocols: in the first one, every participant maintains a separate database on every transaction made around the protocol, in the second one, the way in which accounts are kept updated is made through a subsetting of the databases (called servers), which are responsible for ensuring the truthful representation of the transaction, and the way to grant this honest work was to require a set amount of money (proportional to the computational problem cost function) to be put at stake on the server as a guarantee of its honesty. Dai was inspired by the “Crypto anarchy manifesto”¹⁷. Citing Dai, “in a crypto anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It’s a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.” From the failure of DigiCash, many other attempts tried to replicate its path in a more successful way¹⁸, and we can in a way state that the second “digital wave” reached its peak with Paypal, and we know the rest of the story. 2004, Hal Finney departed from Hashcash protocol to create the so called “reusable proof of work” protocol¹⁹, which is basically the solution of Hashcash non-spendability issue. With proof of work, tokens can’t be spent because the transfer of a token would lead to the double spending problem, so that anyone that is

14 https://en.wikipedia.org/wiki/DigiCash#cite_ref-5

15 <http://www.hashcash.org/papers/pvp.pdf>

16 <http://www.weidai.com/bmoney.txt>

17 <https://keatsmoodledevtest.kcl.ac.uk/pluginfile.php/1251665/course/section/414599/may-crypto-anarchist-manifesto1.pdf>

18 <https://bitcoinmagazine.com/articles/quick-history-cryptocurrencies-bbtc-bitcoin-1397682630/>

19 <https://cryptome.org/rpow.html>

able to alter the code of the transaction could easily “double spend” it. Each reusable proof of work token is simply generated from a correspondent proof of work token so that even if the proof of work or reusable proof of work token can be spent only once, its correspondent can be used to be handed from person to person. The mean through which reusable proof of work works is the property of digital coins to be traced by an autonomous processor that run codes and pairs digital identities with digital coins²⁰. We can see in this new attempt of development, the basis of what is the peer to peer network, a sort of “decentralized system” in which you don’t ask and answer for information to a unique server but to the network itself. The very solution in here is the sequentiality of transactions. At the end of 2005, Nick Szabo created what he claimed to be a “decentralized proof of work protocol”²¹, in which for the first time ever, in substitution of the traditional centralized trust mechanism which could be for example pertaining to a bank, there was a challenging decentralized, trustless protocol, suitable for inflation related issues resolution, rewarding people certifying the network via the proof of work with cash. Szabo will become famous also for the creation of “smart contracts”²².

1.2 Satoshi’s whitepaper: The birth of Bitcoin

Now that we covered the improvements made in cryptography through the last decades, we can use the history to demonstrate that Bitcoin is not something which came out from thin air, but was simply the best assembly ever made with the above mentioned technologies, in an all-in-one technology that uses original inventions (or a part of them) to run the system. With what I would call “Bitcoin’s manifesto”²³, the 31st of October 2008, Satoshi Nakamoto, the pseudonym of what is sustained to be not a single person, but a group of work (and probably founded by many names mentioned above) came out with a paper proposing “a peer to peer version of electronic cash payments”, based on the aim to solve the double spending problem, using a proof of work mechanism derived from Hashcash as a tool to prevent this latter, and incentivizing people elaborating the “proof of work puzzle” with a coin, the Bitcoin itself. The proof of work used in this case is a sort of “perfect mix” between Hashcash way of proving transactions to be happened only

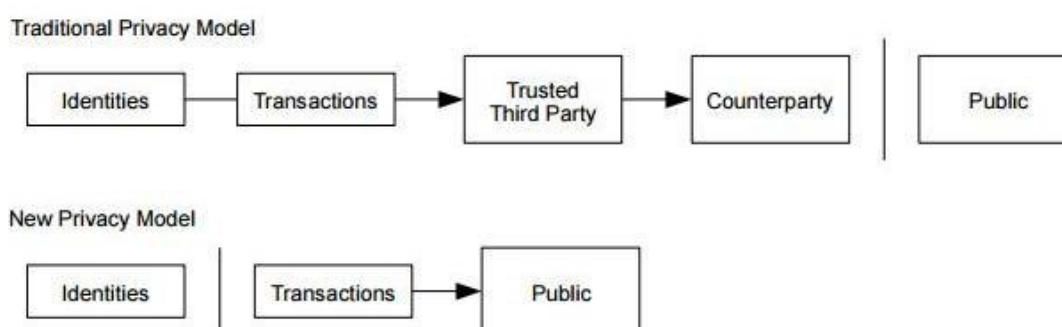
20 <https://nakamotoinstitute.org/finney/rpow/index.html>

21 <http://nakamotoinstitute.org/bit-gold/>

22 http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

23 <https://bitcoin.org/bitcoin.pdf>

once, and Finney's reusable proof of work aim to register the "chain of transactions" occurred in a reliable way, but with the difference that the way in which transactions are approved are in the shape of a "decentralized p2p network". This paper proposes a disruptive new way of conceiving transactions and shorting the "chain" intended to let them be conducted and registered. The logic of the new solution is that if the problem is to make a transaction secure, one has had only one way up to that moment to conduct it, which is to rely on an intermediary to be a good trusted executor for a transaction, and this is what basically describes the "traditional privacy model" shown here below. In this model, one has to accept both its identity and the transaction itself to be known by the intermediary involved and separated by a wall (which in this case could be identified with the server of the intermediary) from the public. The new privacy model instead (described in second row of the image), proposes a new method which is to say "I want everybody to know that a transaction has happened between two or more digital identities, but I don't want anybody to have access to who physically sent what to whom". To sum up, if in the traditional model the trusted party is the physical intermediary, in the new privacy model this "intermediary" could be said to be protocol itself, since everybody knows that a transaction has been added to the Blockchain but only authorized parties can enter into that piece of information and decode it.



24

The revolution in here is not even the decentralized manner in which transactions are conducted so that no one basically controls the network, but it in addition to this, Bitcoin is a distributed protocol, which is to say that no central server or authority owns the whole history, but all of the participant, so that if all is in our own hand, that means that whenever there is a "wrong version" if the truth, the network will raise red flags and reject this latter. The first important conclusion is that we have to keep in mind that all of this digital wave and extremely technical tools have occurred to solve a problem, which is the privacy of transactions and the willingness to "beat the Big brother" by relying on an alternative trusted mean which now has not to necessary be the "devilish banker with

suit and tie” that runs a server and asks for an unfair share of money in exchange for it, but a protocol.

1.3 Bitcoin transactions




How Bitcoin works then? First, parties wanting to do a transaction need to download the Bitcoin software, with which they can generate a public address, comparable to what could be an IBAN id, and that as a consequence is the “known” code that can be exchanged among parties involved to identify each other. Once that address is generated, the parties execute the transaction with the exchange of their own private keys, and this transaction is grouped with other transactions within a “block” which contains other transactions. What happens now is that the parties will have to wait for the network (physically made by all the computers participating to the community) to “mine” the transaction into that block (more on that later) , which is to approve it and fix a certain date on it with a process called “time-stamping”²⁵. This approval occurs with the already mentioned proof of work protocol, which is to require computational power to demonstrate that a block of transaction have had a certain amount of work to be validated. The outcome of this proof of work is the generation of a “hash code”²⁶, which links every block in sequence, forming a “chain of blocks”, the Blockchain itself! If a dishonest node wants to alter this transaction, will have to re-do the already mentioned proof of work of the blocks created such, literary guessing what is the hash function that identifies a transaction in which a given address A sends a certain amount of Bitcoin to address B at a given time-stamped hour.

1.3.1 Blockchain types

When we think about Blockchain as being this pure technology allowing people to trace everything forever and grant decentralization, we need to clarify that we’re not dealing with the whole panorama actually in place, but only with the “hardest” part of that, the most pure one. Indeed, we can classify Blockchain as being of 3 types: public, private and consortium blokchains.

25 https://en.wikipedia.org/wiki/Trusted_timestamping

26 https://en.wikipedia.org/wiki/Hash_function

	 Private	 Consortium	 Public
Access	Permission	Permission	Permissionless
Validators	<u>Predetermined</u>	<u>Predetermined</u>	Proof of work / stake
Identity	<u>Known</u>	<u>Known</u>	<u>Anonymous/pseudonymous</u>
Speed	High	High	<u>Low</u>
Trust	Trust based	Trust based	Trustless

27

1.3.2 Who approves transactions?

If Bitcoin is a “network” of computers, then there will be a certain amount of those that are delegated of approving the transaction, we call them “miners”. Who are miners?²⁸ Put simply, they’re those in the network delegated of “approving” the transactions. The way the approval is made is by solving a computational problem, which is to find a hash function that correctly identifies a block. If one has to be precise, the approval process mustn’t be confused as the process of controlling the content of each block and assessing its truthful representation of a transaction, but rather the consensus mechanism established within the protocol that simply determines what is a valid block in terms of rules to be followed for it to be such²⁹. Claryfing this statement, blocks added to the chain mustn’t be misunderstood as the “only truth present in the network”, but rather as a generally accepted version for those that strictly apply the protocol rules, and thus blocks on which miners can build upon by solving the proof of work of the subsequent blocks. To sum up, the fact that a block is corrupted would automatically lead to the impossibility to link it to every other subsequent block, causing the chain created accordingly to be shorter (in terms of computational amount) than another one, and automatically causing the acceptance of the longest one, with the abandoning of that one which is “corrupted” in a sense³⁰. To figure out how the approval process works, let’s firstly represent a block’s components (figure 1):

27 Custom image

28 <https://www.bitcoin.com/bitcoin-mining>

29 <https://bitcoin.stackexchange.com/questions/57686/how-many-miners-approve-a-block-before-it-gets-added-to-the-block-is-it-51>

30 <https://www.youtube.com/watch?v=wTC31ZI6QM4>

BLOCK 1	
NONCE	70383
DATA	A SENDS 1 BTC TO B
PREV. BLOCK HASH	00000000000000000000000000000000 00000000000000000000000000000000 00000000000000000000000000000000
HASH OF BLOCK N°1	0000EC19855E7C75C2C9D4BE80 45879E1F60B50BE19178287FF1FCF 920AF1929

31 (figure 1)

In figure 1, a block is represented: we call it “genesis block” as being the first hypothetical block of the chain, and it is composed by:

- Nonce³²: is a 32-bit field that is set in order to let the hash code starting with a given number of zeros
- Data: The information relative to the transaction, which could be more than a single one
- Hash of the previous block: is the hash of the previous block that is linked to the block. In this case, being the block a genesis one, we have a “null” hash of the previous block.
- Hash code: is the code that identifies this and only this precise transaction

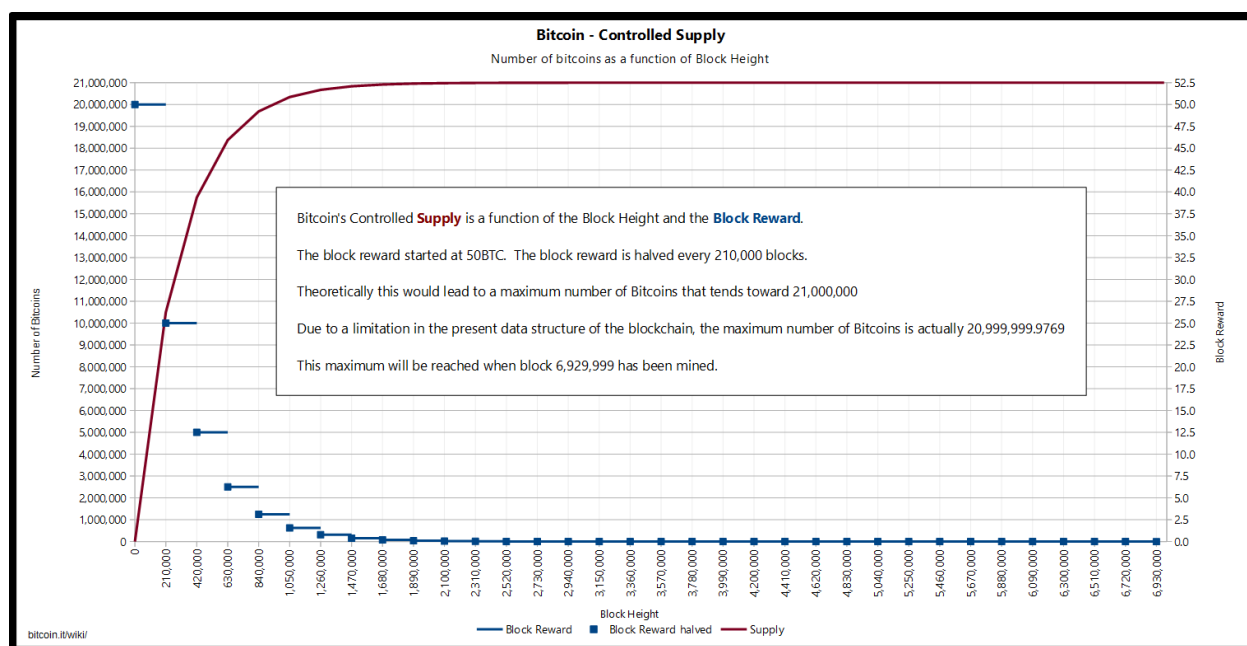
The way the process work can now be simplified in this way: suppose that two parties execute 2 different transactions and let’s say that are contained in two different blocks. As I said before, the blocks are linked one to each other by a hash function as a proof of work certificate, created with an iterative process that increments a nonce value to obtain the set amount of starting zeros for the hash that solves the “proof of the block”. The procedure can be represented as it follows:

31 Rework from <https://anders.com/Blockchain/Blockchain.html>

32 <https://en.bitcoin.it/wiki/Nonce>

1.3.3 How are miners rewarded?

In the Bitcoin whitepaper³⁵ Satoshi Nakamoto describes the protocol as providing miners with an incentive, which is to basically allow them to be rewarded with a coin (the Bitcoin) every time they add a new block to the chain and consequently permit this latter to keep it functioning. Bitcoin total supply is fixed at 21 million and this number will be reached through a constant halving of the amount of reward to which miners are entitled for solving blocks computation. By now, the reward is 12,5 Bitcoin every block and it will halve again once a given amount of blocks (210,000) will be generated³⁶. Considering the fact that every block is generated every 10 minutes on average, that brings money supply to be easily forecasted to end in May 2140, as shown in the graph below



37

Indeed, every time the computational problem becomes “too easy to solve”, the algorithm of the software simply adjusts the difficulty of finding a valid hash so that the same velocity is maintained. The whitepaper then furnishes readers with a solution when Bitcoins awarded will be lower in value with respect to the cost to mine blocks, the difference to break-even will eventually be calculated as a transaction cost, so that the incentive to mine will keep unbroken and not everybody will finish the day after Bitcoin supply is run out. Anyway, the fact that we observe a fixed supply isn't

35 <https://bitcoin.org/bitcoin.pdf>

36 <https://www.bitcoinblockhalf.com/>

37 https://en.bitcoin.it/w/images/en/4/42/Controlled_supply-supply_over_block_height.png

necessary a limit, having Bitcoin the possibility to be divided up to the 8th decimal value³⁸. What has to be reminded is that since Bitcoin supply is fixed, no one actually creates/mints new coin, simply mine them in the network, like gold or diamonds have to be mined in mines.

1.4 The denationalization of money

Broadly speaking, the decentralized money supply was in an indirect way already sustained by the nobel prize and economist Hayek³⁹. Hayek basically sustained that the power of governments as a central authority to mint the only recognized money in a territory is basically given without any technical qualification as a justification for it, they simply took possession of it and made people trust them, but this could be considered as a good function to be exercised by states as long as they only care about “certifying the weight and the fineness of a certain piece of metal”. The problem starts when states become aware about the possibility to profit upon people with a “deliberate determination of the quantity of money to be issued [...] abusing their trust to defraud them”. Having abused of the trust of people, states have practically made a history of inflation engineered by governments. By proposing the “liberalization” of money, Hayek was trying to demonstrate that if different currencies can compete with each other without the “excuse” of legal tender brought as a justification by states, a better currency can emerge above this competition and bring more advantages than actual money system.

1.5 Issues for Bitcoin

1.5.1 Mining pools

One risk to which the whole Bitcoin community is exposed is that of the mining pools. Early miners could profitably mine Bitcoins with their own laptop. Now that the network has grown, no added value is given by a single machine like a laptop which is not even programmed to do such a specific job in an efficient way. The specialization of miners lead to the creation of literary an empire of dedicated softwares and sophisticated mining hardwares. To be clear, if the process requires higher computational power and/or Bitcoin price remains too low, this could give miners an incentive to

³⁸https://www.reddit.com/r/Bitcoin/comments/4dw0aj/could_one_bitcoin_be_split_in_to_more_decimals/

³⁹ <http://nakamotoinstitute.org/static/docs/denationalisation.pdf>

create pools to still break-even. Pools of what? Of processing power of course! The fact that more miners put their own computational power in a single stake could probably lead to the risk of having few miners deciding whether to hash certain blocks or not for convenience purposes, with the result of neutralizing the idea of having a decentralized network in which no one actually controls what can be in or out of the Blockchain. Fortunately, the fact that every time the difficulty lowers it adjusts itself to a higher degree, leads only to a temporary convenience for mining to be executed in pools, since the higher computational power of the pool will cause the blocks to be solved faster, and consequently, causing the solution of a new block to be harder in terms of computing power, and then costly.

1.5.2 Electricity cost

As I mentioned before, running a Bitcoin network requires computational power, as well as a great amount of electricity to sustain this latter. Even if Bitcoin is still a niche instrument, the power required to mine Bitcoin is relatively huge with respect to other types of consumption. The path which electricity consumption is keeping with Bitcoin, if kept in this progression, would lead it to account for the whole electricity consumption in the planet within 2020! But is not an unsolvable problem of course. Firstly because as all the technologies do in their infancy, they are doomed to a certain degree of scaling and to reduce wastes⁴⁰, second, Bitcoin uses the most expensive validation protocol, which is the proof of work, while other crypto currencies like Ethereum are working to pass to the proof of stake mechanism⁴¹. Put simply, what changes in this mechanism is that not everybody in the network can become miner but only randomly selected “validators” (this is the right term to call proof of stake miners). The logic in here is that instead of requiring huge amount of calculation and then electricity costs, reasons on a monetary basis, which is to require validators to put an amount of currency at stake (from which the name proof of stake), which is locked in the network as a guarantee for the honest behavior of the validator. Should the validator behave dishonestly, he will lose the money put at stake, but at the same time, the more money he puts in the game, the more the probability to be awarded coins for the validation work. The way the algorithm is set should select the validators randomly not only on a stake basis, which could lead to perverse mechanisms such as rich people controlling the network and becoming everyday richer than people which have a lower stake, but even in a totally random way. The proof of stake also partly solves the centralization issue connected to proof of work mechanisms. Indeed, in the proof of work mechanism 51% attack is possible because of computing power grouped within a single

40 <https://powercompare.co.uk/bitcoin-electricity-cost/>

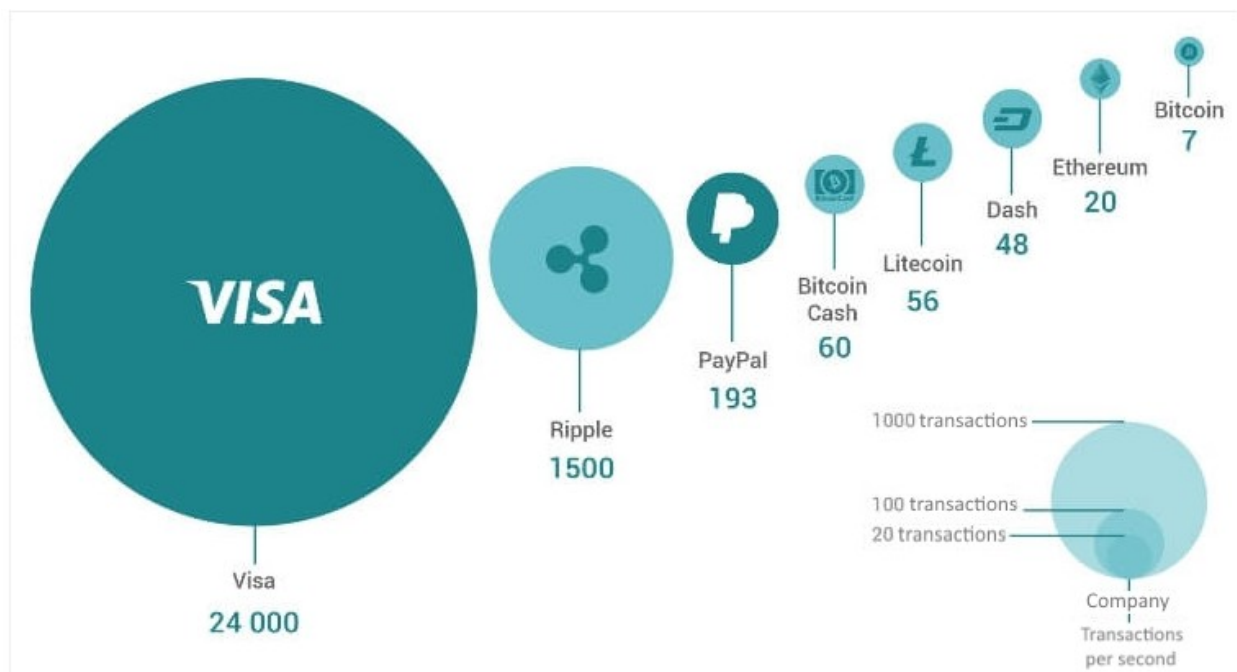
41 https://www.youtube.com/watch?v=M3EFi_POhps

pool, in the proof of stake this 51% attack has to be measured in “stake terms”, so that if we now instantly decide that Bitcoin should be run by a proof of stake mechanism, a single validator should possess half of the market capitalization of Bitcoin, which today, 24 June 2018, is around 45 billion euros (91 billion market cap).

1.5.3 Velocity of transaction

Velocity is all about providing users with the possibility to count on a considerable amount of transactions to be executed within a few seconds, and is straightforward how this characteristic alone could function as a watershed for what is good and what has to be left in the dark in the payments system nowadays. To be honest, we’re still in the dark side for Bitcoin, comparing its transactions to modern electronic payments, this results in a ridiculous gap still existing between traditional payments and crypto-uses (Figure below shows transactions per seconds). New cryptocurrencies have emerged, like Ripple playing an important role in being the faster cryptocurrency ever created, with the adoption of “off ledger” writings⁴², so that one doesn’t necessarily have to track all the transactions “on chain” but simply group a part of them in a resulting “pool” to be validated only once put on the ledger, as a normal Blockchain transaction. Simply put, the way in which a cryptocurrency shows its potential, is for large part explained by the way in which consensus is created among participants, and we can say with certainty that the cryptocurrencies which will have more success will be the ones that matches the trade off “speed, privacy” with consumers exact needs.

42 <https://xrphodor.wordpress.com/2017/09/27/how-xrp-is-faster-than-any-other-digital-asset-or-cryptocurrency/>



43

1.5.4 Money Laundering

Bitcoin's nature is that of being pseudonymous, which means that nobody's actually using its real name, but a public key code which can be generated everytime a transaction is made. As you can imagine, the way Bitcoin is kept secure it is not through an absolute level of safeness, but a relatively high one⁴⁴. Explaining the concept, the fact that people say Bitcoin is anonymous are wrong, and it is not even pseudonymous (like it is) if you use it wrongly. If the same public key is used to do every transaction on the network, the history of transactions can be traced, and every transaction connected to the same public key inevitably narrows the set of possible accounts from which to depart to discover your name and surname. And there are for sure ways to do it⁴⁵, thus, a good way to transact is to basically change the public key every time you do a transaction. Now, one of the bigger issues in Bitcoin is money laundering, favoured by the pseudonymous nature of the protocol itself. A study demonstrates⁴⁶ how nearly the whole amount of Bitcoins laundered comes from exchanges in which launderers try to free their amount of dirty money with fiat money or even other currencies. Is at that precise step of the laundering process that Anti money laundering

43 <https://bitnewstoday.com/market/altcoin/banking-half-blood-ripple-s-life-after-sobering/>

44 <https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/>

45 <https://bitcoin.org/en/protect-your-privacy>

46 https://cdn2.hubspot.net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf?hssc=222901956.3.1516201470218&_hstc=222901956.b7d6531ad164bec182c043c05b5510ba.1516201470217.1516201470217.1516201470217.1&_hsfp=3478668143&hsCtaTracking=66a034a3-865d-481a-8e56-f510419fde74%7C840a3208-7448-4fe6-ad03-a3731f462b7d

(AML) and Know your customer (KYC) regulations still have to be introduced in a standardized way, so that whenever a given amount of money results in a suspect one, the owner can be easily traced. Obviously, I understand those who claim that Bitcoin and other cryptocurrencies are a good incentive for money laundering in a way, but the size of that issue is not as big as they would think or expect. For sure, answering that also Euro or Dollar is being used to launder money is not an answer, but what has to be underlined here is the fact that yes, no single mean of payment can grant to be free from laundering, but Bitcoin and other cryptocurrencies have a strong difference between fiat money that needs to be analyzed more in deep. First, fiat money laundering is done by cash, and cash is for sure a “private method” of doing such an action, while Bitcoin and cryptocurrencies in general work on an “public immutable ledger basis”, so that whenever a transaction occurs it has to necessary be traced in the public ledger. Having said this, is clear that the way in which Bitcoin can be laundered needs to record all the transaction to do so on the Blockchain, meaning that even if your account is pseudonymous, your transaction is forever traced, so that whenever a regulating authority (now or in the future) finds a way (by new technology means or simply using algorithms) to link your portfolio with your real ID, something similar to declare “hey, I laundered X Bitcoins” happen. To sum up, at first glance Bitcoin could be said to be a perfect mean through which to launder money, but at the end of the day, one has to realize that it is a no brainer. One could even argue that this is not a sufficient answer, and at that point, all that remains to say is that yes, moneys can be laundered with Bitcoin, but is the not the main tool with which such actions can be done safely from the launderer point of view. Other cryptocurrencies allow for a greater level of privacy in the protocol like Dash or Monero, so that if one has to be precise, Bitcoin is not the best tool to do laundering.

1.6 Where does all of this started? Preconditions

1.6.1 Decreasing trust on central authorities

Trust matters⁴⁷ and that is an incredibly undisclosed key point in the economics literature to deal with and from which to depart to ask ourselves why economical and social interactions and changes

47 https://www.forbes.com/2006/09/22/trust-economy-markets-tech_cx_th_06trust_0925harford.html#11f46e0e2e13

in their structure occur. Roughly speaking, economics is principally based on markets, and markets exist and operate everyday just because of an untold, implicit “cross trust” mechanism established among parties, so that they exchange things and transfer wealth one to each other because they’re in a way confident both about the future outcome of their actions and the set of enforcement tools that a central authority (being it a state or a private firm) provides them to prosecute whoever behaves dishonestly in the transaction⁴⁸.

Citing Stiglitz⁴⁹, “Trust is what makes contracts, plans and everyday transactions possible [...] It is trust, more than money, that makes the world go round.” The nobel price tends to explain the 2008 financial crisis too with the trust mechanism. What he says is that if practically all banks were involved in the thoughtless securitization mechanism, and loans were granted to whoever asked for, regardless the creditworthiness, it all went fine until few institutions started to collapse and someone other started to distrust the way others were operating, causing the quick and disruptive block of all transactions, and when it came the moment to cover losses with liquidity, the same trust mechanism that has been used to solve this same problem temporarily had rebound back to take its toll. The only problem in matters of trust, is that we can’t straightforwardly define a precise set within which to put our “trust components”, so that if we take as a proxy the possibility to enlarge the comprehensive view of the definition, we can briefly say that countries differ among themselves because of different trust levels, and this occurs because there is no exchange without trust, and therefore there is no market and value creation or transfer⁵⁰. Trust, as one can already notice, is the result of a series of elements, which are diversely and unpredictably combined together and consequently can alter trust as an output depending on their specific (as referred to a specific country or market) correlation. Trust can be said to be the sum of different and even concurrent element which, if found all together, can explain why trust differs among countries and it is at the same time the cause and the consequence of trust and economic consequences.

Tonkiss makes the useful distinction between two characteristics of what I would call “reliability”: trust and confidence⁵¹. Confidence elements are basically “facts enhancing reliability”, trust is something more irrational, a series of beliefs that depend not only on facts but on the heard and what people “want to believe”. The fact is that confidence enhances trust but is at the same time

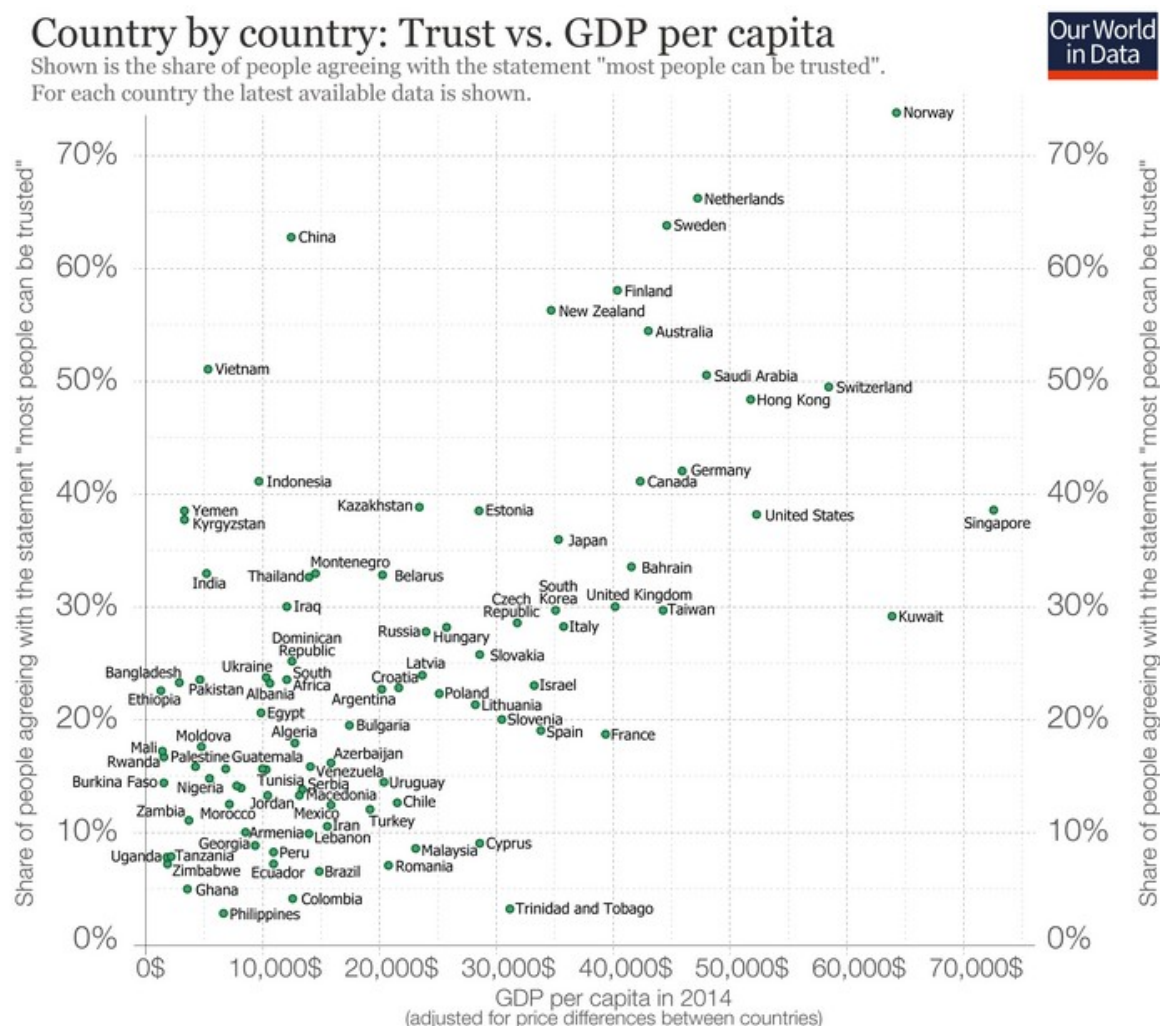
48 <https://poseidon01.ssrn.com/delivery.php?ID=930086105106031114022015079001098029014084048036031020026015124112029007014106119001065094125093001036019030099030003108088017000109082078113092114112110119103010087107031085095005091123&EXT=pdf>

49 <https://opinionator.blogs.nytimes.com/2013/12/21/in-no-one-we-trust/>

50 <https://www.econstor.eu/bitstream/10419/44134/1/394929810.pdf>

51 <https://link.springer.com/article/10.1007/s10272-009-0295-x>

influenced by trust and vice-versa. To make an example, if I'm confident I believe only in what I see as a proof of evidence, if I trust someone is because I believe there must be something out of confidence of which I can rely on. There's also a strong relationship between trust and GDP, which demonstrates that trust at least empowers economic growth and demonstrates how it can't only be treated as a philosophical argument.



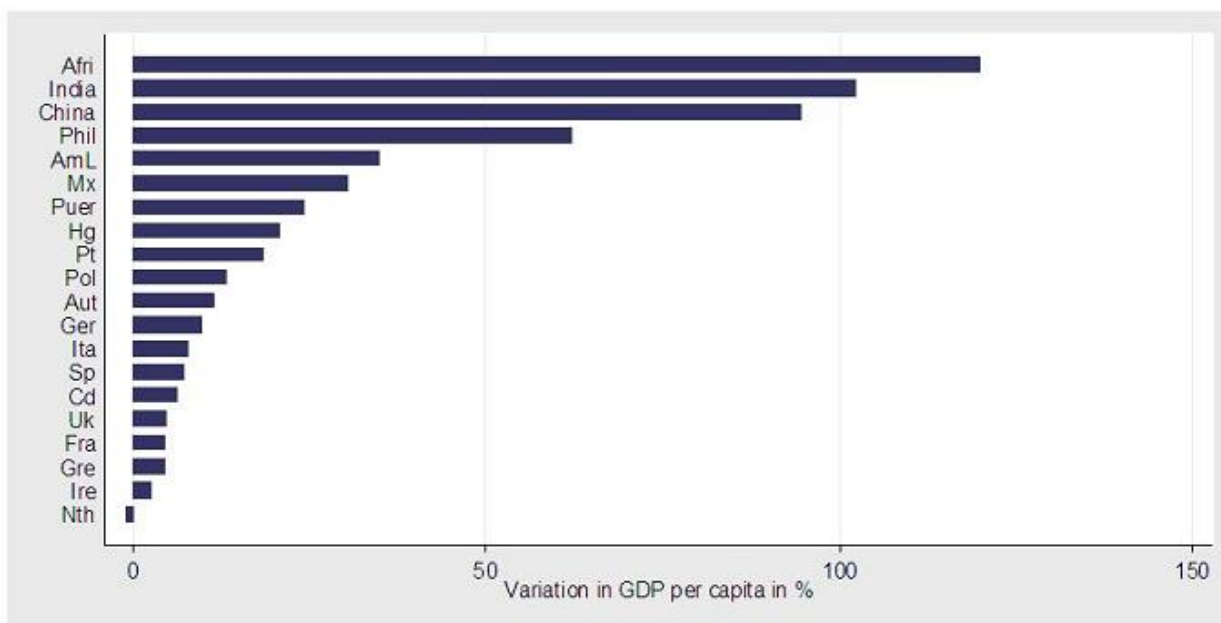
Another proof of the fact that trust and the way it combines its elements matters for transactions is given by the study of Sapienza and Zingales⁵³, which demonstrate a correlation between the level of investments and the tendency to withdraw deposits as well as doubting about the way governments intervention in financial markets, connecting to the level of trust measured accordingly. Trust, finally, is even influenced by the history of a certain country, being it more or less present according to the level of trust between citizens, which in the case of African countries could even be badly

52 <https://ourworldindata.org/wp-content/uploads/2016/07/Trust-vs-GDP-per-capita.png>

53 <http://faculty.chicagobooth.edu/brian.barry/igm/atrustcrisis.pdf>

altered by a recent past of slavery. In the figure below, we see how clearly trust can foster economic growth and explain a big part of differences among countries.

Figure 1 : Predicted variations in GDP per capita in period 2000-2003 if the level of inherited trust of people in working age were the same as in Sweden



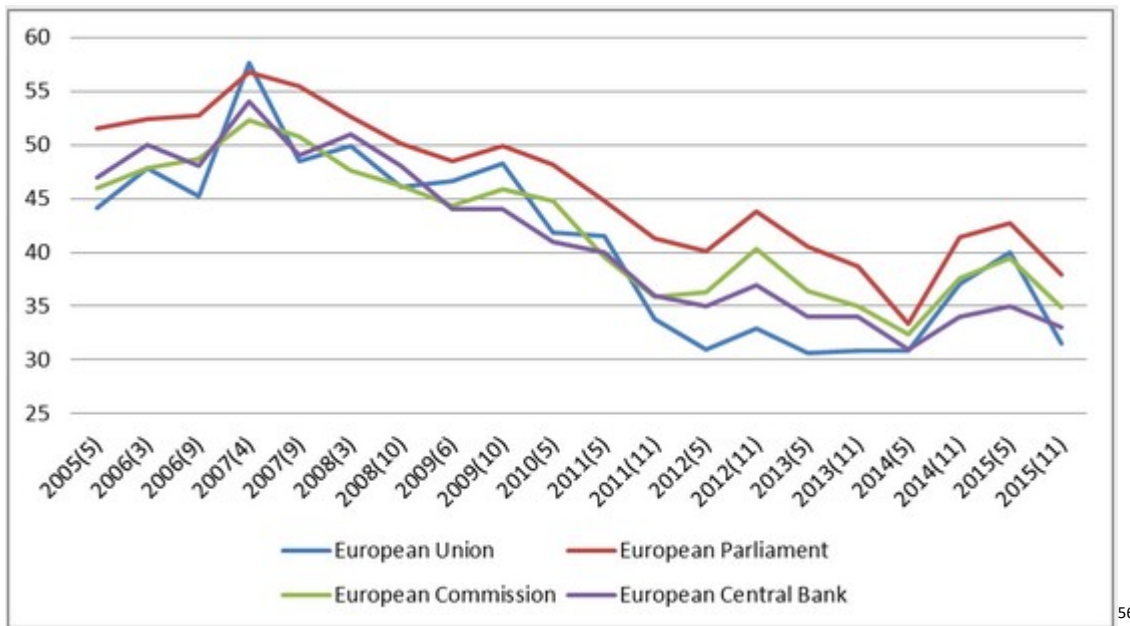
1.6.1.1 Trust trends in the world

The entire world is facing an endless decline in trust, and the studies mentioned above predicted in a way this outcome and foster the need for re-establishing a way of re-gaining trust, even by radically changing the way trust is gained and maintained through time. Investments level are struggling to regain power from the peak in 2008 before financial crisis⁵⁵, and after ten years we still face a distrust problem, people no longer believe in centralized authorities, and centralized authorities themselves don't know how to recover the gap lost in trust, even because they basically never asked themselves how to.

54 <https://voxeu.org/article/trust-and-economic-development>

55

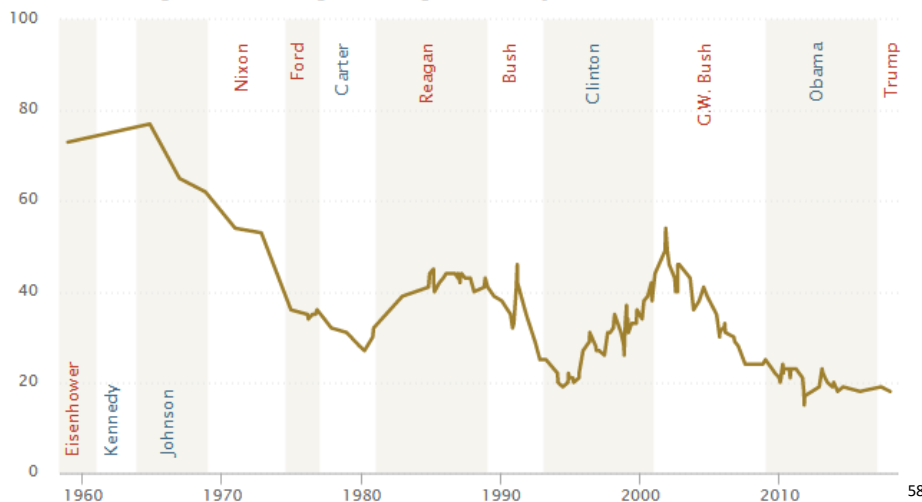
<https://www.atkearney.com/documents/236833/616008/From+Globalization+to+Islandization.pdf/e2d7755-4489-eb87-9664-150ab3839df7>



56

For what concerns Europe, technocrats have failed in building and keeping a trust mechanism among citizens and economic inequalities along with no effective sign of stable and sustainable growth foster this generalized distrust, which reached its maximum peak in 2013⁵⁷. The situation is even more dramatically clear if we look at the decline in trust towards US governments, which saw a sharp and almost monotonic trend to nearly the disappearance of trust toward the US government, regardless the political party which was governing.

% who trust the govt in Washington always or most of the time



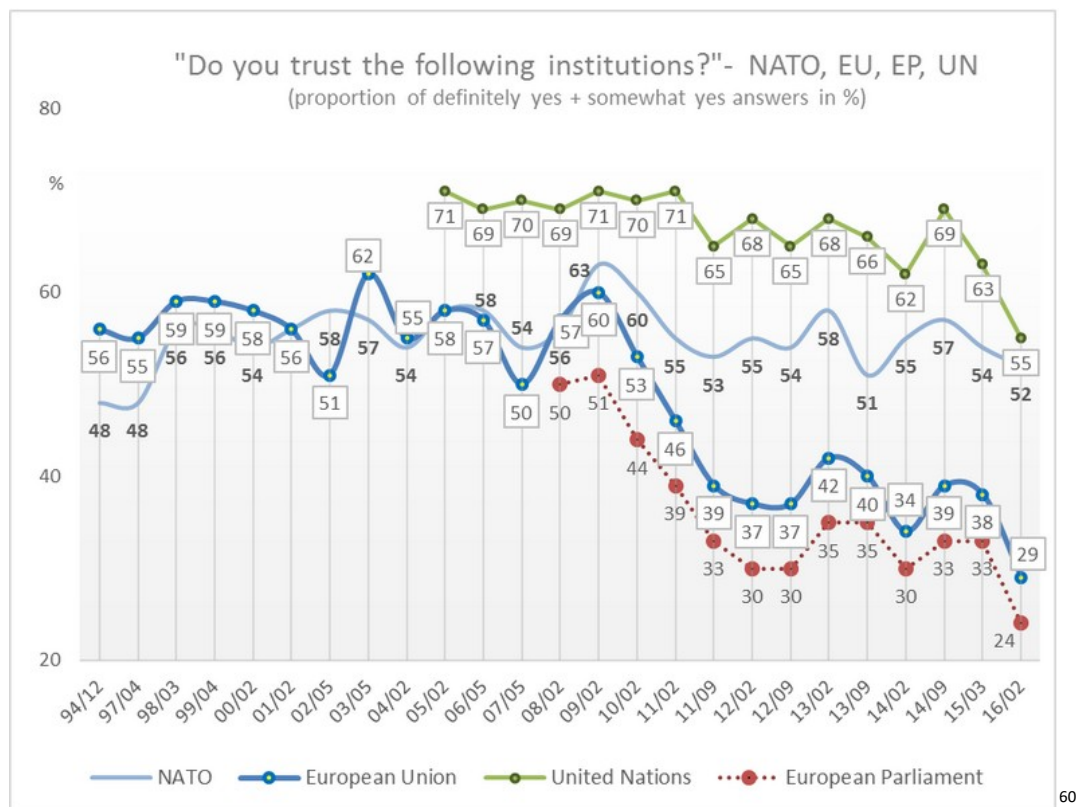
58

The authoritative Edelman trust barometer 2018 reports that US has had the largest-ever recorded drop in the survey’s history (18 years)⁵⁹. Generally speaking, the world as a whole has, on average, remarkably assisted in a decrease in trust

56 <http://blogs.uta.fi/contre/2016/02/11/trust-in-the-eu-short-term-fluctuations-or-a-more-long-term-trend/>

57 <http://blogs.uta.fi/contre/2016/02/11/trust-in-the-eu-short-term-fluctuations-or-a-more-long-term-trend/>

58 <http://www.people-press.org/2017/05/03/public-trust-in-government-1958-2017/>



60

Another remarkable aspect that the Edelman trust barometer suggests, is the fact that “trust has become a line of business”, and the confirmation is in the fact that nowadays people sampled believe that a first CEO worry must be to increase trust in its organization, because “silence is a tax on the truth”.

1.6.2 Information emerging as a new asset class

Every type of transaction basically involves the exchange of information, and the rise of the internet radically changed the way new business are created and run, “moving from being conducted in the physical marketplace to the virtual marketplace”⁶¹. New technologies like data mining, artificial intelligence and machine learning⁶² brought the possibility to establish stable patterns in consumers behavior and predict it, creating the possibility to enhance what is called (or at least said to be the reason for the use of data) consumer experience⁶³. What is remarkable in here is that what was expensive and even time-consuming before the advent of new analysis techniques is now

59 http://cms.edelman.com/sites/default/files/2018-02/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

60 <https://en.stem.cz/trust-in-the-european-union-and-european-parliament-has-significantly-declined-since-last-year/>

61 <http://daneshyari.com/article/preview/379905.pdf>

62 <http://upfrontanalytics.com/data-mining-vs-artificial-intelligence-vs-machine-learning/>

63 http://www.dbjournal.ro/archive/21/21_4.pdf

questionable in value and economically feasible. This radical change made businesses more aware about the value they could extract from customers, and them aware about this too. If information was before a nearly useless ingredient, emerging technologies now provide businesses with a set of tools which allow them to use these information to discover hidden recipes behind and extract value⁶⁴. Information has value on both sides of a financial statement, on the “active side” by enhancing market predictability and on the “passive side” by preventing costs increase and risk occurrence⁶⁵. It’s early days to find a reliable measure for information, Financial Times plays with this issue and tries to figure out how our set of personal information could be easily documented and be used as a commodity to create value⁶⁶. Data are a new asset class, and their amount is expected to be 44 times higher in 2020 with respect to 2009⁶⁷ requiring also the need to think about a trusted authority to manage the way data are exchanged, between who, and in what dimension. If data are an increasingly important asset class, that means that is even becoming relevant to assess how to value them, an “infonomics” argument has to be introduced⁶⁸. For this reason, every company in the world deals with data, but it’s not by chance that now the top 5 companies by market cap in the world have information based (more or less directly to the product they sell) revenues. We can roughly say that 3 out of those 5 have the power to control our life, since “Google can see what people search for, Facebook what they share, Amazon what they buy”⁶⁹. Adding certainty to this statement, it’s unquestionable that the value of the S&P 500 has practically reversed its tangible/intangible composition of value, and being information an intangible component, here’s another confirmation⁷⁰.

However, technologies and information they can extract can’t be considered as being other from proper data management, and the way we deal with this element is directly connected to the likelihood we could profit upon this or, conversely, to destroy value⁷¹. It is also necessary to understand what are the limits of the collection of information, which is privacy based and after quantitative and sector based: quantitative because the “marginal value” of information decreases as

64 <https://www.esmt.org/sites/default/files/peppard-c01.pdf>.

65 <http://www.eurim.org.uk/activities/ig/InformationAsset.pdf>

66 <https://ig.ft.com/how-much-is-your-personal-data-worth/>

67 http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

68 <https://www.forbes.com/sites/gartnergroup/2012/05/22/infonomics-the-practice-of-information-economics/#dbae4a46ee4e>

69 <https://www.forbes.com/sites/gartnergroup/2012/05/22/infonomics-the-practice-of-information-economics/#dbae4a46ee4e>

70 <http://sfmagazine.com/post-entry/may-2017-the-power-of-intangibles/>

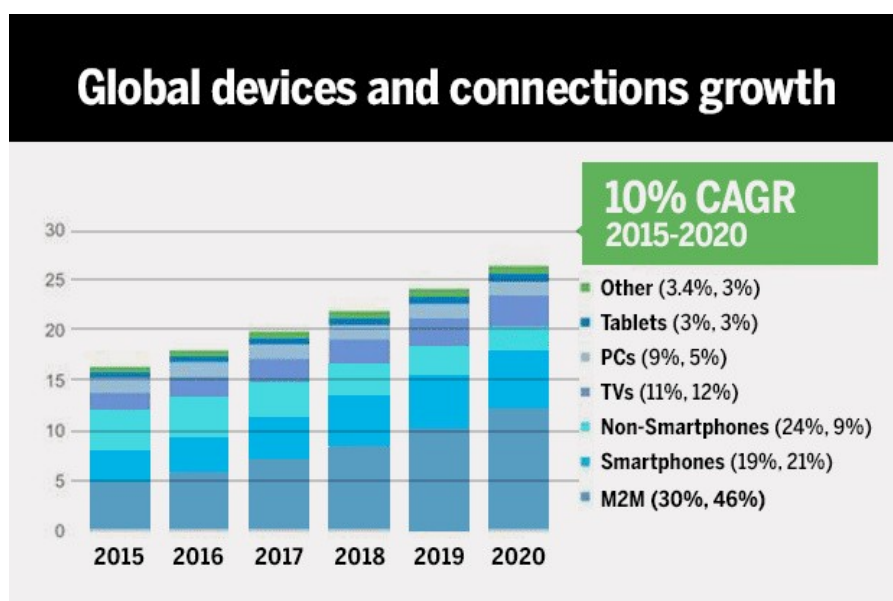
71 <https://www.gartner.com/newsroom/id/3144217>

the cumulative number of information increases and sector based because not all the sectors can be easily conceived as being information intensive⁷².

-

1.6.3 Privacy and transparency issue: the surveillance society

While I'm writing, 3,9 billion internet users are spread around the world, and 2018 will be the year of the 4 billion target reach⁷³. The world is becoming increasingly connected



and thus is becoming everyday more concerning the need to establish a set of rules that can grant privacy protection on an individual side as well as requiring transparency on the institutional side; the two concepts go together, requiring balance⁷⁵. Several scandals concerning “privacy breaches” have occurred, but when it comes to reveal something, it always happens because there is someone (take the example of a whistleblower) who feels there is something to be revealed to the public and to be used as a megaphone to “let people know”. Again, privacy and transparency are two sides of the same coin, and must be treated together. Concerning actual use cases, we only need few examples: let's take WikiLeaks and Cambridge Analytica scandals. I consider those 2 cases as a megaphone for privacy and transparency awareness nowadays.

72 <https://hbr.org/1985/07/how-information-gives-you-competitive-advantage>

73 <http://www.internetlivestats.com/internet-users/>

74 <https://www.networkworld.com/article/3080001/lan-wan/cisco-ip-traffic-will-surpass-the-zettabyte-level-in-2016.html>

75 https://www.huffingtonpost.com/don-tapscott/why-transparency-and-priv_b_643221.html

1.6.3.1 Cambridge Analytica

For what concerns Cambridge Analytica⁷⁶ we are in front of a watershed: the shift from the use of data as a value-creator to be “sold back” to owners with means of better products or services to the use of it as a way “to change audience behavior”⁷⁷. We’re in the Big Brother era, with the remarkable upgrade of having certainties on this affirmation on public web home pages (that of Cambridge analytica itself!) instead of being hidden in secret places. The way Cambridge Analytica database works and has been constructed departed from Professor Kogan studies about psychological traits, namely “psychographics”⁷⁸. Several early studies from Cambridge University itself demonstrated the strong correlation between the information that can be harvested from Facebook and the power to predict behavior⁷⁹. What is remarkable in here is the further step made, which is the production of tailor made information pools through the creation of blog, websites and so on to be brought to target “receptive people”⁸⁰ to alter their perception of things as a result of their culture. Cambridge Analytica ventured the step of re-defining society through the influence of culture. Following Cambridge Analytica whistleblower’s words, perceptions are the result of culture, so that if you want to alter perceptions, you first have to alter their culture, and the only way to do is to make them focus on receptive signals. Here below is shown the graph that demonstrates how advanced analytics could identify people lives in a very accurate way, simply using everyday social information.

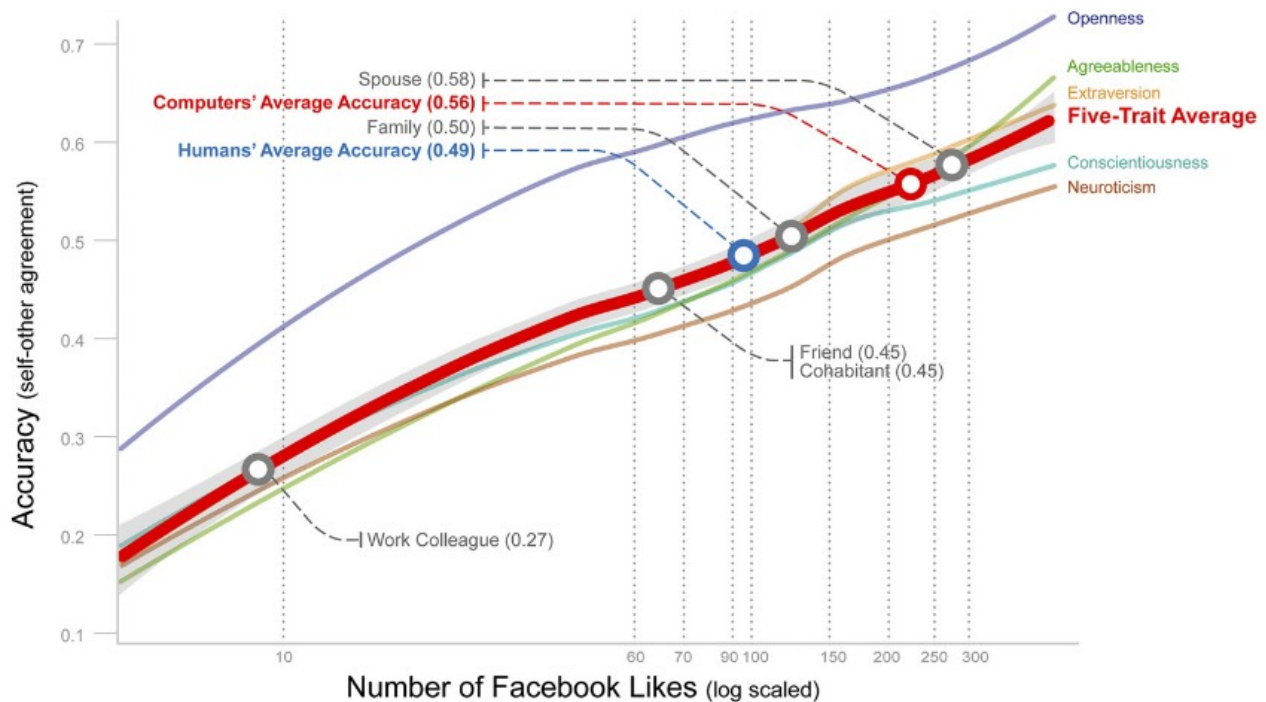
76 <https://hackernoon.com/facebook-data-scandal-50eedc7762b6>

77 <https://cambridgeanalytica.org/>

78 <https://en.wikipedia.org/wiki/Psychographics>

79 <http://www.pnas.org/content/pnas/112/4/1036.full.pdf>

80 <https://www.youtube.com/watch?v=FXdYSQ6nu-M>



But what is the relationship between Cambridge Analytica and the birth of Blockchain? Well, there are many “heards” about Cambridge analytica planning an Initial coin offering⁸² even before the scandal, in order to let users cash in their personal information with a virtual currency, allowing the company to pass from “poacher to gamekeeper”. This is the demonstration that if privacy and transparency is the issue, Blockchain applications like Initial coin offerings are the first way through which these problems can at least tried to be solved. How? ⁸³ Every type of central decision is subjected to “bottleneck” problems. Simply reshaping the way decision is taken, allows to subtract the power of a central authority to choose for someone other, preventing in a way all the possible problems encountered.

1.6.3.2 WikiLeaks

Everybody has listened about this argument. Wikileaks first appearance dates back to 2006, when the founder Julian Assange registered the site domain on 4 October. The main purpose of Wikileaks could be said to bring truth to people, and truth could be the answer to a lack of transparency.

81 Ibid.78

82 <https://www.icoexaminer.com/ico-news/cambridge-analytica-was-planning-data-privacy-ico-before-facebook-saga/>

83 <https://medium.com/deep-code/lets-get-this-straight-bitcoin-is-an-experiment-in-self-organizing-collective-intelligence-52d78212c5e6>

Again, what is the interconnection between WikiLeaks and Bitcoin birth? First, Julian Assange is a Cypherpunk, as he even wrote a book sustaining cryptography reporting the movement's name⁸⁴.

What Assange sustains is that Bitcoin provides basically two essential tools: cryptography as “a key weapon in the fight against empire states”⁸⁵ and timestamping⁸⁶. When he speaks about timestamping, he uses this argument to demonstrate how important is to have an information that can directly be brought to the masses and allow to solve “a mass problem” together with masses and not for the masses, in the way that is retained to be better for a central authority. Bitcoin serves as a transparency tool to verify information reliability, something that can, restating Assange words, allow “to fight bias with another bias working in the opposite direction”. Last but not least, Assange had to fight against what he was calling a “financial blockade”⁸⁷ that brought payments companies to shut payments to Wikileaks. The blockade cut up to 95% percent of the revenues which served to finance new leaks, and that brought to Assange the emergency to find alternatives. This event, triggered the last “public” words of Satoshi Nakamoto as an answer to a user who was proposing to WikiLeaks to use Bitcoin as a tool to bypass the blockade: “No, don't bring it on. The project needs to grow gradually so the software can be strengthened along the way. I make this appeal to WikiLeaks not to try to use Bitcoin. Bitcoin is a small beta community in its infancy. You would not stand to get more than pocket change, and the heat you would bring would likely destroy us at this stage”⁸⁸.

As an answer, Assange decided not to use Bitcoin until the concept was already in a more mature stage and already has its first skyrocketing price events in 2011⁸⁹. Indeed, Satoshi's concern was about the protocol infancy, which, at his advice, could have put too many spotlights by governments in an early stage tool and this could probably have mined its existence.

Conclusion: This set of subsequent elements of matters and reactions to matters seem to be a “block of the same chain”, a set of events which range along a continuum of the same history. What I want to mean by that is that when transparency was an issue, Assange was already thinking of Bitcoin as a good way of enhancing it, and Cambridge analytica was already planning an ICO before the scandal of the data breach because was in a way “concerned about others' concerns”. Questions: Privacy and transparency. Possible answers: Bitcoin and cryptocurrencies.

84 [https://en.wikipedia.org/wiki/Cypherpunks_\(book\)](https://en.wikipedia.org/wiki/Cypherpunks_(book))

85 <https://www.theguardian.com/commentisfree/2013/jul/09/cryptography-weapon-fight-empire-states-julian-assange>

86 https://www.youtube.com/watch?v=MaB3Zw5_p9c

87 <https://wikileaks.org/Banking-Blockade.html>

88 <http://satoshi.nakamotoinstitute.org/posts/bitcointalk/523/>

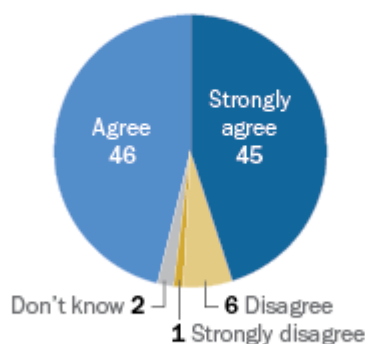
89 <https://www.ccn.com/wikileaks-julian-assange-may-have-saved-bitcoin/>

1.6.3.3 Do we really care about privacy? Few thoughts

Authoritative researches and dedicated databases have demonstrated how we easily and partly unconsciously left the use of our information to third parties without asking ourselves what was the consequence of such an infinite flow of mono directional information, from people to corporates or governments.

Large Majority Says Consumers Have Lost Control of Personal Information

% who ___ that consumers have lost control over how personal information is collected and used by companies



Source: Pew Research Privacy Panel Survey of 607 adults ages 18 and older, January 2014.

PEW RESEARCH CENTER

90

In particular, we've done it so deliberately, that now we declare ourselves incapable of ensuring the proper collection and prevention from misuse of our personal information. Do you care about privacy? Yes of course! Did (I) you ever shared personal information on the internet? Of course yes!⁹¹ The main answer to the question about the privacy issue is that there are many different levels of knowledge with respect to privacy norms. People accept cookie policies but don't know what cookies are. People don't read Facebook terms of use and privacy policy but pretend to be protected. A study demonstrates how countries that trust Facebook the most are also those in which more of Zuckerberg "mistakes" happen⁹², suggesting that privacy will be tailor made according to the "good enough" level required by the context of application. Those issues have to be defined on a

90 <http://www.pewresearch.org/fact-tank/2015/01/16/privacy/>

91 <https://www.forbes.com/sites/gregsatell/2014/12/01/lets-face-it-we-dont-really-care-about-privacy/#3d584e2e5698>

92 https://www.researchgate.net/publication/205694735_Users_Awareness_of_Privacy_on_Online_Social_Networking_sites_-_Case_Facebook

company level, and people have to trust the way companies behave. Even if the trend is to decentralize decision making, not everything can be passed to this new logic in a day, and requires corporates to think about problems before they have to face it⁹³. The new General data protection regulation enforceable from the end of May of this year, brought even more to public interest this issue⁹⁴, and here we see how companies are unprepared to face problems they never doubted should have been managed. What is remarkable is that Blockchain is both solving GDPR requirements as well as breaking them totally from the other side. The issue in here is that while the regulation clearly requires personal data to be kept as long as they are needed and then erased the very following moment they go “out of scope” and accessed by the owners of that specific piece of information whenever is required, from the other side we deny the possibility to erase personal information, with Blockchain being an unremovable stream of sequential data, so that eliminating “a chain” in the Blockchain is impossible, because every information hashed is locked forever in it. I personally believe that the set of different technologies that are coming out from nowadays technology development will increasingly allow us to combine them in the way we want to allow different customized level of privacy, but even for this reason, we need a way to manage those levels accordingly, being Blockchain a possible solution that anyway runs the big problem of having shown its power only after regulations have been implemented in those arguments.

1.6.4 Financial crisis as proof of concern

The proof of the fact that Satoshi Nakamoto’s Bitcoin conception was in a way a rebellion to the traditional financial system is contained in the first block ever created: the genesis one⁹⁵. In the first block, he included an article of Financial Times⁹⁶ speaking about the United Kingdom bailout proposed by the government, something that sounded to him like the proof of the fact that the power to decide needed to pass from central authorities to people.

93 <https://towardsdatascience.com/how-Blockchains-will-enable-privacy-1522a846bf65>

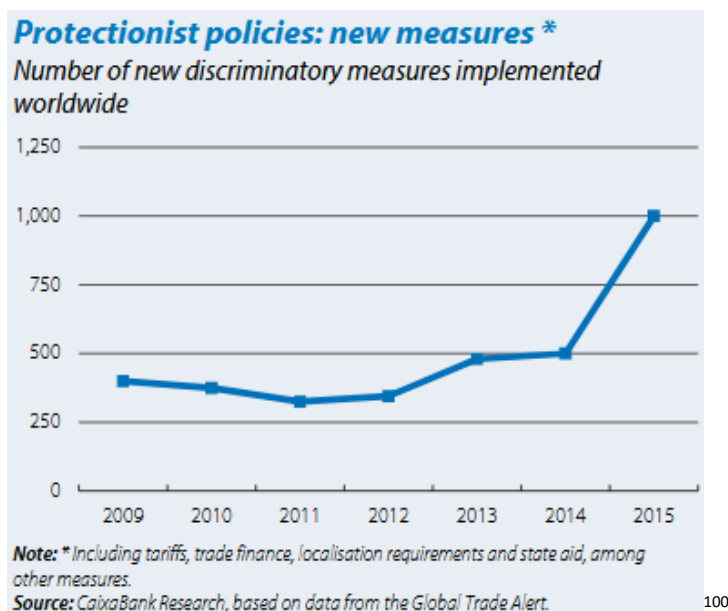
94 <https://medium.com/wearetheledger/the-Blockchain-gdpr-paradox-fc51e663d047>

95 https://en.bitcoin.it/wiki/Genesis_block

96 <https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n91382mn62h>

1.6.5 Globalization as a decentralization enhancer

In my opinion, Bitcoin as a decentralized network in which people can freely exchange money without intermediation is the extreme consequence of the globalization process. The never doubted liberism concepts like decentralization and the deregulation of international markets, brought to the birth of an extremist freedom of trade which in a way empowered the disruptive idea of Bitcoin. Studies are still being conducted to demonstrate the active role of globalization as a booster for decentralization, especially in small countries with open democracies⁹⁷. As a consequence, no matter what I think about it, I would blame those who fear the disruptive technology of Bitcoin as a threat for future economy, because it is the (for sure one of the most perverse, I agree) result of what the decentralization process sustained for years. Anyway, decentralization can't be considered tout-court as the opposite action of centralization, because both are needed⁹⁸, the issue is rather to determine what is the "gold share" of the two systems and in what way to make them better coexist. As a demonstration of the mistake in considering the two terms as opposite, if globalization brought to decentralization and offshoring, the result would be that central governments should have abandoned the market and cut interventions, while instead they became increasingly important in attracting capitals and investments from the world⁹⁹ and implementing a new wave of protectionist measures worldwide.



(Protectionist measures since 2008 by the G20 countries)

97 <https://www.bcg.com/publications/2017/new-globalization-going-beyond-rhetoric.aspx>

98 http://web.undp.org/evaluation/documents/decentralization_working_report.PDF

99 <https://shahrulsufianhamdan.wordpress.com/development-studies/has-the-nation-state-become-more-or-less-important-in-the-era-of-globalization/>

100 http://www.caixabankresearch.com/sites/default/files/documents/16_focus_4_ing_eng_0.pdf

1.6.6 Millennials drive the new emerging markets

Socio-economical change and emerging technologies success and adoptance are also a matter of time and generations¹⁰¹. In particular, an emerging generation is considered to be the driver of social and technological change nowadays: millennials or Gen Y. Millennials are those who approximately (there are different time ranges considered for classification) born from 80's to the new millennium.

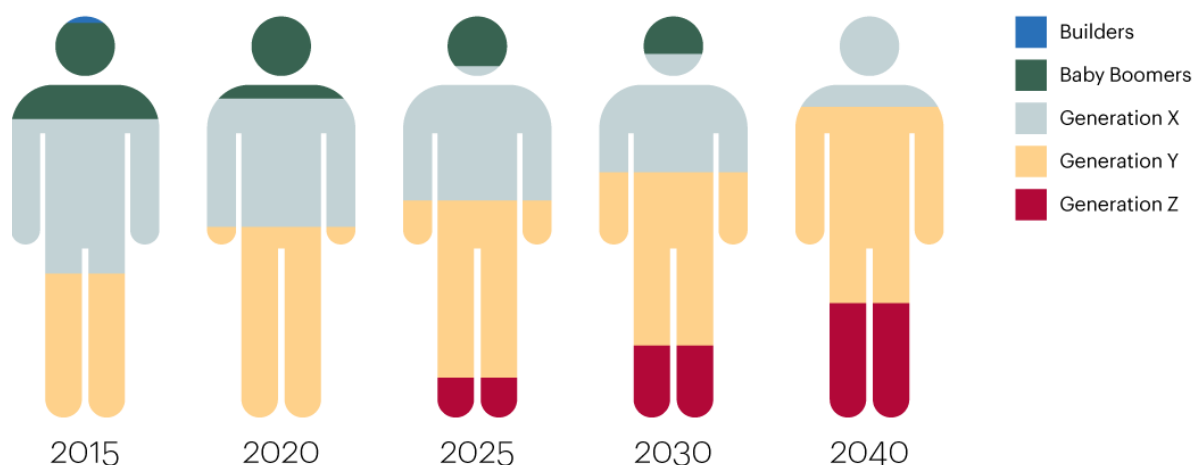
	GI GENERATION	SILENT GENERATION	BABY BOOMERS	GENERATION X	MILLENNIAL GENERATION	GENERATION Z
Years	Born before 1936	1937-1945	1946-1964	1965-1976	1977-1993	1994-
Ages	76+	67-75	48-66	36-47	19-35	18 and younger
Major Events	WORLD WAR II GREAT DEPRESSION	WORLD WAR II GREAT DEPRESSION ADVENT OF TV, TELEPHONES	CIVIL RIGHTS WOMEN'S LIBERATION COLD WAR	VIETNAM WATERGATE ADVENT OF MTV	AIDS TECHNOLOGY	9/11 IRAQ/ AFGHANISTAN WARS MARKET CRASH
Major Traits	FORMALITY UNIFORMITY COOPERATIVE PUBLIC INTEREST OVER PERSONAL GAIN	RESPECT FOR AUTHORITY LOYAL HARD WORK	EXPLORE OPTIMISTIC WORK-CENTRIC	INDIVIDUALISTIC FLEXIBLE SKEPTICAL OF AUTHORITY	TECH- COMFORTABLE FAMILY-CENTRIC OPTIMISTIC	MISTRUST IN POLITICAL SYSTEMS ALWAYS CONNECTED MULTI-TASKERS

102

This generation is expected to account for half of the world population and being 75% of the workforce, so they're expected to be the drivers of change.

101 <http://www.bizcommunity.com/Article/196/163/164811.html>

102 <http://www.thindifference.com/wp-content/uploads/2013/04/Generations-Healthcare.jpg>

Millennials will comprise the majority of the workforce by 2025

Source: U.S. Census Bureau

103

Describing them, one could start from “debunking stereotypes”¹⁰⁴: unhappy, lazy, social dependant people who are financially illiterate and can’t deal with an increasingly complex world. Several and authoritative researches mostly debunk those stereotypes and try to classify the generation objectively. Millennials in US for example, are a highly educated generation, this has partly caused the necessity to go into debt to pay studies, thus, the key concern for a millennial is to pay down debts (43% consensus), and secondly, to save for the future (38%).¹⁰⁵

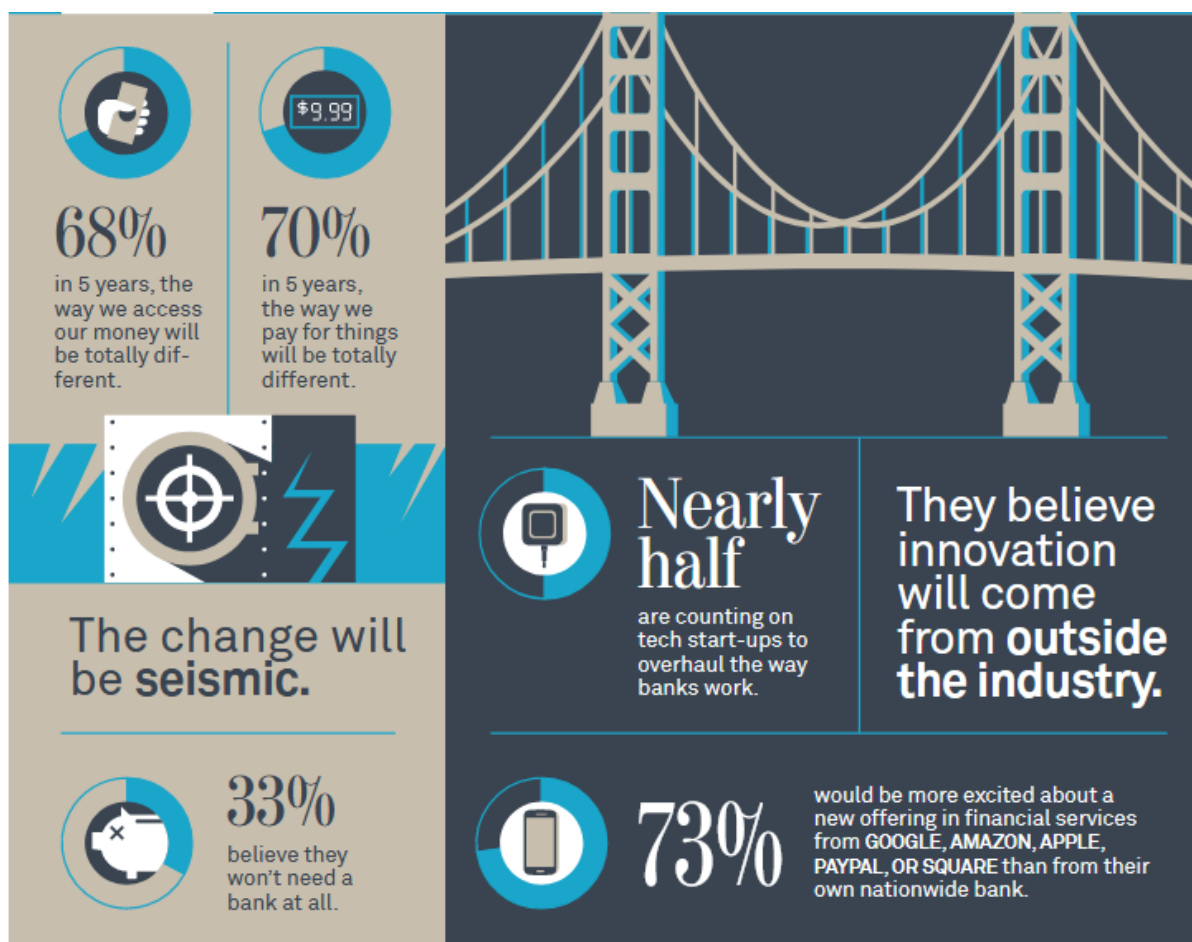
The first contradiction in here is that, despite their needs, much of them don’t have a financial plan for the future (only 37% have one), but they think about short term trends, avoiding long term investments. A second argument is that they don’t invest much, half of them justifying it as a consequence of lack of money and nearly one third of them self declaring a lack of investment knowledge. Regarding their relationships with banks, they expect 3 basic things from them, equally weighting: loyalty, convenience and honesty, being this last quality of double importance with respect to past generations. For what concerns their future view, they see the financial system as a completely changed panorama over 5 years, they tend to prepare to a new way of making payments, even making them with new re-engineered intermediaries such as already existing companies like

103 http://www.atkearney.com.au/about-us/diversity-inclusion/women/research-benefiting-women/additional-research/-/asset_publisher/KKytLSsPNuwg/content/gender-matters-for-generation-y/10192?inheritRedirect=false&redirect=http%3A%2F%2Fwww.atkearney.com.au%2Fabout-us%2Fdiversity-inclusion%2Fwomen%2Fresearch-benefiting-women%2Fadditional-research%3Fp_p_id%3D101_INSTANCE_KKytLSsPNuwg%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1.

104 <https://medium.com/the-mission/the-14-most-destructive-millennial-myths-debunked-by-data-aa00838eecd6>

105 https://fbinsights.files.wordpress.com/2016/01/facebookiq_millennials_money_january2016.pdf

Amazon, Google and Apple.¹⁰⁶ What is remarkable is that they practically don't care about banks, arriving to the point to say that is more interesting to go to the dentist with respect to listening to a banker's speech¹⁰⁷!! Put simply, millennials have new needs¹⁰⁸, the way the world has changed economically brought them to think about social relations in a different way¹⁰⁹ and the way they're looking to traditional banking system is dramatically fostering the need to the whole financial sector re-engineering, both by eliminating disintermediation and shifting from existing players to new ones.



©2013 Viacom Media Networks¹¹⁰

106 <https://cointelegraph.com/news/the-millennial-generation-bankings-big-problem-and-its-a-good-thing>.

107 <http://time.com/40909/why-millennials-would-choose-a-root-canal-over-listening-to-a-banker/>

108 <https://www.forbes.com/sites/danschawbel/2015/01/20/10-new-findings-about-the-millennial-consumer/#6b88341a6c8f>

109 <http://www.goldmansachs.com/our-thinking/pages/millennials/index.html#chart2>

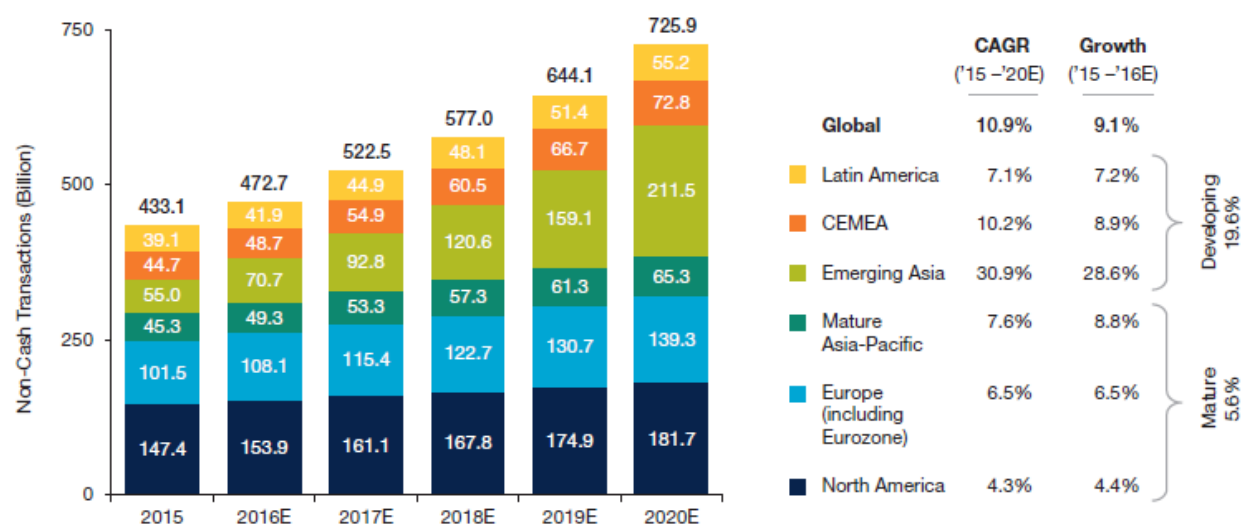
110 <https://www.bbva.com/wp-content/uploads/2015/08/millennials.pdf>

Banks will be “digitally disrupted and reimaged”¹¹¹, but that doesn’t mean that they’re doomed to disappear, for sure they can’t wait and see, indeed they created a powerful consortium of banks¹¹² which actually works in the direction to transform this technology threat of being substituted by smarter intermediaries or new ways of conceiving intermediation in an opportunity to lower the cost list and improving the already low margins with which they operate nowadays.

1.6.7 Trends in the use of paper money: The cashless society

Payment methods rise and widen its possibilities ranges (especially mobile and e-payments), and as a consequence, physical money is no longer an unsubstitutable need, but it still accounts as the main payment method used worldwide. By the way, we’re assisting to a general unrestrainable shift from cash payments to non-cash ones. If you only think about the various cash restrictions introduced last years in different countries, that’s the demonstration that states would like to at least let citizens pay with cards to avoid tax escaping.

Figure 2.1 Number of Worldwide Non-Cash Transactions (Billion), by Region, 2015–2020E



Note: CEMEA (Central Europe, Middle East, Africa) now includes Algeria, Bulgaria, Croatia, Kenya, Nigeria, Egypt, Israel, Morocco, and UAE in Other CE and MEA countries; Latin America now includes Argentina, Colombia, Venezuela, Chile, Peru, Uruguay, Costa Rica, Bolivia, and Paraguay in Other Latin American countries; Emerging Asia now includes Malaysia, Thailand, Indonesia, Philippines, Taiwan, Pakistan, Sri Lanka, and Bangladesh in Other Asian countries; Mature APAC (Asia-Pacific) includes Japan, Australia, South Korea and Singapore; NA (North America) includes the U.S. and Canada; Chart numbers and quoted percentages may not add up due to rounding

Source: Capgemini Financial Services Analysis, 2017; ECB Statistical Data Warehouse, 2015 figures released October 2016; Bank for International Settlements Red Book, 2015 figures released December 2016; Internal Estimates

¹¹¹ <https://capitalmarketsblog.accenture.com/wp-content/uploads/2015/04/Accenture-The-Future-of-Fintech-and-Banking.pdf>

¹¹² <https://www.r3.com/>

An analysis of the non cash share of payments in the world shows huge gaps between “early non cashers” and second comers.¹¹³ There are countries like Sweden in which the use of cash has decreased rapidly in the last decade¹¹⁴ and a shift from cash usage to the adoption of a digital currency is already being discussed (Riksbank proposed the adoption of a digital currency, the e-Krona¹¹⁵, a FedCoin is at its experimental stage in U.S...). Anyway, other countries still struggle with the need to pass from cash to electronic payments. There is something to say about the causes of this phenomenon. Cash usage is influenced by the population density, which strictly results in a lower/higher cost of cash distribution, the higher the competition in banking sector, the higher the proportion of non cash payments, and lastly, being ready to new technologies adoption is for sure a good pre requisite¹¹⁶. Technology adoption has dramatically speeded, and countries are everyday more forced to join the “new technologies” world as soon as possible to keep the pass, while the payment market is favouring the rise of new players and fosters competition¹¹⁷. The level of cash usage in a country is directly related to the number of alternatives proposed to cash ¹¹⁸, and it differs from market to market, causing the phenomenon to be sometimes differences in its causes but for sure being a monotone one worldwide, with few exceptions. What is indeed clear is that paper money is becoming obsolete. 300 means of payments are estimated to exist worldwide¹¹⁹ that we can’t even imagine, while cash still the dominant way of payment. Furthermore, the pass we’re keeping with technology, will let us to live in an increasingly connected world, with a growing number of connected devices per person¹²⁰. Consequently, the number of “connected actions” we are provided with nowadays, will increasingly require the need to think about using as a mean of payment something which could easier and with nearly real time communicate on the same level playing field of technology. To conclude, the shift that cashless share of payments will keep, is strictly correlated with the level of trust in each country, so that low levels of trust can in a way

113 <http://res.cloudinary.com/yummyshojin/image/upload/v1/pdf/future-of-payments-2016.pdf>

114 <https://www.weforum.org/agenda/2017/09/sweden-becoming-cashless-society/>

115 <https://www.riksbank.se/globalassets/media/rapporter/e>

[krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCf%3d%3d&_t_q=CASHLESS&_t_tags=language%3aen-GB%2csiteid%3af3366ed3-598f-4166-aa5a-](https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCf%3d%3d&_t_q=CASHLESS&_t_tags=language%3aen-GB%2csiteid%3af3366ed3-598f-4166-aa5a-45d5751e940b&_t_ip=31.27.212.193&_t_hit.id=Riksbanken_Core_Models_Media_DocumentFile/_108866a5-a031-4de8-a6cb-9403dff9d355&_t_hit.pos=2)

[45d5751e940b&_t_ip=31.27.212.193&_t_hit.id=Riksbanken_Core_Models_Media_DocumentFile/_108866a5-a031-4de8-a6cb-9403dff9d355&_t_hit.pos=2](https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf?_t_id=1B2M2Y8AsgTpgAmY7PhCf%3d%3d&_t_q=CASHLESS&_t_tags=language%3aen-GB%2csiteid%3af3366ed3-598f-4166-aa5a-45d5751e940b&_t_ip=31.27.212.193&_t_hit.id=Riksbanken_Core_Models_Media_DocumentFile/_108866a5-a031-4de8-a6cb-9403dff9d355&_t_hit.pos=2)

116 <http://www.g4scashreport.com/-/media/g4s/cash-report/files/2018-world-cash-report---english.ashx>

117 https://www.capgemini.com/wp-content/uploads/2017/12/payments-trends_2018.pdf

118 <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1685.pdf>

119 <http://www.worldpay.com/sites/default/files/Worldpay-APM-Brochure-EN-u18.pdf>

120 <https://www.futurelearn.com/courses/data-explosion/0/steps/29736>

slow the cashless payments trend, identifying in material, physical money the only tangible way to trust our own wealth.

1.7 Trust and Bitcoin birth

Bitcoin whitepaper describes the protocol as being the first “trustless” one. We can affirm that this statement is partially misunderstood by people supporting Bitcoin. It’s obvious, and researches demonstrate it, that we can’t straightforwardly eliminate trust as a lubricant for all type of interactions, both lucrative and social, because trust is essential to build every type of interaction. It is better to say that Bitcoin is trustless in the sense that it eliminates the need to trust a third party as a necessary mean through which individuals can deal, but it doesn’t abolish trust altogether, it rather transforms the way it can be expressed, and the way it can be expressed is considered as being the technology behind it: Blockchain. We ‘re assisting to an immature but still present tentative to an irreversible shift in the trust paradigm, in which this latter could eventually pass from people hierarchically located in centralized institutions to “peers in a decentralized network”.

2. Chapter 2 ICO market overview

2.1 Introduction to Initial coin offerings

Before dealing with Initial coin offerings, it must be disclosed the fact that this is a nascent market, thus, there is no strong agreement in terms of definitions used and consequently on methods used to analyze, categorize and then evaluate them. In this chapter, I will try to introduce what is my vision of the phenomenon and what are its best suitable definitions and the tools to analyze it, and then try to give a definition of it.

2.2 What is an ICO

Starting with a very broad definition, Initial coin offering is the name referring to literally a public offering within which investors can make their own contribution over a blockchain based “coin” issued and contribute in a company’s project launch. There are many attempts from contributors with very different backgrounds to give a definition of the phenomenon, departing from different observation points to be as much comprehensive as possible, with the result that being the definition simply enlarged from a restrained perspective, is by consequence not exhaustive and (only) artificially right. One focuses on the “means of payment” side of ICOs¹²¹, one focuses on the legal framework to be adopted¹²², one focuses on the comparison between traditional financing means¹²³ like Crowdfunding, Venture capital and IPO and treat them having in mind their affinities. As far as I’m concerned, this phenomenon is so immature that people still focus only on a part of what they personally believe is its core part, and by departing from that, they try to generalize the framework, losing the opportunity to create a comprehensive view of the phenomenon, which I retain is the most consistent way to be adopted in order to clarify many aspects of this latter. The reasoning is that I retain far better to have a comprehensive and verified logic (at the expense of some detail) to be adapted to the whole instead of having few detailed issues without any sort of well defined relationship between the items composing ICOs. In order to do so, I will try to take what I retain to be an ICO minimum content to be analyzed and then I will try to go as much as possible into details.

121 <https://blockgeeks.com/guides/initial-coin-offering/>

122 <https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/regulation-initial-coin-offerings>

123 <https://www.nytimes.com/2017/10/27/technology/what-is-an-initial-coin-offering.html>

2.3 Difference between tokens and cryptocurrencies

Once said this, we have to clarify what really “coin” means and how the term “ICO” could be a misnomer¹²⁴ in the actual panorama. Briefly speaking, the term “coin” contained in the acronym could make one think that all of the ICOs consist in issuing one of this latter, which is to generate a cryptocurrency to be sold in order to finance projects. The first myth to debunk is that not all of the ICOs can be said to be a “pure” cryptocurrency offering. To be precise, we have to introduce a subtle but important difference between cryptocurrencies from one side and tokens from the other one that needs to be distinguished in order to set a proper organizational division of the means through which an ICO is financed¹²⁵. The issue in here is that the two terms are often used as synonymous while instead they have very profound differences between each other that many ICO investors still can’t distinguish clearly. Starting from tokens, they can be said to be a “stand in for something else”¹²⁶. Think about a transaction in your bank account, when you try to send money to someone else’s account, a token is generated. This token is basically a code generated in a sort of “randomizing” activity which lets this code be paired with your real IBAN id, so that when you execute a transaction, hackers wanting to alter the transaction won’t see your real IBAN id, but its randomized version. Dollars, Euros, or whatever is only a representation of an underlying value which is not directly linked to the commodity itself can be referred to as a token. When we buy something, we don’t buy it with the physical coin, but with the value the coin actually represents. Reasoning in these terms, even the whole crypto panorama can be said to be a “token world”, so that when we buy something with Bitcoin (or every other cryptocurrency or token) for example, we don’t really buy it with the coin directly but with an X amount of those “tokens” representing Bitcoins.

2.3.1 Blockchain layers

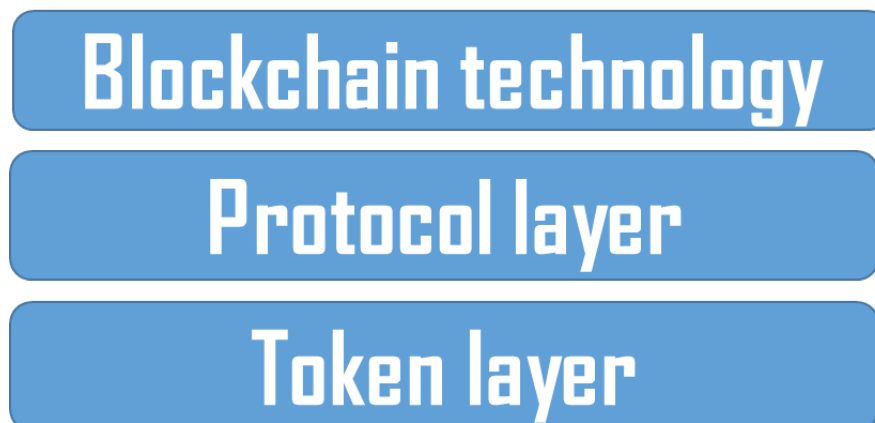
In order now to better explain what are cryptocurrencies and how they differ from what people call token, we need to clarify how they interact with Blockchain technology. Let’s refer to the diagram

124 <https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/>

125 <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-cons-new-paradigm.pdf>

126 <https://cryptocurrencyfacts.com/what-is-a-cryptocurrency-token/>

below to have a brief overview on the structure of Blockchain before going more in deep into the explanation.



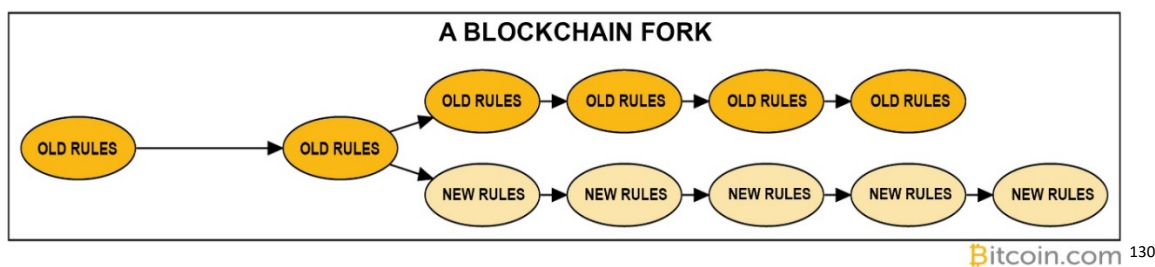
127

Blockchain is that new technology consisting in a new way of conceiving transaction in a chain of linked blocks that need to be validated with a consensus mechanism. Over that technology, a communication protocol is defined. Being more precise, a communication protocol¹²⁸ can be said to be a set of rules to be followed for a network using a specific Blockchain to work properly. Bitcoin's proof of work mechanism for example, could be said to be a part of the protocol, which is to say "every Bitcoin user will have to follow or be subjected to specific rules for the validation mechanism of transactions". Having a protocol, thus, is like having a pre-defined set of rules that require every transaction to be done according to those latter to work properly. Once said this, is clear how the way the protocol is defined inevitably shapes the way the cryptocurrency built within that set of rules is constituted and will work. Indeed, the cryptocurrency built in the Blockchain is even its first application, and it follows the rules the Blockchain has pre-defined in the protocol layer. After having created the first native application on this layer of the technology being the cryptocurrency itself, new applications can be built on top of the protocol without altering its content, which is to say that we're using a different layer of the technology to build them. That other layer, is that one on which "tokens" can be created, and we can state that is the "token layer". Thus, the main difference between cryptocurrencies and tokens is that while cryptocurrencies are native standalone tokens built within the existing protocol of a Blockchain, tokens instead work in a different layer of the Blockchain, which is that one governed by smart contracts, more on that later. Put in other terms, creating a cryptocurrency means to create a Blockchain that works the way the currency itself is intended to be validated by using a pre-defined protocol, so that should every other

127 Rework from <https://www.youtube.com/watch?v=pcilyT3fh-0&t=4s>

128 https://en.wikipedia.org/wiki/Communication_protocol

person want to conceive a new way for this coin to work on that Blockchain, a “fork”¹²⁹ is needed, with this term referring to the creation of a copy of that Blockchain, the modification of the protocol in a way which could make the old one invalid (hard fork) or to simply restrict the set of rules which this changed protocol had already embedded (with no need to invalidate the old ones) and run a newly issued Blockchain with those new characteristics (see figure below)



Tokens instead, as we already said, work on a different layer of the Blockchain which is not that one of the protocol, we could even invent different tokens which could be run on the same Blockchain without the need to modify the protocol. To conclude, having a token is like having a sort of secondary protocol to be executed within the primary one, that in which cryptocurrencies work. The difference between cryptocurrencies and tokens is simple but very much misunderstood or misused in the ICO debate. The term is misused in the sense that according to that reasoning, a token can be both considered as a way to identify every digital element in the Blockchain representing a string of data representing a claim, but it is also used as a way to distinguish standalone tokens being the cryptocurrencies themselves with “secondary tokens” built on the other layer of the Blockchain. The takeaway in here is that “all cryptocurrencies are tokens, but not all tokens are cryptocurrencies”.

2.4 Token classification framework

Now that we clarified what is the conceptual element to which investors can be entitled by participating in an ICO, and in order to establish a path to be followed to classify the rights and obligations connected to a token, a classification framework must be created. The most complete

¹²⁹ <https://www.coindesk.com/information/hard-fork-vs-soft-fork/>

¹³⁰ <https://news.bitcoin.com/a-guide-to-what-a-bitcoin-fork-is-and-why-they-happen/>

one describes it as having 5 main qualifiers that can occur cumulatively and that allows reliability in the categorization: Purpose, utility, technical layer, legal status, underlying value¹³¹ :

- **Purpose:** the purpose of a token could be said to be three faceted:
 - Cryptocurrency token: the purpose is to function as a lubricant for the Blockchain, or, if you want, as the incentive to use this latter.
 - Network token: they can be said to be a tool which allows users to participate in a determinate project and be allowed to buy and sell that instrument according to the position they want to cover with respect to the product or service offered
 - Investment token: they're considered to be a representation of a stake in a company, both from the asset side being the asset appreciation the objective of the investment, and from the equity side by allowing users to have “share like” characteristics.
- **Utility:** In terms of utility provided, a token could be considered as the mean through which to participate in the product or service utilization and/or development, in this case we call this a “usage token”; otherwise, it can be even considered as a mean through which to maintain the product or service still running on a Blockchain, which is to basically use the tokens as a reward for it, called “work token” (like Bitcoin being the incentive for miners on its Blockchain). Finally, “hybrid tokens” can be a mix of these two characteristics.
- **Underlying value:** the value deriving from a token is connected to the way the value is actually being reflected on this latter:
 - Asset backed token: if the value comes from a direct claim towards an asset which is backing the token.
 - Network token: if the value of the token is directly connected to its usage and correlates with the network value we call it as such .
 - Share-like token: if the token grants share-like characteristic like the right to be entitled to dividends it is obviously referred to as “share like token”.

¹³¹ <http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/>

- **Technical layer:** As we said before, the level of the technology over which a token insists shapes its nature as a token:
 - Native token: the first Blockchain usage conception
 - Non native token: the token built on top of the Blockchain,
 - dAPP: token conceived for decentralized applications.

- **Legal status:** Once said this, we can categorize with a good degree of reliability the type of tokens with which we are dealing, let's compare for example the Ether (Ethereum's Blockchain own cryptocurrency) and Bitcoin. Here below a brief example:

Token	Purpose	Utility	Underlying Value	Technical layer	Legal status
Bitcoin	Cryptocurrency	Usage	Network value	Native token	Cryptocurrency
Ethereum	Network token	Hybrid	Network value	Native token	Cryptocurrency

132

2.5 ICO structure

For what concerns the structure of an ICO, being the market still very unregulated, there is no fixed structure, but there are some commonalities that can be highlighted¹³³. Normally, a funding process starts with the announcement to the public of the intention to run an ICO and possibly to collect opinions from interested people to eventually modify some aspects of the project. In a further step, the company describes the main detail of the offering and announces a set of steps to approach the ICO, including the project characteristics, the token sale date and the duration. Contemporarily, the company's creating the official document on which to report all the project details, we call it whitepaper. The funding process, then, can be divided as such¹³⁴:

- **Pre announcement:** like all the steps made in this open space technology, all starts with a proposal made in official channel, in which the group of developers try to convey through an

132 Rework

133 whitepaperdatabase.com

134 <https://medium.com/@rilcoin/what-is-an-ico-initial-coin-offering-and-how-does-it-work-42abfd0e7d26>

executive summary as much information as possible about the ICO project and its main functionalities, to get feedbacks and improving the project in a loop which ends up in the moment in which the developers team is able to go for the offering and has encountered as much demand as possible.

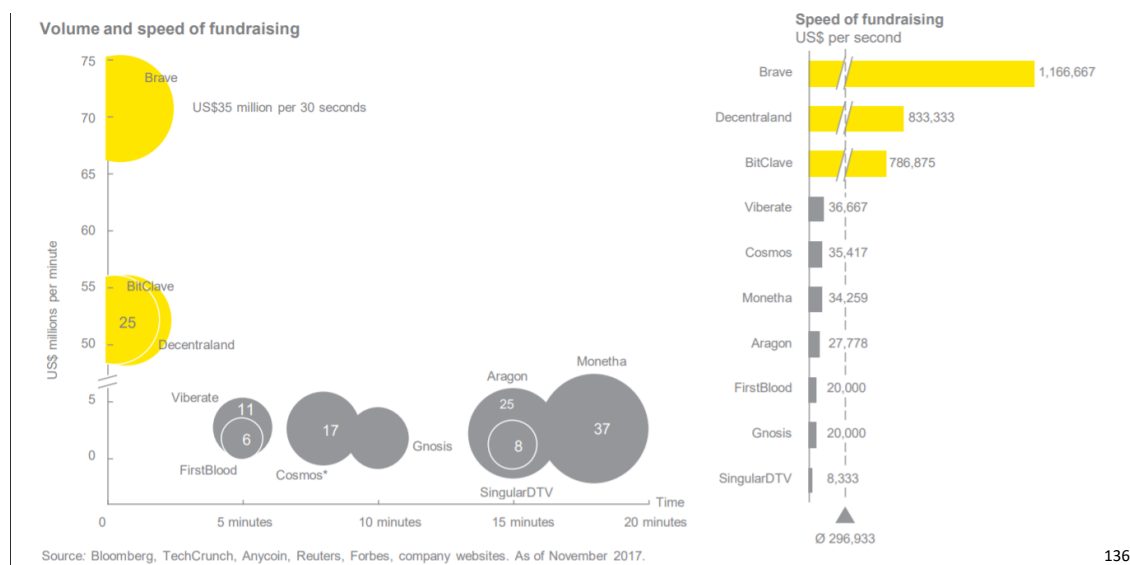
- **Offering:** the Team goes for the publication of a Whitepaper, which is the equivalent of what a mandatory prospectus is for IPOs, the difference is that while the mandatory prospectus obviously requires a minimum content for the offering to be legally documented, ICO's whitepaper's still not regulated, so that every team basically publishes its own vision of the financing event and include very different information, ranging from more technical ones to simply marketing statements to promote the campaign as much as possible.
- **Running Project campaign:** The company is now trying to market its offer as much as possible via communication channels like Facebook, Twitter, Telegram. The aim in here is to convince new investors about the quality of the ICO, by answering questions like: What problems this ICO project wants to solve? Why there is the need to use the Blockchain to solve such a problem? Who are the people involved in the team? What will be the result of the start-up reaching its business goals in the long term?
- **ICO sale:** Once all is set, the sale starts, and investors try to obtain a stake in the offering by submitting requests.

2.5.1 Token sales structure

The main token sale options¹³⁵ are:

- **Capped sale:** The capped option is that one which is preferred in ICO funding, since it creates FOMO and stimulates investors to come and buy, with the result that the funding goals are achieved in matters of minutes (see figure below). Capped sales are also the more reliable financing mechanism according to investors, which are in a way given the guarantee that the project developers have at least an idea of what the project requires in terms of funds to be collected and possibly don't need to raise more money than required.

¹³⁵ <https://blog.coinbase.com/the-perfect-token-sale-structure-63c169789491>



136

- **Uncapped sale:** Uncapped sales show at least uncertainty about the bounty of a project, which resembles to a sort of game in which developer try to fund the project first and only after try to figure out how to spend those money. There is more, uncapped sale are in a certain way a problem for those investors which want to know how big will be their stake into the ICO, given the fact that buying 5000 tokens in a 500000 token offering is different from buying them in a 10000 one¹³⁷.
- **Capped auction:** people formulate their own bid, which is the maximum price at which they're willing to buy the amount of token declared. Once the cap is reached, the price at which the tokens will be sold will be the lowest bid which participated in the auction.
- **Uncapped auction:** Basically the capped auction without cap. Every investor can participate and get a stake in it.
- **Capped with re-distribution:** Investors submit their own total spend and will be endowed with a fix percentage (calculated on the basis of the total spend share among all the participants) of the offering at the end of the sale, with a partial reimbursement if the amount paid exceeds the token obtained.

136 [https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/\\$File/ey-research-initial-coin-offerings-icos.pdf](https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf)

137 <https://vitalik.ca/general/2017/06/09/sales.html>

- **Capped with parcel limit:** it is configured as being a first-come first-served distribution, with investors' stake limited in a fix amount they can afford, to prevent people being endowed with big stakes and possibly to alter market price of the tokens.

Here below a figure representing a summary of all the sales structures analyzed:

Objective	Token sale structure					
	Capped FCFS	Uncapped	Capped Auction	Uncapped Auction	Capped with re-distribution	Capped with parcel limit
Raise a capped amount	✓	✗	✓	✗	✓	✓
Sell a fixed percentage of total token supply	✓	✓	✗	✓	✓	✓
Promote wider distribution of tokens	✗	Some	✗	✗	Some	✓
Sell tokens at market price	✗	✗	✓	✓	✗	✗
Guarantee that all buyers will get some tokens	✗	✓	✗	✗	✓	✗
Enable buyers to buy an ascertainable percentage of the total token supply	✓	✗	✓	✓	✗	✓

138

2.5.2. Soft cap and Hard cap

Ico sales are in a way self-disciplined in terms of the amount to be collected. The soft cap is always defined by the developers to sometimes declare what is the minimum amount they're willing to obtain through the ICO sale, and they sometimes return funds to investors if this soft cap is not reached. The hard cap instead is the maximum amount they want to collect, and it is a limit in which capped sales stop their funding process and return the excess funds eventually taken from investors.

2.6 Global market growth

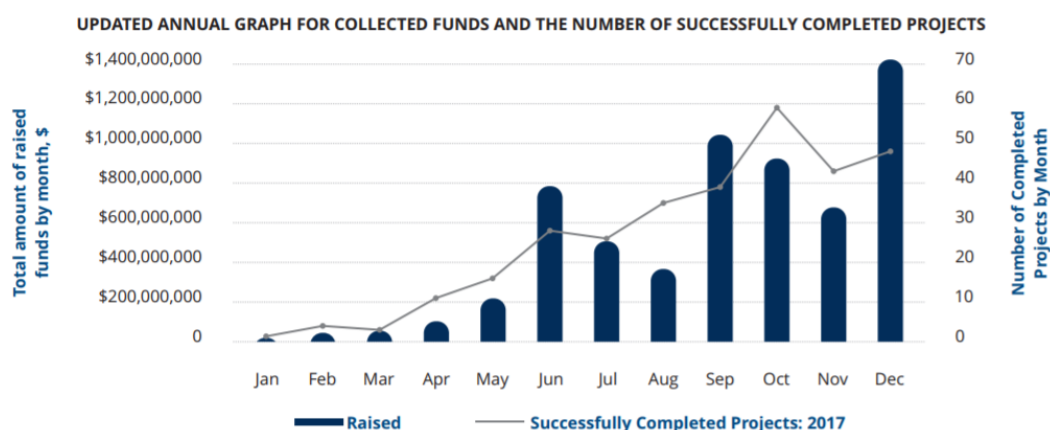
The data surrounding the ICO panorama's still fragmented and then hardly determinable, indeed, many databases report only a part of the ICOs occurred up to now. Since the birth of this new financing tool, up to today 4 August 2018, according to what I retain to be a good comprehensive

138 <https://blog.coinbase.com/the-perfect-token-sale-structure-63c169789491>

database¹³⁹, 4130 ICOs have been conducted (but the number is for sure underestimating the phenomenon), with roughly a cumulative 29 billion raised with that instrument. Being the phenomenon really at its first phase, there is a monotonous positive trend towards the growth of that market, yet having to underline that being the market small in terms of capitalization, the success or the failure of one or more “bigger” ICOs could lead to keep the positive trend on-going or to significantly shrink, to figure out why, the biggest ICO ever reached a stunning 4,1 billion financing, which is basically one fifth alone of the total 2018 funding up to now. The phenomenon is literary exploded in 2017, so that we have to take into account the relative dimensions of this latter and start from here to understand the phenomenon dimensions:

- 2017: ICO project reached an humble yet interesting cumulative funding of about 6 billion, with an increasing number of successful ICOs

NUMBER OF SUCCESSFUL ICOs AND CAPITAL RAISED IN 2017



* A project is considered to be successful if the soft cap was reached, or, if there was no soft cap, the project raised more than \$500,000.

140

Just to figure out how the trend is impressively keeping its pass, according to a smaller database¹⁴¹, of the 29 billion raised via ICO, the first semester of 2018 accounts for nearly 72% of the total amounts ever raised¹⁴². The average ROI obtained by ICOs in 2017 is 116,63%, with the best 10 projects reaching a 6 digits growth while the worst ones basically having no value left to be exploited.

139 <https://icobench.com/stats>

140 <https://icorating.com/pdf/1/1//mjL8hLbkOfPuJCo2KCKq6gPwZUYd72WZrGMSIeco.pdf>

141 <https://digrate.com/en/>

142

BEST ROI RESULTS AS OF 31.12.2017

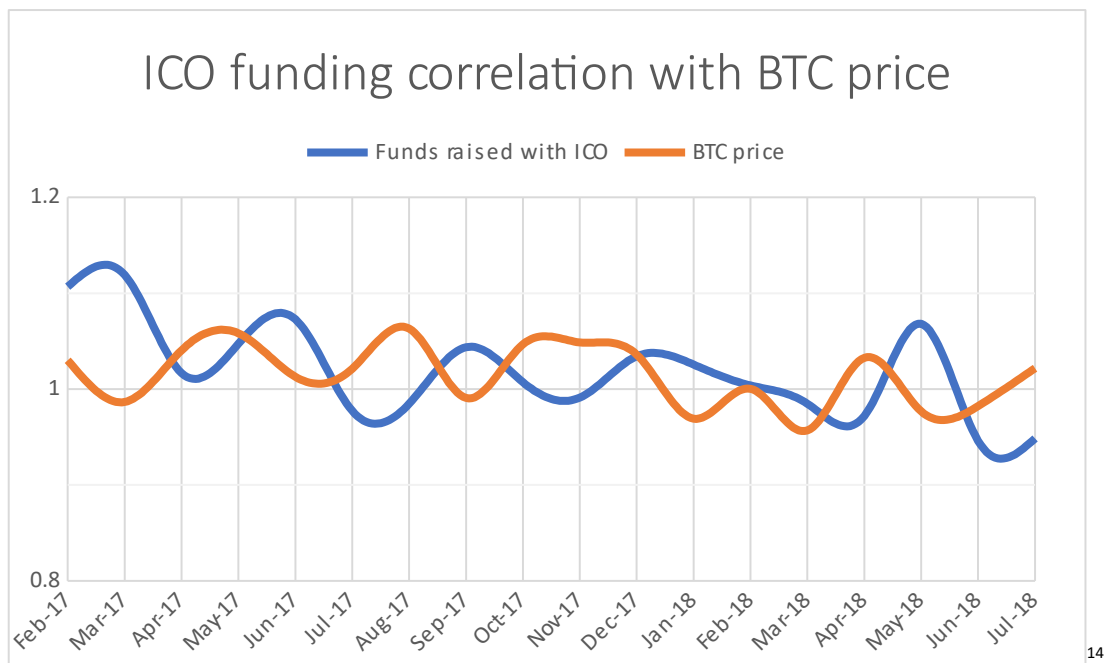
Project Name	Token	ICO token price, \$	Current price (2017/12/31), \$	ROI
Ethereum.link	LNK	0.0173	63.89	369206.36%
NEO	NEO	0.03	75.96	253100.00%
Lunyr	LUN	0.0227	23.33	102675.33%
ICON	ICX	0.01	5.35	53400.00%
Ignis	IGNIS	0.04	14.25	35525.00%
Populous	PPT	0.25	41.53	16512.00%
Matchpool	GUP	0.0083	0.877876	10476.82%
OmiseGO	OMG	0.35	19.89	5582.86%
Edgeless	EDG	0.04	2.25	5525.00%
Wings	WINGS	0.028	1.27	4435.71%

WORST ROI RESULTS AS OF 31.12.2017

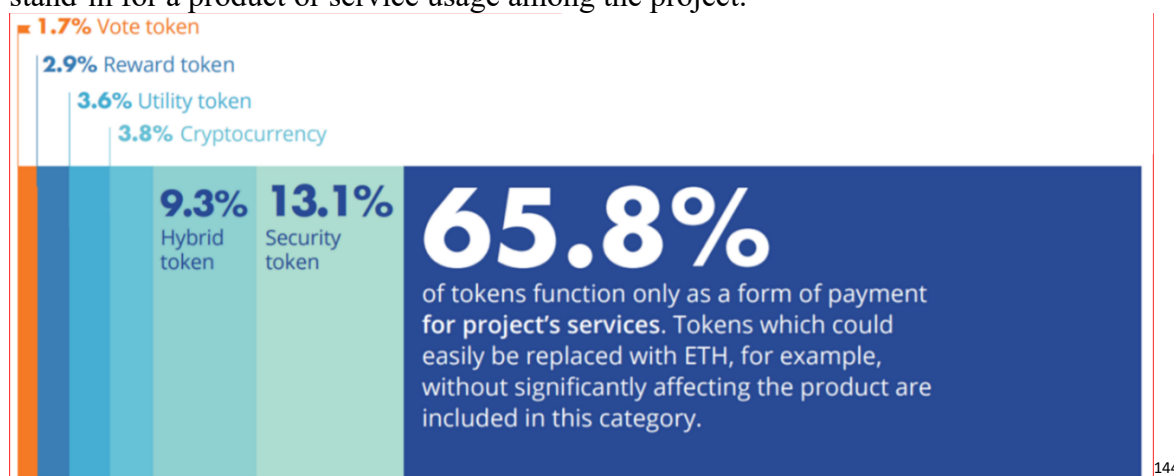
Project Name	Ticker	ICO token price, \$	Current price (2017/12/31), \$	ROI
DS Plus (PlusCoin)	PLC	13	0.000742	-99.99%
PLUSCOIN	PLC	10	0.000742	-99.99%
EncrypGen	DNA	2843	0.688885	-99.98%
BlockMason	BCPT	307.35	0.456501	-99.85%
Bolenum	BLN	5.76	0.023157	-99.60%
E4ROW	E4ROW	13.24	0.088776	-99.33%
OX Fina	OX	0.07	0.000497	-99.29%
Hero	play	2.5	0.020260	-99.19%
Facecoin	FC	1.4	0.012987	-99.07%
Gimli	GIM	2.03	0.059372	-97.08%

In this overview, it is clear how there is at least a clear tendency of successful ICOs to have a very low pricing in the ICO stage while worst results ones having very expensive prices. Indeed, 83% of exchange listed tokens trade below their ICO price. There is still too much noise to clearly understand how an ICO can deliver value. One example is sufficient to clarify this statement. The peak amount of ICO funding reached its peak in the same peak phase of Bitcoin reaching 17 thousands dollars worth, and if we assess the monthly correlation between those two trends starting from 2017 to date, we see a -10,31% linear correlation between them. Of course, the linear regression mustn't be used as a proof for funds being collected because of Bitcoin price, but looking

at the graph there must be a relationship other than a linear one that could describe the fact that when Bitcoin price goes up, funds collected rise again with a little lag with respect to price increase, and funds collected start to decrease only after Bitcoin price is down.



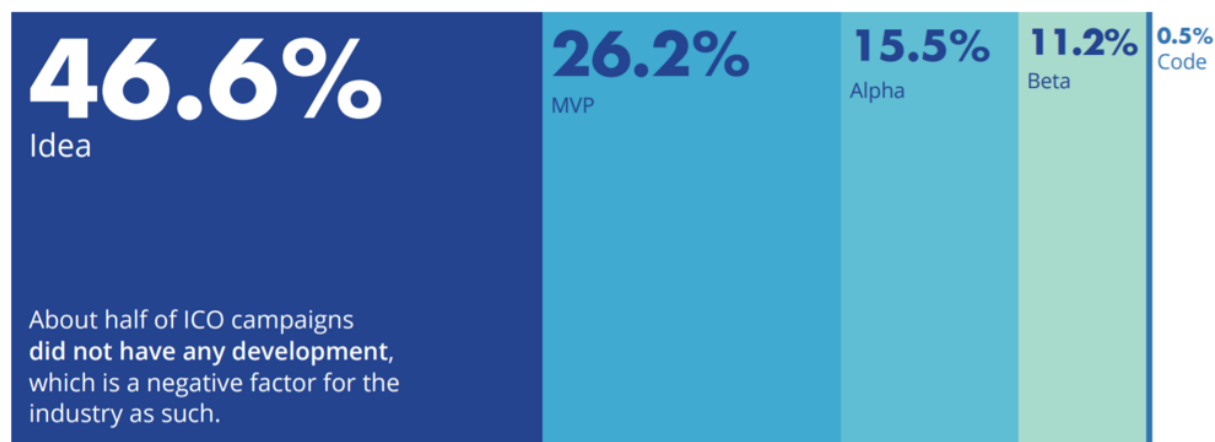
- 2018: looking at Q1 in 2018, 412 projects have occurred with nearly half of the total 2017 fundraising already reached, with the funding period widening up to 2 months from the 30 days of 2017, for sure due to the innumerable ICOs occurred with respect to last year and the impossibility for such a niche market to cover all the supply. Only 9% of the projects had an already running business. For what concerns the token type issued, almost two third are a stand-in for a product or service usage among the project.



143 Logarithmic graph personally created

144 <https://icorating.com/report/ico-market-research-q1-2018/>

For what concerns the development phase of projects, 46,6% of them didn't have any product development before the ICO, meaning that they were basically counting on the ICO to finance their own idea.

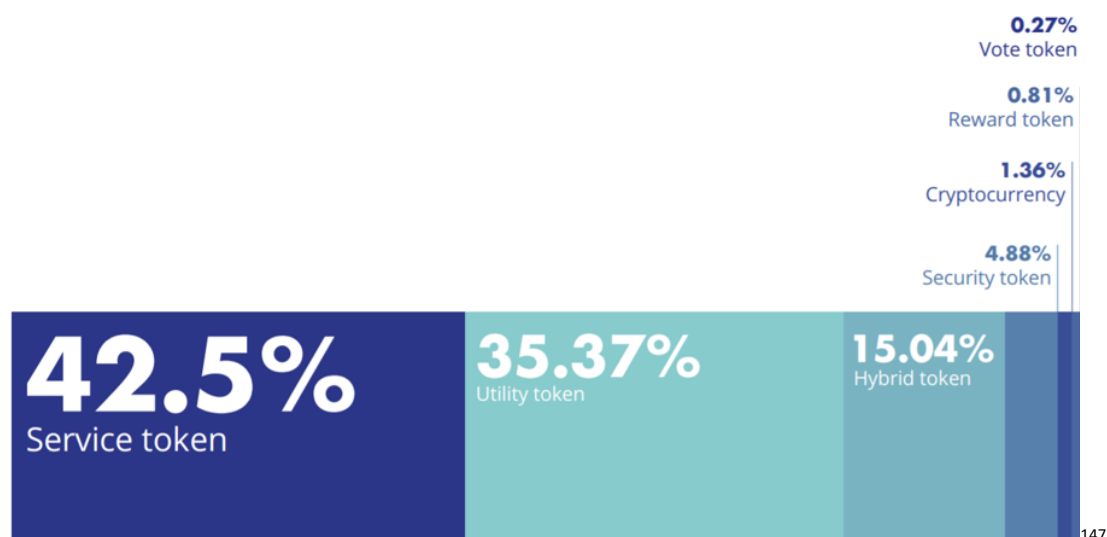


145

In Q2 of the year, the amount raised with ICOs more than doubled with respect to the previous quarter, with 8,4 billion funding, with EOS¹⁴⁶ project (the biggest ICO ever made) accounting for half of the amount. Although this could be seen as an ever growing market, there is one thing to be highlighted in order to assess the quality of this growth: the projects which didn't reached at least 100thousands euros accounted for 13% in Q1 and Q2 of 2017, now turning into a 50% share for the relative Q1 and Q2 of 2018. It's clear how this market's still dominated by last-minute entrepreneurs which try to profit on being the first comer by exploiting people FOMO (fear of missing out). In only one quarter, the share of tokens significantly changed, with service tokens still representing the majority of the tokens but with utility tokens becoming the second type of token. The amount of security tokens issued has significantly shrunk, with more attention to such an instrument by public regulators.

145 <https://icorating.com/report/ico-market-research-q1-2018/>

146 <https://eos.io/>



147

2.7 ICO brief history

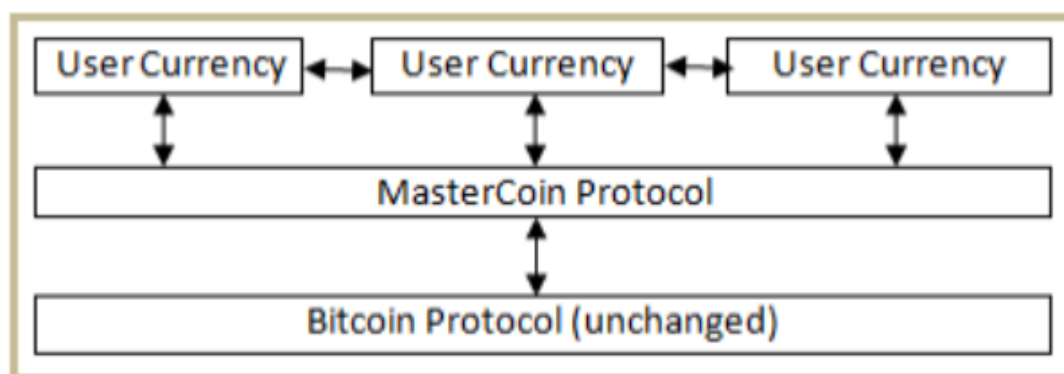
The first ICO ever made dates back to 2013, with the publication of what is renowned as “the second bitcoin whitepaper”, MasterCoin had its birth. Mastercoin describes itself as being the demonstration that Bitcoin Blockchain can be thought not only as a platform intended to run payments within the network but also as the main software layer on top of which new applications with other functionalities can be built and developed¹⁴⁸. The result of this whitepaper is the creation of a sort of new Bitcoin Blockchain with the add-ins conceived by the founder. The ICO reached nearly 500 thousands dollars worth of Bitcoin¹⁴⁹ (around 4700) in the fundraising event, with around 500 investors, and it soon became known as Omni Layer, with the word “layer” suggesting this conception of Bitcoin being a layer on a Blockchain over which other layers could be constructed. The author’s aim in giving birth to such a phenomenon was to find a way to finance the project. Willet was applying his dad’s suggestion about Bitcoin being as follows: “this is a kind of gold rush, and in those days people that really did well were not people out digging in the hills but those who were selling shovels for it”¹⁵⁰. Is clear how the aim has always been that of building an infrastructure that could permit Bitcoin to be more adaptable to people needs instead of creating an own version of this latter.

147 <https://icorating.com/report/icorating-annual-report-2017/>

148 <https://bravenewcoin.com/assets/Whitepapers/2ndBitcoinWhitepaper.pdf>

149 <https://www.weusecoins.com/what-is-mastercoin/>

150 <https://www.youtube.com/watch?v=hLWgaFwq6qM>



151

2.7.1 The Birth of Ethereum

It is the beginning of 2014, and Vitalik Buterin, a 19 years old guy, co-founder of Bitcoin Magazine¹⁵², entered in contact with J.R.Willet, MasterCoin founder. Willet had been already convinced by the other MasterCoin contributors to show Vitalik the content of MasterCoin whitepaper to see if he had suggestions about it or improvements to do. He suddenly came out with the idea of implementing a “Turing complete”¹⁵³ system. A Turing complete system can be said to be a system which is able to potentially calculate every type of computational problem without the need to re-shape the way the system works to adapt it case by case to the computational problem to be solved. Willet was very surprised by this type of proposal, but he was anyway focused on completing MasterCoin basic features implementation, and only after he would have evaluated the possibility to turn it into a Turing complete system. Why a Turing complete system matters? Bitcoin for example, is not Turing complete, meaning that if you would like to do a specific transaction other than the transfer of money between Bitcoin users, you simply can’t do it unless you succeed in changing and make the other agree about the change and run the new algorithm¹⁵⁴. Another characteristic of a Turing complete system is that it can replicate an algorithm with the use of a “loop” which replicates that same algorithm as long as the objective is reached, but with a limit, the uncertainty of the duration of that calculation. This “loop” feature is absent in Bitcoin, so that if you would like to replicate the same transaction you would have to copy and paste the same transaction code as much as you need. This leads to justify why Bitcoin developers didn’t choose to endow it with Turing complete system: hundreds, thousands of loops running on the same Blockchain could have overloaded this latter, turning it into a useless running machine with an output which is

151 <https://blog.omni.foundation/2013/11/29/a-brief-history-of-mastercoin/>

152 <https://bitcoinmagazine.com/authors/vitalik-buterin/>

153 https://en.wikipedia.org/wiki/Turing_completeness

154 https://www.youtube.com/watch?v=um9_sXhY014

uncertain in its computational time needed. With this idea of Turing complete software in mind, Vitalik Buterin soon became impatient of this novelty and he was looking forward for it to be introduced in the Blockchain world and gave a sort of ultimatum to Willet, to let him implement this feature in the MasterCoin protocol, or to leave it creating a new platform from scratch; this is basically how Ethereum Blockchain was founded in 2014¹⁵⁵. Roughly speaking, Ethereum is a Blockchain for the building of decentralized applications. The way the applications work obviously requires the system to handle different transactions both in terms of content and number of loops required for them to work properly. It is in this new need that relies Ethereum innovation, the possibility to run smart contracts¹⁵⁶ that can handle various need from different business models to be run by startups with no need to necessarily revise the platform for every new feature, but providing those startups with a ready-made standard on which to build its own vision.

Having clear in mind what Ethereum is, serves as a basis for understanding the ICO panorama, since 80% of ICOs create their own token on Ethereum, and the Ether is conceived as the money meant for execution.

Tokens creation in Ethereum follow standard protocols which ease the creation process and enables tokens interoperability, the most know standard is the ERC20, (ERC stands for “Ethereum request for comment”¹⁵⁷) which contains bugs that result in a permanent loss of tokens when a transfer is wrongly executed by the contract code. For this reason, new ERC standards have been created ¹⁵⁸ to solve the security problem or to function as a 2.0 version of the ERC20 token.

2.8.1.1 Smart contracts

The way tokens are governed and become able to run on the Blockchain is made through the use of smart contracts. Smart contracts simply state and regulate who possess what and what triggers the inflow or outflow of money from a contract to another, according to a predefined set of rules which obviously the parties involved have agreed upon. The figure below represents one example of smart contract.

155 <https://en.wikipedia.org/wiki/Solidity>

156 https://en.wikipedia.org/wiki/Smart_contract

157 <https://en.wikipedia.org/wiki/ERC-20>

158 <https://www.cointelligence.com/content/comparison-erc20-erc223-new-ethereum-erc777-token-standard/>

```

/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then communicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw; // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw; // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw; // Check allowance
    balanceOf[_from] -= _value; // Subtract from the sender
    balanceOf[_to] += _value; // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

```

159

The first time ever a smart contract is mentioned dates back to 1994, when Nick Szabo came out with the following definition: “A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries”¹⁶⁰. Smart contracts on Ethereum can be said to be a software program which is embedded in the Blockchain itself and can auto-execute transactions whenever an event is triggered. As Buterin itself says, smart contracts mustn’t be identified as being pre-defined digital papers to be filled in but to function as a program that can execute a potentially unlimited number of transaction. Smart contracts are projected on a “if-this-then-that” logic, which is to say that a contract is activated by a triggering event and the consequence of this triggering is the occurrence of one or more clauses specified in that latter. It is easier to understand what’s the innovation in here by making a comparison. Think about a normal transaction between two Ebay parties: the seller of an object and the buyer. The buyer wants to be sure that the seller will send the object once the payment is received and the seller wants to be ensured of the money to be in its account to send the object. What can happen in the state of the art is that both the seller and the buyer could potentially try to escape from their relative obligation, having the possibility that:

159 <https://blockgeeks.com/guides/smart-contracts/>

160 <http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>

- 1_ The seller receives money but doesn't send the object
- 2_ The buyer receives the object that the seller could eventually have sent before the payment is officially accounted, and then withdrew the transaction without paying.

Smart contracts can in a way eliminate every aspect related to an intermediary which should function as a guarantee for those 2 bad scenarios to don't happen. The two parties can set a sort of digital automated intermediary being the smart contract itself to function as a "box" which is initially endowed with the seller right to receive money and the obligation to send the object and the buyer right to receive the object and obligation to pay the amount of money required. This box being the smart contract could lock the money sent from the buyer up to the moment in which the seller notifies the sending of the object, so that the two parties can receive their right and owe their obligation without the need to wait for one party to start first. Another clear example is a crowdfunding campaign like those of Kickstarter: a team publishes a fundraising campaign which tries to collect X euros, if the campaign is successful and reaches then the funding goal, they will be allowed to retire the funds, otherwise the funds will be refund back to investors. But if in the state of the art there is a possible risk of those funds to be retained without any permission, smart contracts can ensure investors that their funds will be refund back only if a minimum amount (hard cap) is not reached.

2.7.2 The DAO: smart contracts and hacks

Nevertheless, smart contracts are not a perfect machine, they function with strings of code written to be interpreted by the computer, so that should those codes be wrongly written or having "holes" that could be exploited by hackers, they can suddenly become extremely fragile, and this is what happened in one of the biggest scandal ever in the Blockchain community, this is the case of The DAO organization. DAO stands for decentralized autonomous organization¹⁶¹. The aim of that organization was to basically substitute traditional management with a set of predefined rules that once agreed by the participator could auto-manage the organization. The whitepaper of the Dao describes this new conceptual way of governance as a way to solve several problems:

1. People do not always follow rules.

161 [https://en.wikipedia.org/wiki/The_DAO_\(organization\)](https://en.wikipedia.org/wiki/The_DAO_(organization))

2. People do not always agree what the rules actually require.
3. Minority stakes are not easily controlled directly from their contributors and can suffer from majorities decisions such as governance change or new ownership rules to exclude minorities.

All of these problems, the whitepaper says, can be solved by simply substituting writings with codes contained in a smart contract and let this automated process regulate all the stuff regarding the management of the company. The organization then works as follows:

- Investors send a minimum, set amount of Ether to be considered as an investor and to have voting rights to be exercised with the exchange of the Ether amount into DAO tokens. Voting rights are proportional to the amounts funded to the organization and allow to vote for or against projects within the organization.
- Anyone's allowed to move for a proposal and let the other vote. Should a proposal be implemented and then turn profitable, participators could retain a proportional part of that profit according to their contribution.
- Should a part of the investors be contrary to the majority's will, they can at any time retire their funds and start a new DAO.

This process tremendously resembles to a public offering made by a listing company, and in particular, it can be paired to a SPAC¹⁶²(special purpose acquisition company). In a SPAC, a company gets listed, and their contributors vote proportionally to fund one or more project, if the participators are not willing to participate in the project and be subjected to a majority, they can get their funds back. The DAO was created in May 2016, and this concept was able to raise 150 million dollars worth of Ether¹⁶³ in the ICO. The 17 June of the same year, after many developers already identified a hole in the coding of the organization, an hacker succeeded to implement what is known as a “recursive call”¹⁶⁴. What he did (simply explained) is as follows: the DAO code was written in a way that once a participator wanted to get its money back, a specific function from its own portfolio could be deployed to let the DAO code run a withdraw of those money. It all went fine

162 <https://www.investopedia.com/terms/s/spac.asp>

163 <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>

164 <https://www.youtube.com/watch?v=5JrdR6SRIWE>

until this hacker exploited the possibility (which the DAO team hadn't prevented) of a recursive call on the "withdraw" function. Indeed, any user can set its own portfolio coding script as it prefers, and this allowed the hacker to set its own in a way that he was basically establishing a loop in the withdraw function before the balance was updated to zero, which is to say that its balance was never updated to 0. The result is that the hacker was basically withdrawing money multiple times simply because the withdraw function in the DAO code was calling itself and by doing this was allowing the hacker's account to withdraw the same amount of money up to he basically wanted, since the only error he could not have committed is that of establishing a finite number of loops to don't block the system. All of this mess could be even prevented by a single line of code put in a different place in the coding block that wouldn't have allowed any hacker to withdraw a new amount of money before the balance was set to 0. One thing has to be explained first. What is happened with the DAO is a coding error, and not a weakness of Ethereum platform. The DAO created another important issue in the Blockchain community, which is that of immutability. What happened is that with this attack, hackers had succeeded to steal at least one third of the raised funds, and this brought the Ethereum developers to decide to go for a hard fork to restore the lost funds to the owners. This inevitably created an issue: those sustaining Blockchain characteristic of immutability blamed the developers to have altered this single version of the truth being the Blockchain itself, and as a response, they didn't accept to pass from the old version to the new one, causing a split in two; from one side the older Ethereum users which is now known as Ethereum Classic and from the other side the Ethereum new platform supporters.

2.7.3 Security offering

The most obvious classification among the ones mentioned above is that of tokens being considered a "cryptocurrency token", functioning then as a mean of exchange within the network. As said before, everything which is not only a mean of exchange in terms of payment functions and that can have many other functionalities within the network (to support the network in some way or to serve as a mean to buy future products) is said to be a "utility token". The residual category remaining, that of "security token" is the more controversial, since the categorization of a token in this category automatically leads to the uncertainty of its treatment and the still not very clear way through which something can be considered as security, with possible consequences of direct taxation on the capital gains. The SEC in US for example, applies the so called "Howey test" to assess the security-like characteristics of an ICO, and we can take this procedure as a general framework to assess the security characteristic of an instrument: The Howey test requires 4 elements to be satisfied

simultaneously for it to be defined as a security¹⁶⁵, more on that later. Being the DAO organization set as such, it was also eligible for being a security offering under the famous Howey test made in 1946, and consequently, the organization should have had all the mandatory steps required for such a financing mechanism, such as a prospectus and all the steps requested by public regulators. With a pronouncement made in 25th July 2017, the SEC recalled the characteristics of a financial instrument to be identified as a security, namely, a “tradable financial asset”¹⁶⁶.

The Howey test requires four evaluation steps to decide if a financial instrument could be considered an investment or not¹⁶⁷:

1. An investment of money
2. in a common enterprise
3. with a reasonable expectation of profits
4. to be derived from the entrepreneurial or managerial efforts of others

To better understand how this evaluation mechanism is conducted, is worth it remembering the sentence from which this test took the name, the Howey case¹⁶⁸. Howey was an agricultural company which basically was offering lands to people in a lease-back agreement and guaranteed that they would have been able to pay it with the company growing, harvesting and then made profitable through selling and sharing the profit generated with them.

Going through the assessment of the Howey case prongs, it is clear that the Howey case resembles:

1. An investment of money: furthermore, the definition has been enlarged conceptually by the SEC including also investments with means other than money.
2. In a common enterprise: this remains the most debatable prong, and is conceived as being a pool of investments made by different actors to identify a sort of “common destination” of the funds to be assessed whether they’re an asset or not.
3. with a reasonable expectation of profits: the company itself guaranteed that the payments due for the land would have been guaranteed by the company running activities on those lands
4. to be derived from the entrepreneurial or managerial efforts of others: It’s clear how the payment of the lands was uniquely connected to the efforts of the company running activities on the lands given in the lease-back agreement. To miss this prong for example, it would

165 <https://www.coinist.io/the-howey-test-the-sec-and-ico/>

166 [https://en.wikipedia.org/wiki/Security_\(finance\)](https://en.wikipedia.org/wiki/Security_(finance))

167 <https://www.sec.gov/litigation/investreport/34-81207.pdf>

168 <https://www.youtube.com/watch?v=ZkZuChRr5BU>

have been sufficient to state that the lands were in charge of the buyers so that “efforts” were in a certain way associable with themselves and not the company running lands.

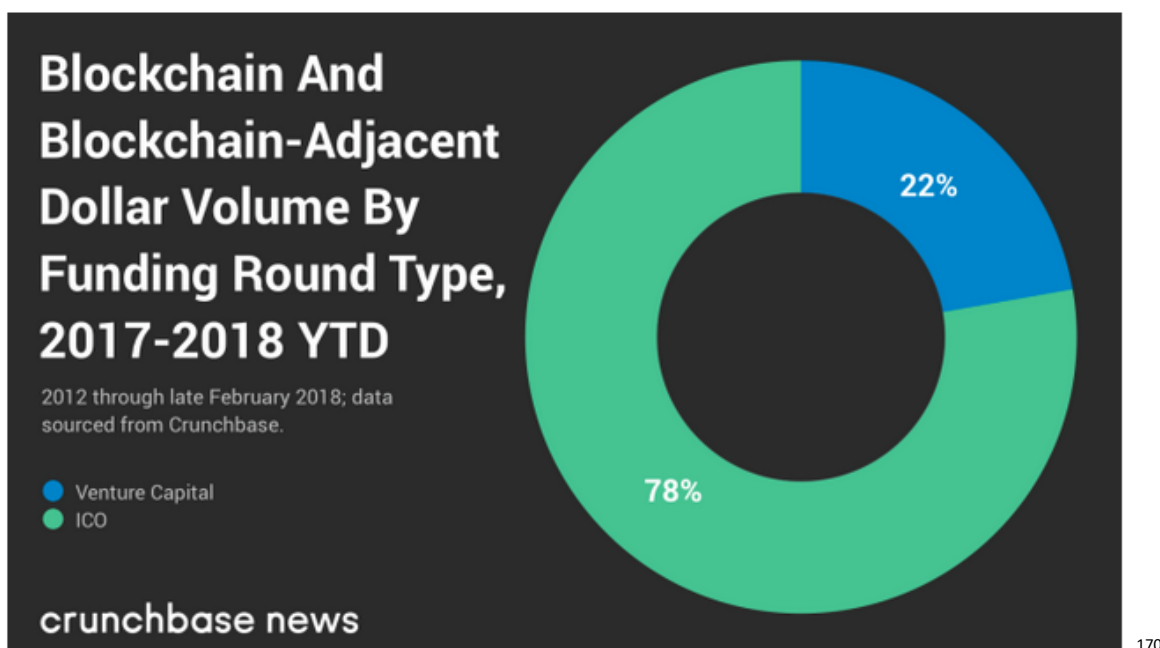
The DAO had the same treatment, and was considered an investment in this common enterprise called DAO with profits resembled to dividends in a listed company that would be generated by the company running the projects voted for this objective.

After that episode, it's clear how the companies coming after the DAO tried to escape the definition of their own token as being a security, declaring it to be a utility token or a cryptocurrency. Many other failed in defining a token which was really different from a security, thinking that a different definition of this instrument would lead the SEC to avoid its classification as being a security. The issue in here is that whenever an instrument resembles to an investment is considered as being such, no matter how it is declared to function by their creators.

2.8 Ico comparison with VC

It is interesting to start with a data: ICOs raised up 5,3 billion in 2017, being the amount more than five times (0,95 billion) that reached by VC financing by early-stage start-ups in Blockchain projects¹⁶⁹. A brief premise must be done: if a new financing tool emerges as an application of a new technology and new financing methods born using the “same language” of the technology the're financing, that means that there is for sure an incentive to use this new financing tool instead of traditional ones like Venture capital. One of the main advantages with ICO financing with respect to venture capital is liquidity. Here below, we can see how Blockchain funding has overtaken that made with VC funding .

169 <http://www.visualcapitalist.com/ico-crypto-venture-capital/>



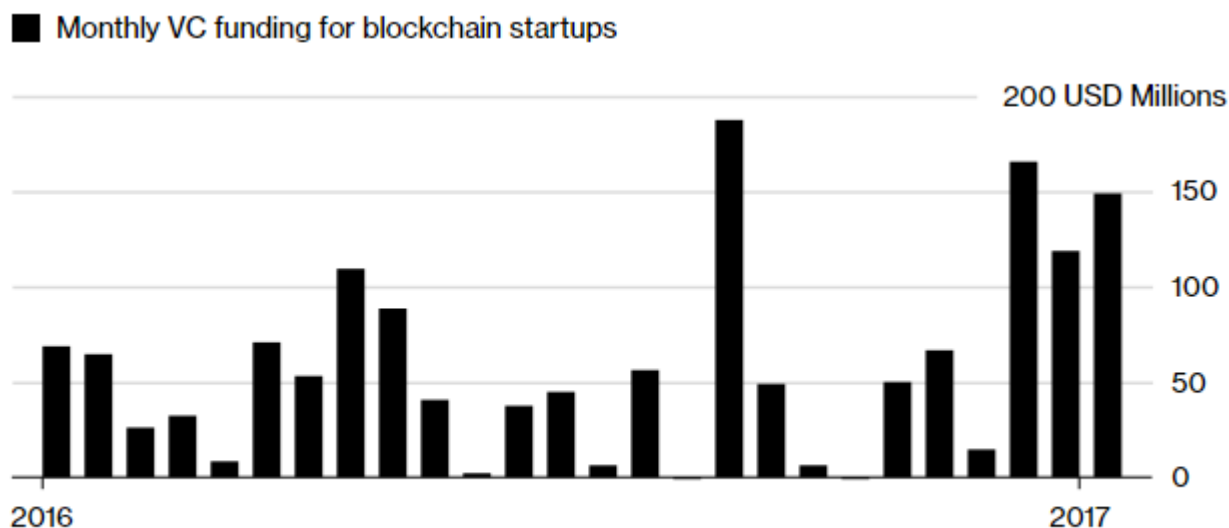
170

Considering all the documents analyzed for this purpose, it is clear that we can classify ICO companies as having done ICOs instead of VC funded their own business for the following reasons:

1. They didn't succeed to go for the VC option: ICOs have become the last chance for startups to finance their own business once they failed in doing so with traditional financing methods.
2. They have a Blockchain based business model which lets the project be more interesting for investors: it is obvious that there are businesses which really deserve to be analyzed more in deep because they've been planned to function within the Blockchain environment and solve a real world problem.
3. They want to use it as a long term strategy to still reserve the option for IPO: The reasoning is simple, why should they struggle to IPO, spending much more money and running the risk of investors being skeptical about the long-term perspectives? ICOs are actually the best short-term financing mean which allows companies to become known for future IPOs objectives while still collecting even more funds than with other types of instruments.

A clear trend is that one in which we see VC firms passing from funding startups directly to invest in their own token offering, meaning that ICO are seen as a double faced instrument, a direct competitor for VC firms whilst a risky booster for their annual ROI.

170 <https://techcrunch.com/2018/03/04/icos-delivered-at-least-3-5x-more-capital-to-Blockchain-startups-than-vc-since-2017/?guccounter=1>



Source: CoinDesk

2.9 ICO comparison with IPO

Coming to IPO comparison, which I think is the most interesting one we can do with ICOs, there are many reasons for which ICOs reveal to be an excellent financing mean. There are anyway few conceptual differences that need to be mentioned:

- ICOs are an entry strategy, while IPOs are one possible way to exit from a corporate and cashing out an investment¹⁷¹.
- Unless there is a declared willingness for the ICO to be considered as being a security offering, tokens offered are not diluting the ownership of founders, whilst this is what happens with IPOs.

2.9.1 Advantages and disadvantages of the two financing means

ICOs provide liquidity to early stage companies with even no running products or existing business models¹⁷², and they're even backed by a secondary market in which investors are provided with a tradable token they can exchange or even use as a means of payment for the service the company's actually providing or still trying to provide.

Anyway, the existing secondary market is not easily liquid in the sense that is all subordinated to the token being a good mean to be traded among investors, and the flood of money coming to early stage start-up could create a huge misalignment in terms of incentives given to entrepreneurs to

¹⁷¹ <https://www.feedough.com/initial-coin-offering-ico-vs-initial-public-offering-ipo/>

¹⁷² <https://outlierventures.io/research/cutting-through-the-ico-hype/>

really bring their own idea into life. Liquidity is one of the main potential given by ICOs, they can even fund projects which to the eye of investors could even not possess any characteristic of sustainable business model and therefore have any value. Thus, if one wants liquidity for ICO to become an incredible advantage instead of a limit, a regulation in the sense of limiting the developers with the possibility to cash in the token after the ICO's finished is needed, for example providing them with a clause that allows them to retire funds only with a given % and after the token holders being a sort of digital shareholder agreeing on the issue. This solution is already provided by the idea of DAICO. DAICO is the name provided to a sort of perfect mix between the DAO concept and ICO¹⁷³ and the idea was first presented by Vitalik Buterin (Ethereum founder). It basically consists in "additional coding lines" to smart contracts in a traditional ICO that can limit the company owners in the amount they can withdraw from the funding one, and be subjected to what is called a "tap clause" that allows them only to reduce the maximum amount unilaterally, but not to raise it without the consensus of the token holders. Put in this way, DAICO appears to be even worse from entrepreneurs' point of view in terms of freedom to operate with respect to the idea of having shares in a listed company, with investors being not only the ones responsible of shaping the price of the token by making exchanges, but they're in a way put in a position which they can exploit to guide the company's business and finance it accordingly, with entrepreneurs needing to establish a good balance of trust with them to conduct the business almost alone. Of course, this is a suggestable path to be done by the ICO world if one wants it to be sustainable in the long period, but there must be incentive for it to be implemented. There are many advantages in conducting an ICO instead of relying on traditional financing means like IPO. Here below and in the table, I summarized the main elements of distinction between the two:

1. ICO can compensate initial developers without giving them more control of the network than any other token holder.
2. ICO provides the issuer with an early signal about consumer demand

173http://www.ecgi.global/sites/default/files/working_papers/documents/finalhowellniessneryermack.pdf <https://ethresear.ch/t/explanation-of-daicos/465>

3. ICOs provide a great amount of potential liquidity, which occurs when a cryptocurrency exchange permits trading in the new token. In many cases, the token is tradable for cryptocurrency or fiat currency within a few days of the ICO. However, there are two caveats:

- Some ICOs offer or require lock-up periods, during which ICO participants may not sell their tokens.
- Liquidity is not guaranteed. Many ICO tokens are never exchange-traded, and even if the token is listed, a holder may not be able to find a counterparty. Related to liquidity is the ability to take advantage of temporary overvaluation, a phenomenon that also exists in IPO markets¹⁷⁴. Here below a resume of the main differences between the two financing methods:

Main characteristics of ICOs and IPOs

Criteria	Initial Coin Offerings (ICO)	Initial Public Offerings (IPO)
Motivation	Funding by issuance of tokens	Funding and exit motivations by shares
Regulation	Uncertainty about regulatory environment	Highly regulated area
Status with global regulators	Allowance, ban, warnings and alerts	Global convergence of established standards
Issuer status	Idea, prototype and early stage business	Proven business models, small to large caps
Investors	Crowd investors in the internet	Retail and institutional investors
Offering document	Primarily white paper	Approved security prospectus
Placement type	Direct placement and usage of ICO platforms	Intermediated by investment banks
Technology	Block chain based technology	Custody, clearing and settlement systems
Security offerings	Most ICOs prevent tokens to be a security	Different share types representing ownership
Utility offerings	Most ICOs issuing utility tokens	Not applicable
Payment	Cryptocurrencies (e.g. Bitcoin, Ether, Ripple)	Fiat currencies (i.e. USD, €, HKD)
Trading	Volatile trading on ICO platform yet	Active trading on established exchanges
Price and liquidity	High volatility of token prices	High liquidity and relative stability of prices
Parties involved	Issuer, promoter and platforms	Issuer, lawyers, auditor and investment bank

175

2.9.2 Differences with IPOs

¹⁷⁴ <http://www.csef.it/pagano/jf-1998.pdf>

¹⁷⁵ [https://www.ey.com/Publication/vwLUAssets/ey-ipo-and-ico-markets-at-a-glance/\\$FILE/ey-ipo-and-ico-markets-at-a-glance.pdf](https://www.ey.com/Publication/vwLUAssets/ey-ipo-and-ico-markets-at-a-glance/$FILE/ey-ipo-and-ico-markets-at-a-glance.pdf)

ICOs have profound differences with respect to ICO. According to an omni-comprehensive study accounting for 4003 ICOs, done by Hugo Benedetti and Leonard Kostovetsky¹⁷⁶, we can find two main differences between ICOs and IPOs:

- **Returns:** The first day's average abnormal returns range from 14% to 16%, 30-day average abnormal returns range from 41% to 67%, and 180-day average abnormal returns range from 150% to 430%. If we compare this data to the table below reporting IPO average first day return we see that the very first day return of ICOs is very similar to that obtained by IPOs during decades, but the trend increasingly differs as time passes, with ICOs stunning price increase during the following 6 months, while IPOs suffering a down-pricing or a stable return at best¹⁷⁷.

Key US IPO statistics	2017
Average total return	20.7%
Average first-day return	11.7%
Average aftermarket return (from IPO to end of year)	-7.4%
% trading above issue at year end	58.9%
% deals with negative first-day return	24.1%
% deals priced below the range	25.9%

- **Underpricing:** The degree of underpricing is much larger than that for IPOs but is not surprising considering the entrepreneur's lack of expertise in determining market demand for the token/platform, greater uncertainty about the value of a startup company whose platform is typically still in the idea stage, and the urgency in distributing tokens to allow the platform to function. On the other hand, the age of the firm (based on its Twitter account activation date), a proxy for information asymmetry, is not related to ICO underpricing, a significant difference between ICOs and IPOs. Interestingly, in contrast with IPOs, there is no indication that more established companies, with a longer track record as proxied by the length of time since their Twitter account was activated, suffer from less pricing. Unlike ICO underpricing, the results for long-run performance (at least in the first year) run completely

¹⁷⁶ <https://poseidon01.ssrn.com/delivery.php?ID=884112031001096099084019119023008024001024032007049053005121114102085112088114081121124025056115114005124127026111096098104111023039056023040029119004100001004072040073010075091088009002106116126112020000118068117072012014022021018103097118074119065&EXT=pdf>

¹⁷⁷ <https://www.fidelity.com/viewpoints/active-investor/IPO-opportunities>

counter to what prior research has shown for initial public offerings. This could be due to the lack of a lockup period for most ICOs, which would cause the opening price to already reflect the supply from insider sellers, while for IPOs, the supply would be released after the lockup leading to lower returns. Another explanation is that ICOs are much younger and riskier and thus need to provide a high expected rate of return to create investor demand.

2.9.3 Reverse ICOs

We speak of reverse ICO¹⁷⁸ when we face the situation of a company with an already existing business and working products or services going to execute an ICO. The word “reverse” is taken from the reverse IPO method,¹⁷⁹ which is the situation in which a private company acquires a listed one, thus avoiding all the listing process. By the way, the term “reverse” used in IPO stands for the process of a private company becoming a public one, while the ICO use of the term is conceived to highlight the fact that a traditional process like that of ICO, used basically for startups, is used by well-known companies to avoid IPO process and raise funds more flexibly.

A main difference with respect to traditional ICOs is that while those latter are conceived as a way to escape the security classification by regulatory institutions, reverse ICOs are by default conceived for the use as equity. Put in other terms, we’re facing a security-like instrument which could be even used as a mean of payment for the products/services provided by the company. Furthermore, the fact that the reverse ICO is done by companies with existing business model, allows for the collection of a group of information about “real numbers” that provides investors with a better understanding of the project being financed and let the ICO be more liquid.

These are the main differences found for IPO comparing to reverse ICO:

178 <https://steemit.com/bitcoin/@g-dubs/what-is-a-reverse-ico>

179 https://en.wikipedia.org/wiki/Reverse_takeover

IPO	Reverse ICO
Public capital market	Public capital market
Issues equity	Issues equity
Stock Certificates	Tokens
Rights, dividends, voting, etc.	Rights, dividends, voting, etc.
Little or no innovation	Huge innovation. Tokens can contain logic and become part of technological infrastructure. Breakthroughs in business models.
Full IPO, Reg. A+, Reg. D	Full IPO, Reg. A+, Reg. D, <u>Reg CF</u>
Stock is priced and issued via banks and stock markets	Tokens are priced and issued on web site, directly to purchasers
Only for the biggest companies	Good for any size company
Medium valuation	High valuation
Purchased by stock investors	Purchased by crypto investors
Moderately liquid	Highly liquid
Not for small to mid-size tech firms	Easy for small to mid-size tech firms

180

2.10. Debate in the valuation framework: a far to complete process

The valuation framework for such a category is still in its infancy, with many methods used to try to at least guess what the rationales behind such token are, but the quality encountered of course does not permit to be precise. There are anyway many interesting point to discuss, and from which to depart by analyzing them. The problem the market is facing is that of company's infancy, which is to rarely have cashflow producing businesses, and thus we can only rely on proxies for the discovery of value. During those few years from the birth of the crypto-space, many authors tried to identify a reliable measure for detecting price movements and give a certain value to a particular token/cryptocurrency. The following methods are the ones I retain far more reliable in terms of conceptual framework, even if the variables in place are so different that is difficult to implement them.

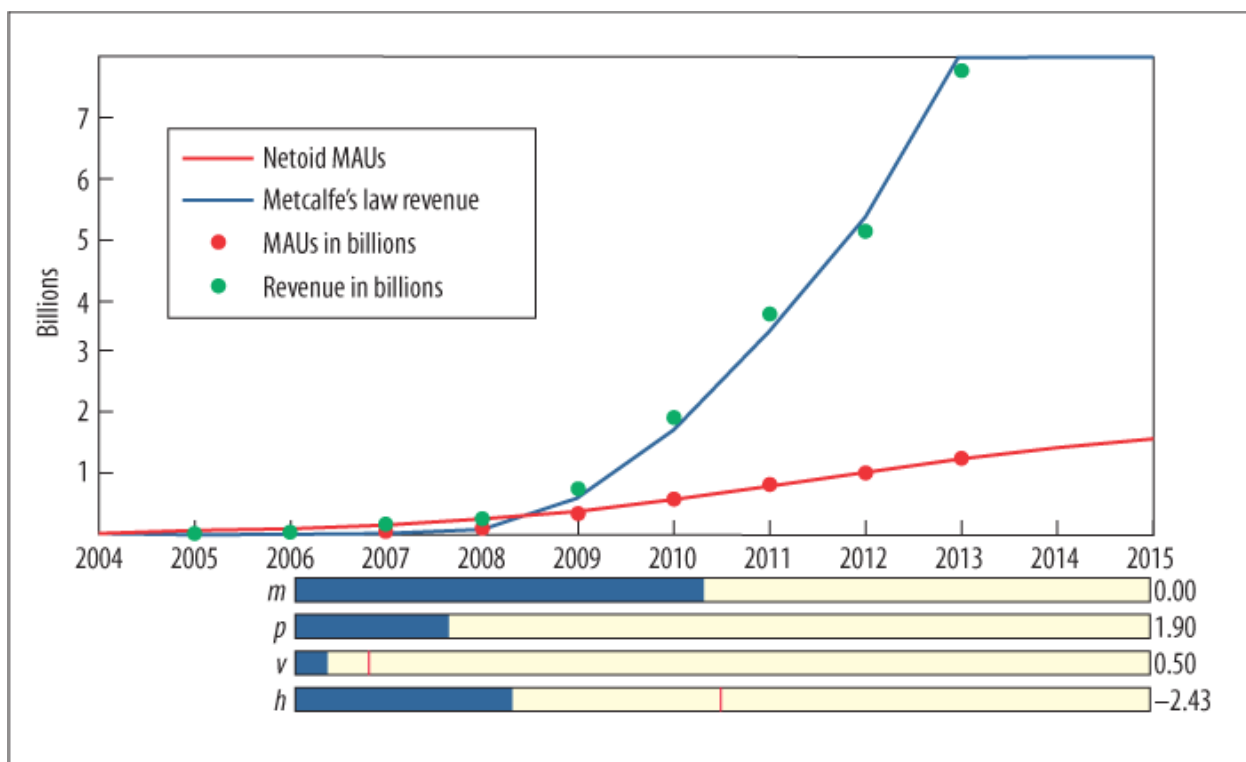
2.10.1 Metcalfe's law

In the early 80's, Robert Metcalfe, the creator of Ethernet, came out with a law describing that the value of a network should be proportional to the square of number of users within that network¹⁸¹. To figure out how this law works, we can make a simple example. First, the users network value can be represented as such: $n*(n-1)$. This formula tells us that if we have a market, and let's say that is about fax machines, the value of the fax machines market is proportional to the number of nodes we can create with those fax machines. Just to give a simple example, if the market has only a fax machine, its value is $1*(1-1)=0$, but if we only raise the number of fax machines to two we have

180 <https://venturebeat.com/2017/09/29/reverse-icos-may-be-your-best-vc-portfolio-exit/>

181 https://en.wikipedia.org/wiki/Metcalfe%27s_law

$2*(2-1)= 2$, and the value goes up to 6 with only 3 machines. The concept is that we can't create a network with only one fax machine, but if we only have two, we can create two connections, one from machine A to B, and viceversa. Roughly speaking, one could approximate this law by stating that the value of a network is proportional to the square of the number of users within the network. Up to 2013, no one ever tried to use Metcalfe's law to demonstrate a fit in the real world, when suddenly Metcalfe itself used Facebook data to demonstrate that the law has a good application in the real world too. He basically described the value of a network to be identified by the so called "netoid function"¹⁸² and used Facebook's revenues as a proxy for value and obtained a strong fit like you can see in the figure below:



183

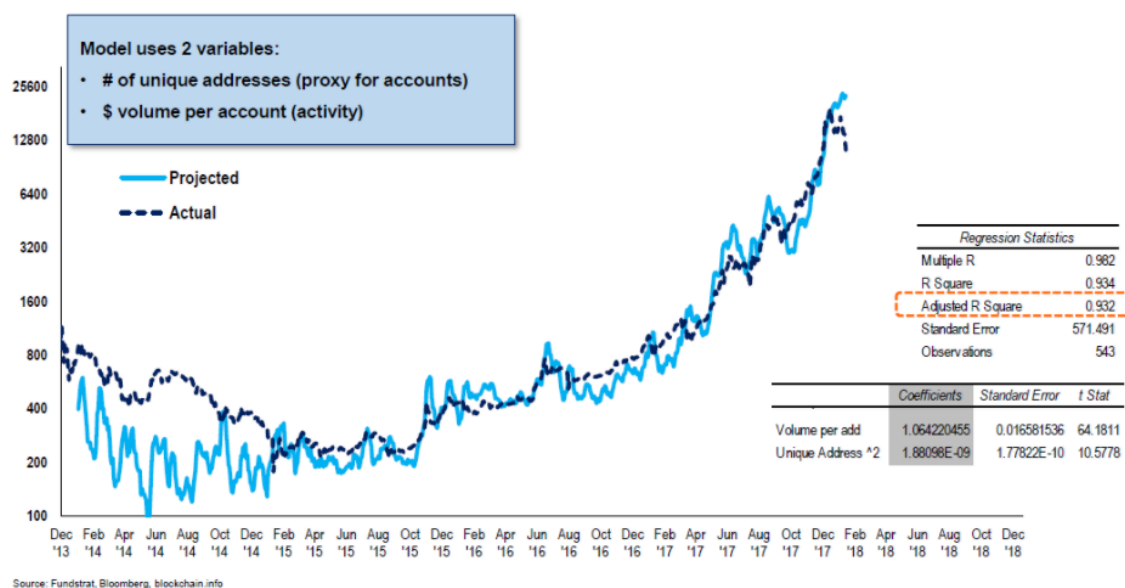
Tom Lee from Fundstrat demonstrated that Bitcoin price itself can be explained quite accurately with a 93% fit with Metcalfe's law, and predicted Bitcoin price to reach at least 6 thousands \$ within 2018¹⁸⁴. Here below the statistics about the model application:

182 https://ipfs.io/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Netoid_function.html#cite_note-1

183 https://www.google.it/search?biw=1366&bih=582&tbm=isch&sa=1&ei=XyGeW6WxM8fUsAfn8J_YDg&q=netoid+curve+facebook&oq=netoid+curve+facebook&gs_l=img.3...1833.2617.0.2694.6.6.0.0.0.100.403.5j1.6.0...0..1c.1.64.img..1.0.0...0.yzVesymIdQU#imgrc=M1uQua7ni6-HqM:

184 <https://cointelegraph.com/news/wall-street-s-tom-lee-says-bitcoin-price-to-hit-22k-by-year-s-end-can-reach-25k>

Figure: Comparative Price of Bitcoin against a "Model-based Bitcoin" using volume and unique addresses Since 2013



185

Another proof for Metcalfe's law to hold is given by the same application done by Xing-Zhou Zhang, Jing-Jie Liu and, Zhi-Wei Xu. They did the same test of Metcalfe by applying the law to Facebook and Tencent's data, obtaining a strong fit also in this case¹⁸⁶.

My opinion about the law is that I retain for sure interesting that a function could describe the value of a network so accurately, but there are some still questions for which to find an answer:

1. A network of n users doesn't necessary need to connect all of the $n-1$ users everytime. Think about a Facebook account, this account could have for example 1000 friends, and this could mean $1000 \cdot (1000-1)$ connections, but this is the only real value it actually has, while the total number of connection a single account could have is only potential. Thus, I like to see this law as being the maximum value a network can have in the long-term, but not it to describe short term trends
2. One could argue: "Why you don't rely on a law which obtained strong fits both with Bitcoin and Facebook/Tencent's data?" My answer is that confirming that the value at which an instrument being Bitcoin or Facebook actually trades is not necessary the value it actually has, and it tells nearly nothing about its over/undervaluation. The reasoning is that since we can't demonstrate Bitcoin or Facebook are actually quoting fair prices, a law fitting with actual numbers is simply a good outcome to be taken in consideration, but if we assume for

185 <https://steemit.com/cryptocurrency/@swinn/common-bitcoin-metcalfe-models-explained>

186 <https://link.springer.com/content/pdf/10.1007%2Fs11390-015-1518-1.pdf>

a while that Bitcoin is a bubble, finding a good law describing it is only helpful to confirm a bubble, not to identify real value. Put in other terms, I think that law is way too optimistic.

2.10.2. Quantitative theory of money applied to crypto

For those tokens which function as a mean of exchange, it becomes of some kind of utility assessing the value of them as a currency, thus the quantitative theory of money could be applied. Briefly speaking, this theory states that the overall value connected to a currency is given by the monetary base in circulation multiplied by the velocity at which currencies pass from hand to hand. To resume, the equation states that $MV=PQ$, which is to say that the amount of money M exchanged at a velocity V equals the price of the resource bought multiplied for its quantity. Chris Burniske did an interesting job by adapting the model to an hypothetical token called INET¹⁸⁷. This token is the representation of a bandwidth provider service, and the work starts by defining a Total addressable market (TAM) for this token. Once the TAM is defined, projections about this service adoption are made to quantify the PQ side of the equation, which in this case can be said to be the internal GDP generated by the service in providing bandwidth. Once one side of the equation is calculated, only the velocity (V) at which the token representing the service is exchanged could lead us to obtain M , which is the value the token should have embedded to serve the market forecasted. Once having defined M , we only need to divide by the number of tokens in circulation to obtain the price per token. Of course, this model too could only be thought as being a proxy to establish stable patterns among an unknown market, the author itself declares it not to be a model to be used for evaluating when to buy tokens.

2.10.3 Network value to transaction ratio

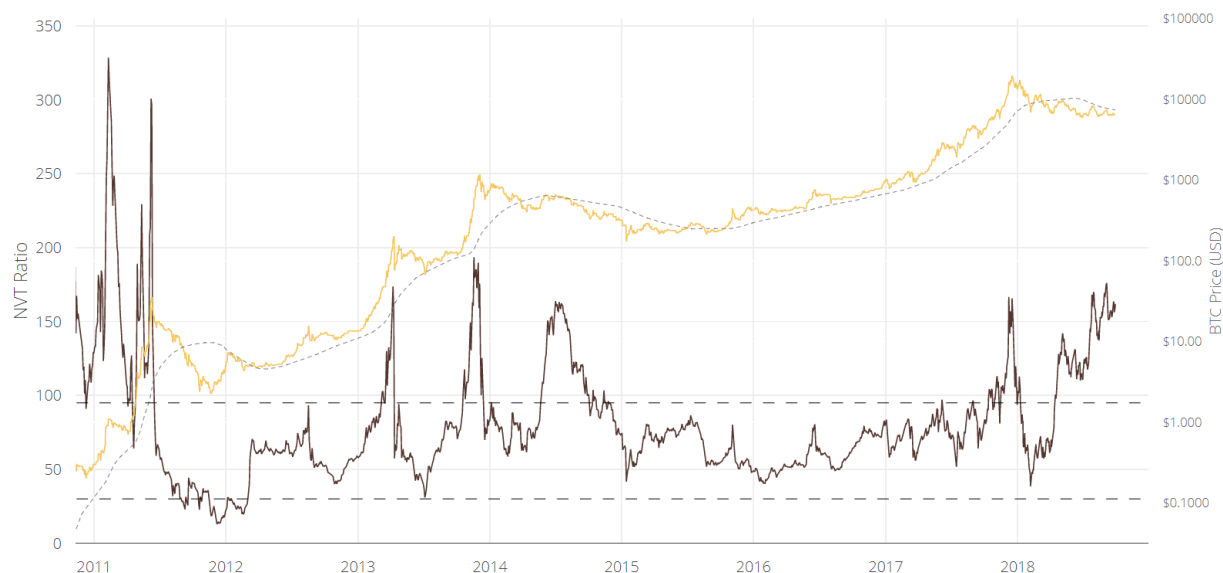
Being the crypto market so different in terms of instruments actually in place, it is also difficult to rely on traditional measures to find a relative valuation model. This is why many authors tried to find and adapt old traditional methods to fit with the totally new world of cryptocurrencies. This is basically how the Network value to transaction ratio (NVT) born¹⁸⁸. The ratio is calculated as such:

$$NVT = \frac{M}{T}$$

187 <https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7>

188 <https://woobull.com/introducing-nvt-ratio-bitcoins-pe-ratio-use-it-to-detect-bubbles/>

M is the market capitalization of the token being analyzed, while T is the value of the daily transactions occurred within that network of token holders. NVT can be paired to what P/E is for traditional companies, whilst taking in consideration that tokens don't produce earnings, but using the value coming to that network of users as a proxy for company earnings¹⁸⁹. When this ratio is high, that means that the market cap is unjustified relative to transactions, while if it is too low, that means that the amount of daily transactions occurring within the network is somewhat unreflected in the token price and suggests an under-valuation. Adding to the NVT, the creators of that ratio, noticed that this punctual measure was in a certain way discovering over/undervaluation only after the price went up or down for a token, thus they tried to smooth it by using moving averages from 14 days to 90 days ones. Here below an example of how the author of the NVT ratio tried to predict Bitcoin overvaluation: in orange is traced Bitcoin price, while the darker line shows the NVT ratio smoothed with a 14 days moving average. The chart clearly shows that the ratio can at least suggest when it's time for the price of a cryptocurrency to fall or to be stable in price according to the "inflation" given by the network. Few thoughts, if we make the paradox of taking into account a network which has a market value of few euros and we assume there are no daily transactions because nobody's interested in the network, the value goes up to infinite! But this outcome seems reasonable as long as we know that we have to treat this possible outcome as reasonable to demonstrate that in this case infinite equals zero.



190

189 <https://blog.coinfabrik.com/a-review-on-cryptoasset-valuation-frameworks/#what-is-fundamental-analysis>

190 <http://charts.woobull.com/bitcoin-nvt-signal/>

2.11 What factors determine the success/failure of a campaign?

An interesting study confirms what can even rationally determined in the ICO panorama ¹⁹¹. The factors determining the success of an ICO can be summarized as follows:

- **Number of tokens sold:** Intuitively, being the market founded on greed and people searching for the next Amazon in the Blockchain world, it's clear how the number of tokens issued matters, and is even reasonable to see this result: the more the tokens issued, the more the campaign can become successful. There are a few reason for this to happen. First of all, if the average investor is focused on the price of the token to rise, that means that the more token he can buy with a single amount X, the more is interested in buying as much as possible with the hope of having “rubbish to become gold” one day. Then, given an amount X, the average investor, rationally, will put it in the “growing lab” in which there is much more to grow. Second, since the entrepreneur managing the ICO is basically allowed to choose whatever he think is a good token supply, he is basically allowed to “create value from thin air” up to the moment in which there are enough people buying the product. This point is confirmed also by the fact found above that the more an ICO is high in terms of price per token, the lower is the price at which this token is actually trading with respect to ICO event.
- **ICO duration:** The more the ICO is marketed around the crypto enthusiasts, the more is probable that the FOMO (fear of missing out) will lead them to run and buy a share of interest in a candidate for success. Like a normal IPO process, but even more in general, creating scarcity leads to more attention with respect to allowing anyone to participate.
- **Correlation with the main cryptocurrencies:** of course, being the market still small in terms of market capitalization, currencies are highly correlated with themselves, and the rise or the fall of Bitcoin basically sets the path for the rest of the market for the days to come.
- **Presence of a whitepaper:** the most amazing thing encountered in the study is the fact that having a whitepaper is not a bad thing but neither a good one, to be clear, people don't read what is written on the whitepaper.

¹⁹¹https://www.researchgate.net/publication/323958952_Initial_coin_offerings_ICOs_to_finance_new_ventures_An_exploratory_study

- **Presence on GitHub:** Most of the ICOs (nearly 80% of the sample analyzed) have a GitHub account. This is the most famous site on which to “host” the token code to be shared and improved by developers and become desirable by future investors.

Chapter 3 Fundamental value for ICOs

3.1 Framework

The attempt here is to analyze ways of detecting fundamental value for ICOs, if any. Since basically we’re dealing with start-ups, we don’t have cash flows information because of lack of viable products and thus the possibility to discount those latter with a proper rate. What I thought is that the only way to establish a point of contact between traditional valuation models and token valuation models is to find a correlation between the price of a traditional instrument and that one of the token being analyzed. A possible solution to that issue came discovering (at the end of 2017) that there were a bunch of listed companies which already done an ICO or at least were announcing one. I then imagined that if it was (and it is yet) impossible to define a proper valuation method which could depart from traditional ones, I could instead try to establish a connection path between the price of the stocks of those few companies and the token that has been issued during their own ICO.

3.1.1 ICO use case presentation: Overstock’s subsidiary tZERO

Coming to a practical use case, the best way to compare traditional financing methods to new ones like that of Initial coin offering is to find the most similar method which resembles the most the traditional one to which it can be compared, that is the case of Overstock doing an ICO for its subsidiary tZERO. As the start-up site reports, “tZERO’s Blockchain technologies aim to revolutionize the market and fix the inherent inefficiencies of Wall Street so that financial processes are less beholden to traditional, institutional market structures”¹⁹². tZERO, as the name suggests, is

¹⁹² <https://www.tZERO.com/>

the name referring to the main goal of the company, which is to function as a disruptor for financial markets. The president of the company, Joe Cammarata, says “Wall Street likes inefficiency, they like making millions on the current 3-day settlement.”¹⁹³ Starting from this idea of the third day settlement actually in place, Overstock’s CEO Patrick Byrne came out with the idea of using Blockchain technology to reduce this “time 3” (t3) to time zero (T0), which is exactly why the company has this name. The outcome of this reasoning is that financial markets could be disrupted by putting an accent on liquidity, democratizing the way with which they function and distribute wealth.

3.2 tZERO company overview

As the Sec document clearly reports¹⁹⁴, tZERO is “a financial technology company focused on the development and commercialization of financial applications of cryptographically-secured, decentralized ledgers—often referred to as distributed ledger or Blockchain technologies”¹⁹⁵. The company was initially a wholly owned subsidiary (from the end of 2014) by another Overstock subsidiary named “Medici Inc”. Medici aim from the beginning was that of providing an “advanced Blockchain technology to broaden access to capital, financial markets and other applications”¹⁹⁶. Due to the purchase agreement conditions, Medici stake was reduced by transferring a 24.9% stake to third parties the year after, on July 16. On October 21 2016, Medici name was finally changed in tZERO. Here below the company structure as of today:

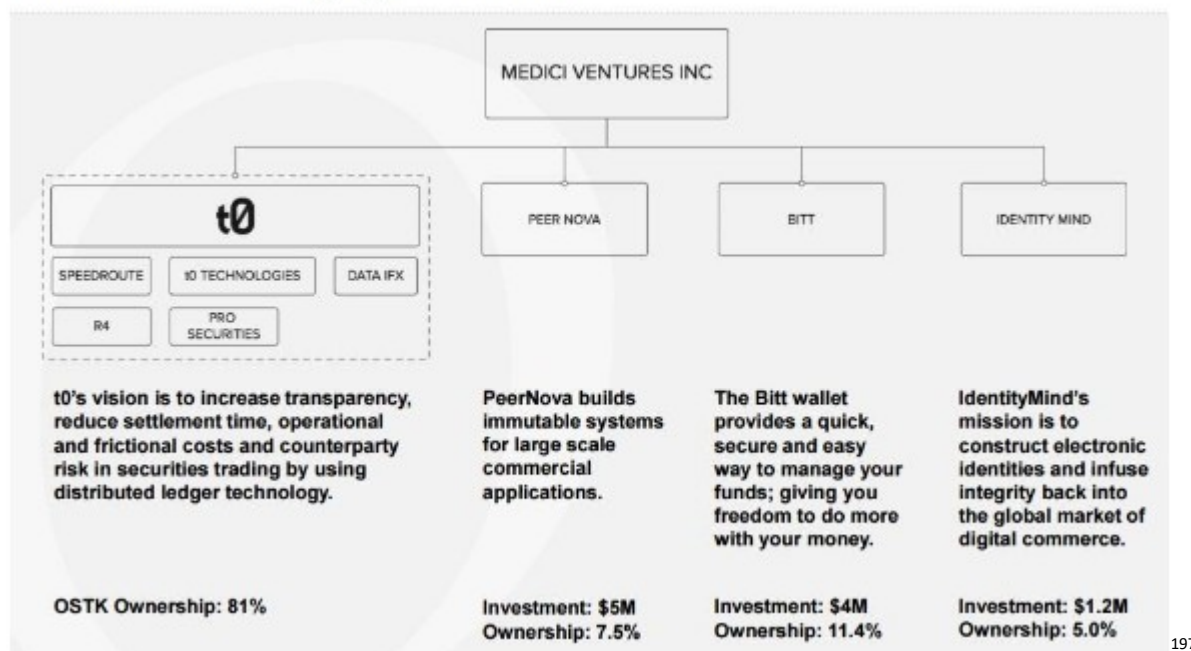
193 <http://www.johnlothiannews.com/2017/07/round-one-overstock-com-tZERO-aim-knock-wall-street/>

194 https://www.sec.gov/Archives/edgar/data/1130713/000110465918013731/a18-7242_1ex99d1.htm

195 Ibid.

196 http://www.annualreports.com/HostedData/AnnualReports/PDF/NASDAQ_OSTK_2017.pdf

Medici - Emerging Structure



3.3 ICO structure

According to the Sec filing by Overstock, tZERO ICO consists in a so called SAFT agreement, a parallel to the more traditional SAFE agreement, which stands for Simple agreement for future equity¹⁹⁸. A SAFE is a contract that entitles the buyer to receive a given percentage of shares, with this event triggered by a specific occurrence. A SAFE is very similar to a convertible note, but the fact that it doesn't have a defined maturity and is no-interest bearing makes it an equity instrument. Coming to the comparison, A SAFE and a SAFT are basically the same instrument, a security giving contract holders the possibility to receive/acquire a stake in an instrument once one or more conditions are satisfied, what changes for SAFT is that the object of the agreement is no more a direct stake in the equity like SAFEs, but a token¹⁹⁹; thus we're dealing with what is called a Simple agreement for future tokens. The company counted to place tZERO ERC-20 compliant tokens, to reach a maximum amount of 250 million \$, and considered the possibility to raise additional 50 million \$ by exercising a green shoe option, totaling an offering of 300 million \$. Tokens sold in the agreement are classified as "restricted securities". The price range of the token was structured as follows:

197 Overstock.com

198 [https://en.wikipedia.org/wiki/Simple_agreement_for_future_equity_\(SAFE\)](https://en.wikipedia.org/wiki/Simple_agreement_for_future_equity_(SAFE))

199 <https://medium.com/@bekhzod/safe-as-saft-understanding-simple-agreements-for-future-tokens-3e7af6498878>

- Up to 9,999,999 \$ funding: 5 \$ per token, with maximum investment fixed at 250,000 \$
- From 9,999,999 to 49,999,999 funding: 6,67 \$ per token, with minimum investment fixed at 50,000 \$ but no cap on maximum amount.
- From 49,999,999 \$ to 99,999,999 \$ funding: 8 \$ per token, without any limit on amount
- Over 99,999,999 \$ funding: 10 \$ per token, with the company's sole discretion of discounting the price, and a minimum amount of 2,000 \$, with no cap on maximum amount.

The first two tranches were conceived for institutional and strategic investors, while the fork ranging between 8 and 10 is conceived for non-strategic ones.

Regarding the amount of tokens issued, the company was aiming to issue no more than 59 million tokens and the only right to which token holders could be entitled was that of receiving a dividend which is calculated as the 10% of the company's consolidated adjusted gross revenues, whilst not containing any voting rights. Each dividend could be paid in U.S Dollars, Ether, Bitcoin or additional tokens, configuring this dividend as being a PIK²⁰⁰ one, confirming the trend for ICOs to give stakes in high risk instruments. The company has the right to redeem tokens in a proportional way or other equitable methods, paying no less than the maximum ICO price, which is indeed 10 \$. The tZERO platform main highlights are as follows:

²⁰⁰ <http://docenti.luiss.it/bruno/structured-finance/teaching-material/materiali-didattici-protetti/>

ECONOMIC OVERVIEW	
Symbol	TZRO
Cap	\$250,000,000
Token Price *	\$10.00
Token Type	ERC-20
Fundraising Goal	\$250,000,000
Pre-Sale Launch	12 / 18 / 17
Green Shoe Option	\$50,000,000
* Discounts applied to certain investors participating in the token pre-sale and otherwise in the Company's discretion	

201

The Startup opened the ICO pre-sale on 18 December 2017, and the company was able to publicly state on 1st March 2018 the collection of 100 million, with the execution of SAFES with approximately 1,100 accredited investors. tZERO closed out its Security Token offering the 6 August 2018, raising \$134 million in aggregate consideration (this sum includes \$30 million from repayment of intercompany debt between tZERO and Overstock. After that, Overstock officially announced²⁰² it had entered into a short-term agreement with Hong Kong private equity firm GSR Capital to buy:

- \$270 million in tZERO equity
- \$30 million purchase of tZERO Security Tokens from Overstock.com
- Up to \$104.55 million in shares of parent company Overstock.com, at a price of 33,72 \$ August 1st closing price less 5 %

201 <https://www.tZERO.com/tZERO-overview.pdf>

202 <http://investors.overstock.com/mobile.view?c=131091&v=203&d=1&id=2363163>

3.4 Valuation multiples

According to the SEC itself, being the token offered during the ICO a security (it grants 10% dividend, thus it can be said to be an instrument that relies “on the effort of others”). Starting from this point, I thought that if this instrument is paired to equity, than it has to be treated like equity, and equity is made of shares, thus I imagined that by choosing this company, I could have the possibility to do a comparison with ICO while still using traditional methods like that of comparable transactions. Coming to valuation, I found the company’s financial statements on the SEC memorandum, which highlight a situation in which it can’t be performed a DCF analysis, having negative cashflows to discount. What I could indeed do, was to establish a set of comparables and using the financial statements identified for tZERO to find an enterprise value, then making assumptions about the number of tokens issued and trying to justify a price per token.

3.4.1 Assumptions on comparables

In order to find comparables for the valuation of tZERO token price, I used the following criteria, using Eikon Thomson Reuters²⁰³ as the database for financial statements data:

- I took as comparables only companies pertaining to the “Financial & Commodity Market Operators & Service Providers” sector, being tZERO aim to be associated to that sector and to disrupt this latter.
- Furthermore, I needed to take into consideration companies running (at least a part of) a Blockchain business as much as I could, to take into account the difference in technology that leads to profound difference in the financial indicators measure.

The selection process resulted in the selection of the following comparables:

- LongFin Corp: Longfin Corp. operates as an independent finance and technology company. The Company offers commodity trading, alternate risk transfer, and carry trade financing services. Longfin also provides hedging and risk management solutions to importers, exporters, and small medium business enterprises²⁰⁴.

²⁰³ <https://eikon.thomsonreuters.com/index.html>

²⁰⁴ <https://www.bloomberg.com/profiles/companies/LFIN:US-longfin-corp>

- Greensky INC: s a financial technology company founded in 2006 based in Atlanta, Georgia. The company provides technology to banks and merchants to make loans to consumers for home improvement, solar, healthcare and other purposes. Financing for GreenSky credit programs is provided by federally-insured, federal and state-chartered financial institutions²⁰⁵.
- MarketAxess: is an international financial technology company that operates an electronic trading platform for the institutional credit markets, and also provides market data and post-trade services. It enables institutional investors and broker-dealers to trade credit instruments, including corporate bonds, and other types of fixed income products²⁰⁶.
- Virtu Financial Inc: is one of the largest high-frequency trading and market making firms. It provides two-sided quotations and trades in equities, commodities, currencies, options, fixed income, and other securities on over 230 exchanges, markets, and dark pools²⁰⁷
- Interactive Brokers LLC: s a U.S.-based electronic brokerage firm. It is the largest U.S. electronic brokerage firm by number of daily average revenue trades, and is the leading forex broker. The company brokers stocks, options, futures, EFPs, futures options, forex, bonds, funds and CFDs.²⁰⁸
- Riot Blockchain: Riot Blockchain Inc, a onetime biotechnology firm²⁰⁹. The company is building a cryptocurrency mining operation, operating mining computers to generate cryptocurrency (primarily Bitcoin)²¹⁰.

3.4.2 Multiple used

For problems relating to reliability of other ratios due to negative indicators like EBITDA and EBIT, I used the EV/Sales ratio, and I obtained an average EV/Sales of 11,43, that I multiplied with the 2017 Sales of TZERO, obtaining an EV of roughly 200 million, to which I subtracted the net debt, to arrive at an equity value of roughly 138 million. Then, since I had not information about the number of tokens issued during the ICO, I needed to create a proxy for this number. What I've done is to derive the number of tokens issued for every price range declared by the company, thus I divided the first \$ 9,999,999 to be funded by the price at which they have been bought, then I

205 <https://en.wikipedia.org/wiki/GreenSky>

206 <https://en.wikipedia.org/wiki/MarketAxess>

207 https://en.wikipedia.org/wiki/Virtu_Financial

208 https://en.wikipedia.org/wiki/Interactive_Brokers

209 <https://www.reuters.com/article/us-riot-Blockchain-moves/riot-Blockchain-names-new-leaders-as-previous-boss-faces-fraud-charges-idUSKCN1LQ04G>

210 <https://ir.riotBlockchain.com/annual-reports/content/0001079973-18-000410/0001079973-18-000410.pdf>

moved to the second funding range and divided again for the price of the tokens for this range, repeating this step until I arrived at the maximum price practiced by the company whatever the funding would have been. Then, once calculated all the tokens issued for the funding ranges identified, I derived the “missing funds” (out of the 134 that the company has officially declared to have raised) by making the difference with the amount already funded, and again I divided this residual amount for the full price practiced for this case, \$ 10. What I obtained is that the number of tokens issued during the ICO is a number between 17 and 18 million tokens. All I had done then was to divide the equity obtained as described above for the price of the tokens issued to find a price per token.

The equity value of the company is very close to the amount funded, and the price per token obtained by dividing for the number of tokens is reasonable: \$ 7,84.

Ranges	Amount	Price per token	Estimated token amount
1 st Range	\$ 0 to \$ 9,999,999	\$5,00	\$1.999.999,80
2 nd Range	\$ 9,999,999 to 49,999,999	\$6,67	\$5.997.001,50
3 rd Range	\$ 49,999,999 to 99,999,999	\$8,00	\$6.250.000,00
4 th Range	Remaining \$ 34,000,000	\$10,00	\$3.400.000,00
			\$17.647.001,30 Total

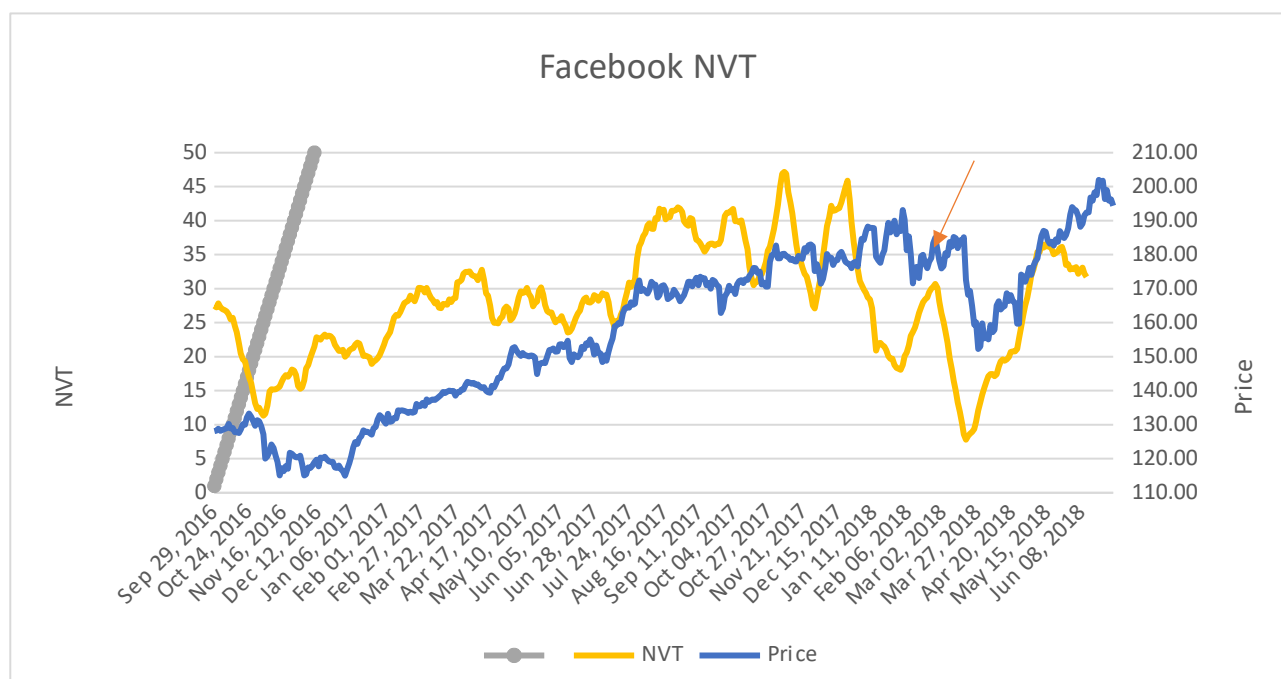
Company name	EV/Sales		
LongFin Corp.	3,40	tZERO Revenues	\$16.733.000,00
Greensky	13,54	EV	\$191.230.301,67
Marketaxess	16,77	Debt	\$54.680.000,00
Virtu financial	5,62	Cash	\$1.885.000,00
Interactive	15,70	Equity	\$138.435.301,67
Riot Blockchain	13,54	Estimated tokens	\$17.647.001,30
AVG EV/Sales	11,43	Price per token	\$7,84

If we even account for the new equity injection the company had from GSR equity capital of 270 million, the price per token goes to \$ 23,14.

For the calculation done up to now, the price of \$ 7,84 per token seems to be an indicator of the token being priced too much for the final investors, but the equity injection mentioned above could potentially nullify that threat.

3.4.3 Detecting overvaluation with NVT ratio

Unfortunately, Tzero securities have not been already issued, thus, we can't compare the token quotations with respect to their price to compare it with the NVT, but we can make a comparison between other listed companies having an already traded token to see if the indicator can at least help in finding moments of over/undervaluation. Remembering Metcalfe's law, if it's true that Facebook price can be clearly determined by this law (Metcalfe itself proved this law to work for Facebook), that indirectly means that the value of the network should be a sort of predictor of the price going up and down, no matter the other financial indicators. Here below I used the NVT ratio to try to predict value for Facebook:



Two interesting considerations can be done here:

1. As the arrows show, the NVT anticipates at least two the possibility of an undervaluation, especially in the price drop identified by the rightest arrow.
2. This ratio only helps us ex-post in finding an additional signal of over/undervaluation, but it doesn't help in predicting the price movements of a stock for two reasons:
 - a. The data with which is constructed (14 days moving average) are more precise than a punctual reference to the ratio, but they run the risk of retarding the signaling effect
 - b. There is no evidence of which is the "acceptable range" within which a NVT should be in order to be sure that there is an under/overvaluation. For this reason, it could be

211 Data about historical prices and market cap taken from Yahoo finance

better to use a % change in that ratio to see if its volatility helps us in making the model more precisely.

3.5 ICO announcement and stock value

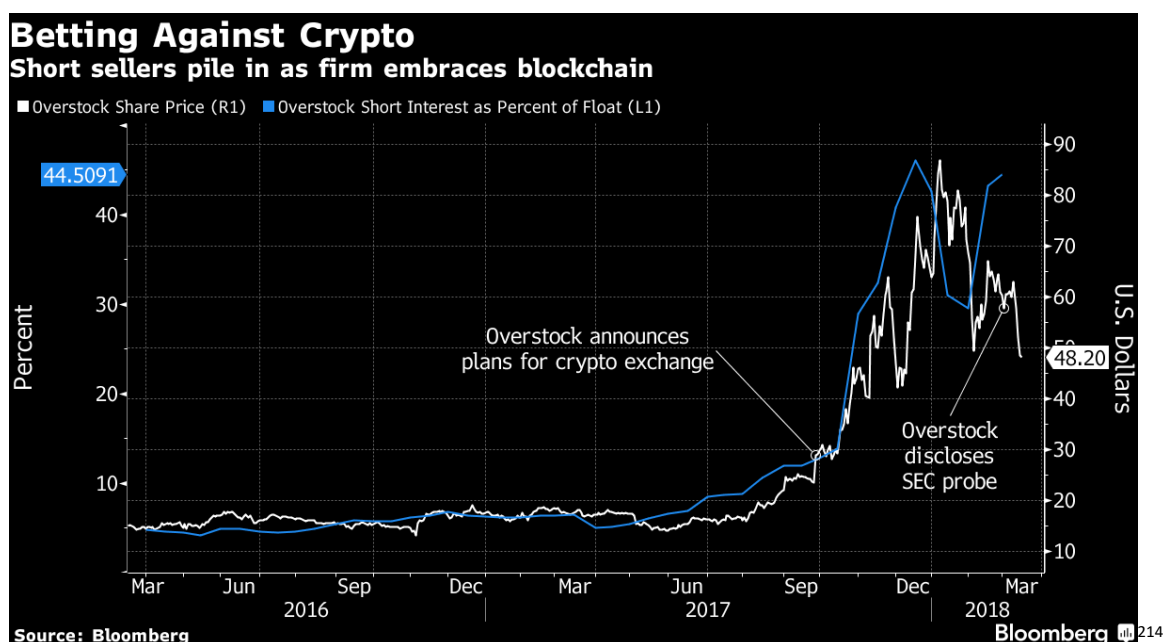
tZERO holding Overstock²¹² saw its stock price soaring after the ICO announcement, with news about negative EPS that seemed to don't affect the share price.

Fiscal Quarter End	Date Reported	Earnings Per Share
Jun2018	08/09/2018	-2.2
Mar2018	05/08/2018	-1.74
Dec2017	03/15/2018	-2.71
Sep2017	11/08/2017	-0.03

213

212 <https://www.overstock.com/>

213 <https://www.nasdaq.com/earnings/report/ostk>



What is amazing is that analyzing the correlation between Overstock price and that of Bitcoin, we can identify how the stock is not anymore influenced by real business data but is directly connected to the price of Bitcoin, no matter the earnings reported by the company, which are. Here below the correlation coefficient analyzed for 3 different time ranges, analyzed weekly to limit the distortion effect caused by stocks trading only 5 days per week while Bitcoin being traded 24/7 ²¹⁵:

	5Y to date (3/09/2018)	2Y to date	Y to date
Correlation	0,87	0,91	0,78

What gives evidence of a non-casual correlation is the following list of events, occurring together:

- After the January 2018 bubble burst, both fell to their first bottom on the exact same day, February 6.
- Both would go on to experience a relief rally of which both peaked on February 20.
- Both prices fell to their lowest prices of 2018 on the exact same day, June 28.

214 <https://www.bloomberg.com/news/articles/2018-03-15/overstock-hands-win-to-bears-with-probe-warning-strategy-shift>

215 Historical price obtained from Yahoo Finance



216

3.6 Bubble to burst? Comparison with dotcom bubble

A bubble is “an economic cycle characterized by the rapid escalation of asset prices followed by a contraction”²¹⁷. The definition anyway, doesn’t allow to underline few hidden aspects of this phenomenon. First, when there is a big misalignment in the value of something and the price at which this thing is actually bought, that means that a triggering event has changed the way this thing is conceived by people in the market. Thus, when the price fluctuates with no accordance to its value, it’s because its price is now influenced by a sort of new expectation towards that instrument. This is what basically happened during the tulip mania with the so called “herding behavior”²¹⁸. Even if we don’t perform a thorough financial analysis, it sounds strange that someone sold its own house to buy a tulip, but this is what basically happened. Tulips from Turkey were of many varieties, leading rich people to literary fight with others to have one, they passed from being flowers to represent a sort of “new status” to rich people. It’s clear that when something like this happens, it is not anymore a matter of valuing tulips, but it suddenly becomes a play in which a crowd of people bets that rich people will buy tulips. The DotCom bubble is the same, people were buying stocks in .com just because there was an expectation from the whole internet market to rise. With the financial crisis, banks were granting loans to whoever asked simply because there wasn’t

216 <https://www.coindesk.com/what-etf-theres-a-wall-street-stock-thats-already-tracking-bitcoin/>

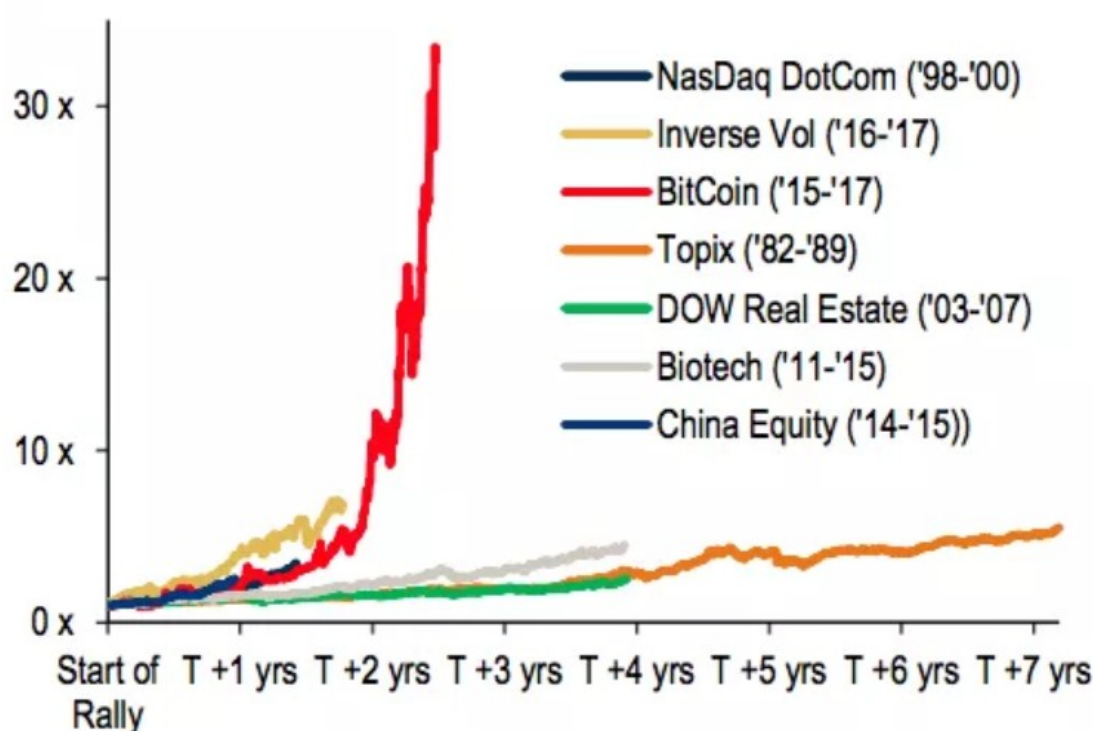
217 <https://www.investopedia.com/terms/b/bubble.asp>

218 <https://arxiv.org/pdf/1806.11348.pdf>

anymore the willingness or the need to check for houses real value, and then all the securitization mechanism did the rest. Blockchain is doomed to have a similar path, people will become more and more engaged with such companies, and will invest money not in real products, but in expectation on Blockchain technology, forgetting about what to buy, but to buy it because of the Blockchain hype.

Are we in a bubble, then? Well, if one looks at the graph below, there's not much to complain about it, and the dynamics happening are more or less the same of what were on the Dot.com bubble

Chart 42: Are bubbles becoming more “bubbly”?



Source: BofA Merrill Lynch Global Research. Bloomberg. Using TPX Index, CCMP Index, DJUSRE Index, NBI index, SHASHR Index, XIV US Equity and XBT Curncy. Data is normalized and rebalanced at 100 at the start date of the rally (lowest data point) and ends at the top of the rally (highest data point).

219

There are more analogies than differences between those 2 bubbles, the main difference is that the DotCom bubble was the result of the big amounts of money put at stake by institutional investors, while the ICO is basically a sort of B2C or even C2C phenomenon in which everyone is allowed to participate, anyway the interest towards that instrument is rising also in institutional investors, putting cryptocurrencies like Bitcoin in their portfolio not to diversify a portfolio but to boost its

219 <https://heisenbergreport.com/2017/11/25/bitcoin-explodes-through-8700-to-record-high-thanksgiving-table-discussion-was-all-about-bitcoin/>

returns.²²⁰. Coming to analogies²²¹, like in years 2000, companies in ICOs process show lack or absence of a real viable business model like it was for the Dot.Com bubble, and marketing expenses which even overtake the cost of the business to be run. The problem here is that is all about advertising and marketing campaign, and not about building a sustainable business. Here below the list of the major companies rise in public companies within the year 2017 by simply mentioning the word “Blockchain” in their new names:

Name	Trading range 2017 (high vs low)	Former name(s)
Bitcoin Services Inc	42500%	Tulip BioMed Inc, Cell Bio-Systems Inc, Direct Music Group Inc, BMX Holdings Inc, JLL Miami Enterprises Inc
UBI Blockchain Internet Ltd	20445%	JA Energy
Blockchain Mining Ltd	12021%	Natural Resource Holdings Ltd, Cidav Printed Circuits Ltd
HIVE Blockchain Technologies Ltd	6384%	Leeta Gold Corp, Pierre Enterprises Ltd, Carmelita Resources Ltd
First Bitcoin Capital Corp	5897%	Grand Pacaraima Gold Corp, Mindenao Gold Mining Corp, United Development International
Global Blockchain Technologies Corp	2900%	Carrus Capital Corp
NXChain Inc	1700%	AgriVest Americas Inc, Robocom Systems International Inc, Robocom Systems Inc
Riot Blockchain Inc	1611%	Bioptix Inc, Venaxis Inc, AspenBio Pharma, AspenBio Inc
Bitcoin Group SE	1503%	AE Innovative Capital SE
Online Blockchain Plc	1300%	On-Line Plc
Long Blockchain Corp	458%	Long Island Iced Tea Corp, Cullen Agricultural Holding Corp
Blockchain Power Trust Unit	309%	Transeastern Power Trust

222

220 <https://icowatchlist.com/blog/differences-crypto-dot-com-bubble/>

221 <http://www.irma-international.org/viewtitle/32329/>

222 <https://qz.com/1175701/putting-bitcoin-or-Blockchain-in-a-company-name-is-sometimes-enough-for-a-pop-on-the-stock-market/>

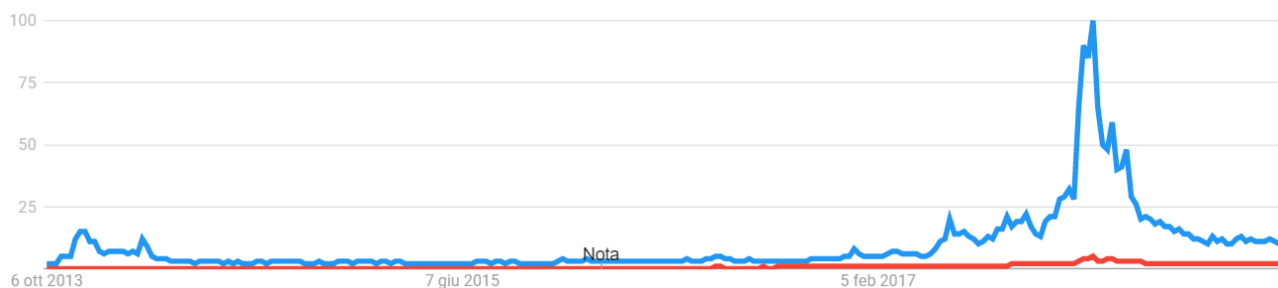
An authoritative study demonstrates how during the 1998-1999 period²²³, the average rise in price during the period within the previous 2 days and the 2 days after the announcement of the name change by the .com company is around 93%, with the appreciation effect being not temporary.

Conclusions

After having disclosed the main aspects of Blockchain technology, is clear how it constitutes the common basis for all new emerging technologies, the main ones being Artificial Intelligence, Internet of things and Big Data. The exponential growth in the amount of data processed and the need to store them and be exchanged between different parties requires a safer way to keep them stable and accessible at any time, with the need to have a technology which could let the other ones being interconnected with a single, verified and forever traced flow of data. All the ICO panorama is built around that new technology, and the success or failure of this latter is extremely correlated with:

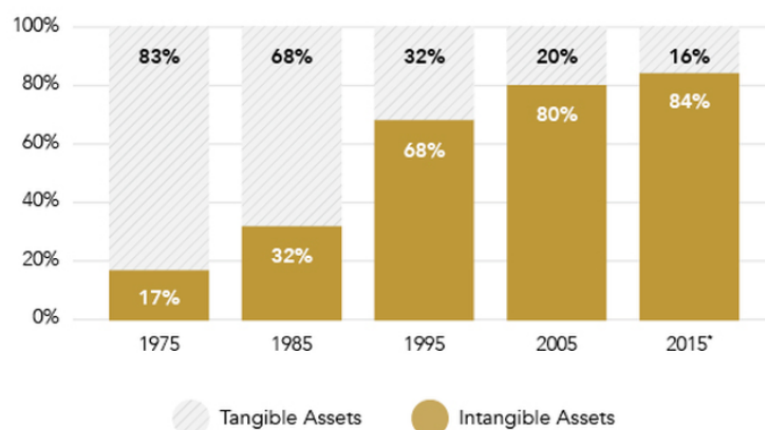
1. **The creation and implementation of viable use cases for Blockchain businesses:** Blockchain's speech is still all about this technology making all dreams possible, with still too few ideas (but of course we have very interesting exceptions) on how to run a business which is based on this latter.
2. **“Blockchain not Bitcoin argument”:** ICO success will be totally correlated to the success of Blockchain, what needs to radically change is the process of Bitcoin price news dominating the talk, and a downfall in Bitcoin price could also be seen as a good news for the Blockchain community, allowing people and entrepreneurs to focus only on real business purposes. By the way, the fact that we're still in the “Bitcoin not Blockchain” trend, is also due to natural causes like the need to adapt existing technologies to the new one whilst Bitcoin being a ready made application that could already exploit all of its value. Here below I traced Google trends data about Bitcoin vs Blockchain. Guess what is the line representing Bitcoin? And that line is impressively similar to that of Bitcoin price. Put in other terms, if Bitcoin continues to go up and down, people will still focus on Bitcoin and not Blockchain, which will be (literally) put on the floor like it (still!) is in the graph.

223 http://www.andreisimonov.com/NES/BF/Cooper_A_Rosecom.pdf



3. **The role of cryptocurrencies as a competitor of fiat currencies:** For what concerns the future of cryptocurrencies, they're here to stay and to let us remember that it could be time to move from the old conception of paper money toward a new digital representation of this latter. There is a reason for this hard statement to make sense. Indeed, there is a unprecedented shift from material goods and services to immaterial ones, just look at the figure below about intangible assets proportion to tangible ones in S&P 500.

COMPONENTS of S&P 500 MARKET VALUE



224

Once said this, it is also unquestionable how we are becoming increasingly correlated on a worldwide level: communication channels, international trade, are only an example of how it is all becoming bound, and since those “connected points” are everyday more intangible, there should soon be the need to treat intangible goods or services with the same level playing field currency. The principle is that we nowadays accept Euros, US dollars or whatever is considered to be an official currency just because we trust the value it actually represents. There is no longer the reason to stop cryptocurrencies just because they have no legal tender, and not because we're all suddenly became libertarian, but just because paper money will no longer help as a valid mean of exchange as they did up to now, or better, it will lose its value as such just because new technologies enhance the characteristic of

immateriality among material one. The world we're (they're) imagining, its certainly based on technology guiding our lives from the "programmed morning coffee" to the dinner meal cooked by a robot. We've heard millions of times about smart cities concept, and I will take this concept as an example. Think about a city in which in an everyday routine a man could start-up its own car with the smartphone, charge batteries with the push of a button and be informed about traffic while it is travelling in real time. It is all soon potentially possible, or at least they repeated it many times it is, isn't it? Now think of (at least) one of those real time services being offered for a fee. Would you use all of those real-time connected services while still paying with heavy-unconnected coins? In a real world, they will probably charge you an extra fee for this... Where would you bring your heavy cash if the world is increasingly offering services without physical spaces in which to go? One could argue we already have Google wallet or something like that to pay without cash....But again, what is the control level of such a great amount of data with traditional technologies? Would you exchange all of this impressive amount of data (with different levels of privacy embedded, depending on the situation) with the risk of having them hacked or misused by (even authorized) third parties? Here it comes the utility of Blockchain, helping all of these goods and services to be stored forever and kept safe, with a unique channel over which digital goods and services could be exchanged or cryptocurrencies, with the single user deciding on its own to give to a third party or not the "keys" of a certain subset of its own data. To summarize this point, Blockchain is not only useful for the present, but is increasingly important for the world that WE imagined for the future, and it is useful because we're imagining that precise kind of future full of technologies exchanging impressive amounts of data. For the cryptocurrency environment to prevail on fiat currencies, I see these scenarios occurring (together or alone) in the following 10-15 years:

- The process of cryptocurrency adoption in member states will start with few first comer countries which will substitute their own fiat currency with its crypto-equivalent while maintaining ATM running for the exchange of those latter in other fiat currencies to be used towards fiat-currency based countries. The shift process will be longer with respect to what happened with Euro introduction, but with the same mechanism of retiring fiat-money to issue the crypto-equivalent. I expect those countries to be among the first countries by cashless transactions and digital innovation index, like it could be Sweden or Estonia. Or, to be preceded by hyperinflationed countries in which the abandoning of the local

worthless fiat-currency could be a booster for cryptocurrency adoption, given that it is well-endowed in technological infrastructure to support such a new economy. There are already interesting tentatives of new emerging cryptocurrencies trying to beat fiat currency for its price stability, with the example of Tether being backed 1 by 1 with US.Dollar²²⁵. For what concerns EU, regulators are prohibiting EU countries to issue their own cryptocurrency, but I think that this behavior will be soon abandoned if cryptocurrencies will become mainstream in some countries, with the clear need for regulators to at least accept this new framework to become legal.

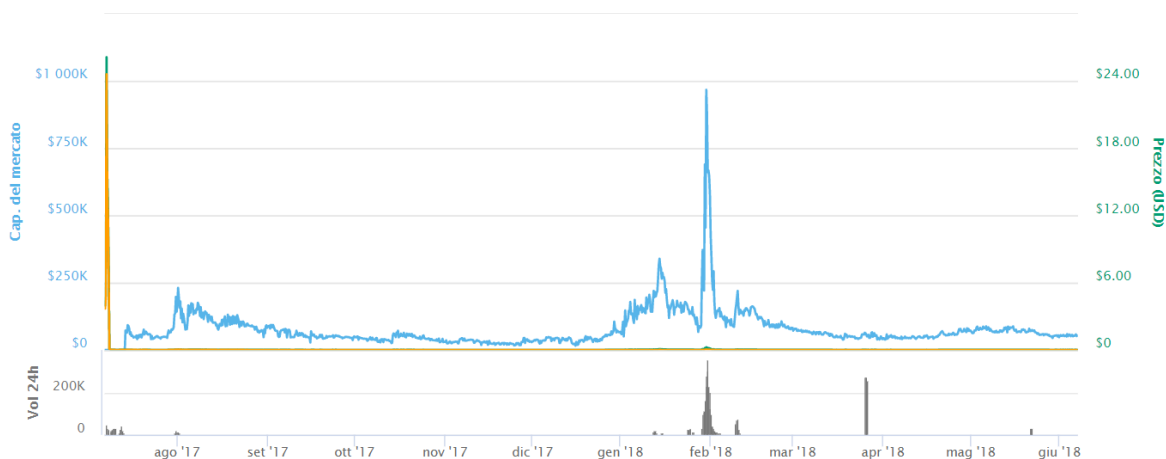
- Consequent to the point above, it will be possible that since there are hundreds of cryptocurrencies issued, we could potentially face a situation in which different cryptocurrencies are accepted in a country as long as one of them reveals to be the best one, and then go for the adoption, or to choose to maintain this corridor of currencies competing with themselves.
- According to level at which Blockchain adoption will be in the future, it could happen that there will be not only competing cryptocurrencies for a whole economy, but for different services offered and for different privacy levels for example. In a phrase “there will co-exist different cryptocurrencies for different use cases related to privacy and utility”.

ICOs are here to convey the message that everything can be tokenized: a product, a service, a financial instrument, whatever could be represented as a sort of digital representation of this latter. What has to be remarked first is that whilst ICOs are an unstable, risky operation, they also provide start-ups with unprecedented amount of money. By the way, the market is still immature, FOMO is dominating the speech, and one impressive example is given by the ICO called “Useless coin” which raised around \$ 70 thousands and nearly reached 1 million market cap during the end of the year 2017 cryptocurrencies price rise, as a clear signal of people investing their money even without reading at those few clear sentences in an ICO site within which the author itself declares the financing event to be a joke (see the 2 figures below).

225 <https://tether.to/>

But remember—this is a *completely honest* ICO, which means I don't want anyone to mistakenly *expect* the value of the tokens to go up, either. They're called Useless Ethereum Tokens for a reason.

226



227

There is evidence (and also a great amount of other examples) for large part of ICOs like the one reported above to be a total scam, but there are also interesting projects which need to be taken into serious consideration and be evaluated according to the contribution they could bring to the Blockchain environment, regardless of the price at which their own token is traded in this irrational market. This new financing mean being ICOs has the potential to disrupt traditional financial markets. Indeed, it becomes clear for example how VC will be forced to change investment strategy by being no longer only financiers of start-ups but also active investors in crypto financing startups. They won't disappear then, they will simply change the level playing field on which the funding mechanism happens. What will probably change forever instead, is not the type of financing used, but the way the same old financing mechanisms are built, with institutional investors (centralized institutions, then) decreasing their share over individual investors funding startups together in crowds.

For what concerns IPO future, they run the risk of being substituted by ICOs, which already accounts for nearly half of the total IPO funding this year²²⁸ and promise to overtake that amount

226 <https://uetoken.com/>

227 <https://coinmarketcap.com/it/currencies/useless-ethereum-token/>

228 <https://www.forbes.com/sites/caitlinlong/2018/07/22/icos-were-45-of-ipos-in-q2-2018-as-cryptos-disrupt-investment-banks/#57d3a9f1794c>

soon. A possible scenario is for sure that of big multinationals doing their own ICO, and I think we can see something like Facebook or even more probably Amazon launching their own token within the next 2 years. What is clear is that future regulation about a practically unregulated environment could be the watershed for ICOs to become mainstream over IPOs too or to be doomed to failure. The future of ICOs in general is strictly connected to the development of use cases for Blockchain companies. What happened up to now is that many makeshift entrepreneurs tried to profit on this period of easily-funded crypto start-ups without a clear idea on the business model on top of which to base the company's destiny. Then, what needs to happen as soon as possible for all of this phenomenon to become sustainable, is to shift from the obsession of prices to the conception of Blockchain as a business disruptor to be implemented in basically all sectors. Bubble, then? Of course it is, and complete scams ICO raising hundreds of millions are, together with people buying "only in crowds" like it happened at the end of 2017 with Bitcoin reaching nearly 20 thousand Dollars, a sufficient proof for it but with the addition that we still don't have an idea of what is the intrinsic value on top of which we're letting this bubble grow. Consequently, we don't even know how big this bubble is and how big it could become. For sure regulators are hiding enough to let it grow without any uncertainty, and they will be in part responsible of this latter to eventually burst. Technology speed can't be for sure overtaken by rules, but regulators should try to at least follow such a quick change instead of using the wait-and-see approach. What is worrying in here is how easily regulators let new instruments be used without arguing on the method. Briefly, I think that we didn't learn much from 2008 financial crisis, I'm not saying that is time for it to repeat, but the fact that we're letting those (still) unknown instruments trade in traditional markets (I'm thinking about Bitcoin futures on Chicago mercantile exchange) are both a tentative of making a totally different instrument become step by step a "traditional one", which is wrong by nature and a way to sow the seeds for a chain of events being for example Bitcoin put in company's financial statements as an investment asset without even having idea of its real value. No matter the future outcome, ICOs are the demonstration that traditional financing mechanism and financial models have to be at least rethought to be adapted to this new type of business, not just because they passed from being reliable to be useless all of a sudden, but just because the assumptions on which they work are wrong for a market which is now "full of peers" with even irrational expectations about price. What is indeed clear is that the way new emerging business raise money can't magically change the way they're valued, thus, a convergence between valuation models will occur in the next years and Blockchain panorama will start to correlate more traditional financial markets.

Bibliography

C.Burniske; J.Tatar; “The innovative investor’s Guide to Bitcoin and Beyond”; McGraw Hill; 2017

Sitography

www.anders.com
www.andreisimonov.com
www.annualreports.com
www.arxiv.org
www.atkearney.com
www.bbva.com
www.bcg.com
www.bitcoin.com
www.bitcoin.it
www.bitcoin.org
www.bitcoin.stackexchange.com
www.bitcoinblockhalf.com
www.bitcoinmagazine.com
www.bitcoinmagazine.com
www.bitnewstoday.com
www.bizcommunity.com
www.blockgeeks.com
www.blog.coinbase.com
www.blog.coinfabrik.com
www.blog.omni.foundation
www.blogs.uta.fi
www.bloomberg.com
www.bravenewcoin.com
www.caixabankresearch.com
www.cambridgeanalytica.org
www.capgemini.com
www.capitalmarketsblog.accenture.com
www.ccn.com
www.cdn2.hubspot.net
www.cms.edelman.com
www.coindesk.com
www.coinmarketcap.com
www.cointelegraph.com
www.cointelligence.com
www.cryptocurrencyfacts.com
www.cryptome.org
www.cs.ru.nl
www.csef.it
www.daneshyari.com

www.dbjournal.ro
www.deloitte.com
www.digrate.com
www.ecb.europa.eu
www.ecgi.global
www.econstor.eu
www.ee.stanford.edu
www.eff.org
www.eikon.thomsonreuters.com
www.eos.io
www.esmt.org
www.eurim.org.uk
www.ey.com
www.faculty.chicagobooth.edu
www.fbinsights.files.wordpress.com
www.feedough.com
www.fidelity.com
www.fon.hum.uva.nl
www.forbes.com
www.futurelearn.com
www.g4scashreport.com
www.gartner.com
www.goldmansachs.com
www.google.it
www.hackernoon.com
www.hashcash.org
www.hbr.org
www.heisenbergreport.com
www.hit.bme.hu
www.huffingtonpost.com
www.icobench.com
www.icoexaminer.com
www.icorating.com
www.icowatchlist.com
www.ig.ft.com/
www.impresaemangement.luiss.it
www.internetlivestats.com
www.investopedia.com
www.ipfs.io
www.ir.riotBlockchain.com
www.irma-international.org
www.it.finance.yahoo.com
www.johnlothiannews.com
www.keatsmoodledevtest.kcl.ac.uk
www.law.ox.ac.uk
www.link.springer.com
www.masterthecrypto.com
www.medium.com
www.nakamotoinstitute.org
www.nakamotoinstitute.org
www.nasdaq.com

www.networkworld.com
www.news.bitcoin.com
www.nytimes.com
www.opinionator.blogs.nytimes.com
www.ourworldindata.org
www.outlierventures.io
www.overstock.com
www.people-press.org
www.pewresearch.org
www.pnas.org
www.poseidon01.ssrn.com
www.powercompare.co.uk
www.qz.com
www.r3.com
www.reddit.com
www.res.cloudinary.com
www.researchgate.net
www.reuters.com
www.riksbank.se
www.satoshi.nakamotoinstitute.org
www.sec.gov
www.sfmagazine.com
www.shahrulsufianhamdan.wordpress.com
www.sophia-project.org
www.springer.com
www.steemit.com
www.stem.cz
www.techcrunch.com
www.technologyreview.com
www.techopedia.com
www.tether.to
www.theguardian.com
www.thetimes.co.uk
www.thindifference.com
www.time.com
www.towardsdatascience.com
www.tZERO.com
www.uetoken.com
www.untitled-inc.com
www.upfrontanalytics.com
www.venturebeat.com
www.visualcapitalist.com
www.vitalik.ca
www.voxeu.org
www.web.undp.org
www.weforum.org
www.weforum.org
www.weidai.com
www.weusecoins.com
www.whitepaperdatabase.com
www.wikileaks.org

www.wikipedia.org
www.woobull.com
www.worldpay.com
www.xrphodor.wordpress.com
www.youtube.com

Resume

Overview

“Disrupt it, or be disrupted”: this could be the main message that this work wants to convey. New emerging technologies are everyday challenging and breaking man’s habits, from the way he could drive cars to the communication channel with which it can rely on other parties while being 24/7 h connected. Technologies are no longer waiting for man to adapt to the future; in the last decade, they turned upside-down the way we think about technology, passing from thinking about technology as a solution to be created for man’s needs, to an unrestrainable flow of innovation which leaves man with only a decision to be taken: adopt it, or let it be adopted by others and then be forced to follow.

Schumpeter would have thought about years 2000 as an economic cycle in which a cluster of innovations would shape the economy for the years to come, Internet being the first above all technologies. From this main innovation, all the other ones followed, and the disruption of course is enhanced by the increasingly combinable features of completely different technologies. We saw the rise of social networks and e-commerce platform as a way to make official the change of paradigm: we’re no longer alone and separated by physical geographical boundaries, but we constitute a web, a network, a community which everyday interacts and share information. New emerging technologies such as Big data & analytics, Internet of things, Artificial Intelligence are the proof of the fact that we’re increasingly creating value by combining more and more things together, with sophisticated analytics used as an input for other technologies to work more efficiently and consequently giving back a better output. For all of these reasons, the amount of information with which we’re dealing every day is multiplying its size, introducing the need to use new technologies to process all these information and extract value by combining them. Blockchain technology candidates itself as the one which could function as the main layer on top of which all other technologies rely on. For this reason, is important to understand what are the main characteristics of this technology, and how it could potentially shape a completely new world.

From the ashes of financial crisis, Bitcoin was created by an author under the pseudonymous name of Satoshi Nakamoto. Bitcoin already reveals itself as a way to protest towards the establishment, with the first transaction ever made reporting the link of an article whose title was “Chancellor on brink of second bailout for banks”, with the clear reference to a protest toward the way financial crisis are managed, but more in general to how the financial system works. With the Birth of Bitcoin, centralized authorities (not only financial ones) are now conceived as pool in which all the

decision making flows and all the actions take place, these latter representing, for example, inflationary monetary policies conducted by central banks through centuries, or the massive use of data and the need for a new privacy framework to protect people's private life from "Big brother's eye". Bitcoin comes out as the natural consequence of all of these concerns, and constitutes what is called a killer application, to which goes all the merit of having introduced the Blockchain to the world, for sure accelerating the approach to new currency frameworks and financing tools such as Initial coin offerings. The financial deregulation occurred through the last decades has certainly contributed to such an "anarchist-like" currency framework like Bitcoin is, and this latter could be potentially seen as the most recent outcome of this idea of self-regulating markets which leads to more efficiency. Years of increased competition and globalization provided the world with a new environment, without old monopolies conducting discriminatory prices. It's quite natural that at the end of this de-monopolization process, one of the main monopoly ever created is put into discussion, with this latter being the issuance power in the hand of central banks.

One of the main important outcomes of Blockchain technology is constituted by Initial coin Offering as the first financing mean through which to finance companies which are running Blockchain businesses. Initial coin Offering candidates as the "public alternative" to traditional financing methods like Initial Public offerings and Venture capital, with its size already challenging those latter. ICOs rise as an alternative way to manifest the fact that the world is changed, and there's no longer the reason to wait for single entities to decide whether or not a start-up's worth something, but to refer to a network of peers we all constitute to reach that objective, breaking old financial barriers and permitting financial inclusion to potentially every smartphone-endowed person. Of course, there is hype among this argument, with fear of missing out (FOMO) driving investment decisions and leading to perverse mechanisms of prices going up and down with apparently little or no evidence of rationality.

The result of this "irrational behavior" is greed dominating the entrepreneurs' side of ICOs, requiring far more money than they need to develop their own business idea, or even taking the money and use them for other purposes. The figure of the entrepreneur is radically changed, new businesses are increasingly conducted by people with technology know-how, and this technology know-how sometimes reveals to be even more important than managing one. Blockchain technology applied to ICOs is also showing a changing job market too, with companies requiring more and more "tech savvy-people" in proportion to managers with economic background. Here below, it will follow a brief resume of the chapters' content and the logic through which they have been built.

Chapter 1

The chapter wants to provide the reader with a thorough analysis of the technical and historical background surrounding the argument that is treated in this work, as a sort of “to-have” knowledge to be able to understand the meaning of what is following in the next pages. The chapter starts by introducing a starting point as a justification for what is following in the description, which is the privacy issue to be found in what is called the Cypherpunk movement, born with the aim to solve the privacy problem in the electronic age, age in which the rise of an impressive amount of information and transactions are continuously and increasingly connecting people, requiring the exchange of information (or at least a part of them) which could even be unnecessary for the transaction itself and lead to information misuse or stealing. Once covered all the improvements made in cryptography as a technology with which this privacy issue had been faced, this results useful in demonstrating that Bitcoin is not something which came out from thin air, but was simply the best assembly ever made with the previously described technologies. The reason for speaking firstly of Bitcoin while making all the other themes follow is due to the fact that:

- Bitcoin is the first application ever made with Blockchain technology, it constitutes its killer application
- Speaking of Bitcoin first helps to describe both the causes and the consequence of the birth of Blockchain technology and its consequent further applications.

In chapter 1.5 I then listed and explained the main issues encountered with Bitcoin, with the main aim of showing that what is uncritically accepted as the future of money that will let all the people become rich without any counter-effect, has for sure its bad sides too, with money laundering issues and velocity of transaction as the main problems to be overcome in the next years for the cryptocurrency world to reveal a real competitor to fiat-currencies. Then it comes the most ambitious part of the chapter, which is that of trying to identify the main causes of Bitcoin pre-conditions for its birth, which I retain are far more than just privacy related issues. The main aspect I identified are, as a consequence, the general decrease in trust towards centralized institutions, as authoritative studies like the annually published Edelman trust barometer helps to clearly identify, caused by power being wrongly exploited by authorities and resulting in people distrusting the way their lives are shaped from the top of the social pyramid, with communication channels too declining their levels of trust and peaking this distrust trend in Cambridge Analytica scandal. Information too reveals to be both the cause (Cambridge Analytica case shows it clearly) of such a great rise in the importance of giving power to people in managing their own data and even questioning about the “fair value of information”, which is returned back by companies in the form

of products or services which could have embedded (or not) in the price the value extracted from those free flow of data taken from the web. Last but not least, I identified the trend in the use of paper money as being a good component for predicting Bitcoin adoption worldwide, to show again that all of the causes encountered as a reason for Bitcoin's birth are in some way correlated (obviously, I couldn't calculate this empirically) to Bitcoin 's adoption rate. What I underline in this dissertation is that basically all the causes encountered as a justification for Bitcoin's adoption are linked to each other, with one cause enforcing the occurrence of another one. For this reason, I tried to conduct an empirical demonstration of these causes to have shaped Bitcoin adoption in each country. What I was trying to do was to set a scoring map in which I was entering country names in terms of their position in Digital innovation index, Corruption perception index, Internet penetration rate, Trust levels between each other, Competitiveness index and so on so forth, taking the first 5 countries which scored the lowest cumulative position (the lower the value, the higher the position of the country in every single indicator) as the 5 countries in which there was the highest adoption for Bitcoin, using Bitcoin software downloads per 100000 capita as a proxy for adoption. The model was not included because of uniformity of data issue, different indicators reporting different time ranges for listing, different inputs and different country lists in the reports encountered. Anyway, this model was already identifying how there were recurring country names (with exceptions caused by information bias already mentioned) among the first countries like Sweden, Estonia, Norway, Denmark, Netherlands, Singapore. It was not a surprise then to notice that those countries had at least one of those (even occurring together) characteristics:

- Strong presence of Bitcoin
- Own-cryptocurrency adoption speeches
- Countries conceived as an ICO hub like Singapore was (and it is).

Chapter 2

The chapter is conceptually divided in two parts: the first part wants to give a comprehensive overview of the ICO market and describes the main definitions used to be taken into account when dealing with such an argument, while the second part is set for analyzing actual valuation models and identifying pros and cons for such tools. The chapter starts with a very broad definition of the term Initial coin offering, trying to provide the reader with the necessary tools to enter the argument instead of giving a set of doubtful definitions. Once given a general introductory speech about Initial Coin offerings, the chapter contains a thorough explanation of what we mean by referring to that term, with the necessary distinction between cryptocurrencies from one side and tokens from

the other one, in order to set a proper organizational division of the financing means through which an ICO could be identified and through which it conducts financing events, being tokens the real instrument to be bought via ICO. The issue in here is that the two terms are often used as synonymous while instead they have very profound differences between each other that many ICO investors still can't distinguish clearly. To explain that difference, I introduced the conceptual division between token and cryptocurrency, being the first a technically different instrument with what is a cryptocurrency and explaining how talking about Initial coin offerings could lead to a misconception of the instruments used within a financing event. Indeed, the characteristic of the instrument issued inevitably shapes the Blockchain layer on which this latter resides and the treatment reserved for it according to its previous classification. Once defined the token classification framework, the chapter goes on by trying to define a common path for ICO process, which is still in its infancy and then can be summarized only by listing general steps:

- Pre announcement: The entrepreneur tries to convey through an executive summary as much information as possible about the ICO project and its main functionalities, to get feedbacks and improving the project in iterative process which ends up in the moment in which the developers team is able to go for the offering and has attracted as much demand as possible.
- Offering: the Team goes for the publication of a Whitepaper, which is the equivalent of what a mandatory prospectus is for IPOs, the difference is that while the mandatory prospectus obviously requires a minimum content for the offering to be legally documented.
- Running Project campaign: The company tries to market its offer as much as possible via communication channels like Facebook, Twitter, Telegram. The aim in here is to convince new investors about the quality of the ICO, by answering questions like: what problems this ICO project wants to solve? Why there is the need to use the Blockchain to solve such a problem? Who are the people involved in the team? What will be the result of the start-up reaching its business goals in the long term?
- ICO sale: Once all is set, the sale starts, and investors try to obtain a stake in the offering by submitting requests.

For the same logic for which I described ICOs before even giving a definition about this term, I decided to put the general information about the market for ICO after the description of the ICO process, which I think can convey a much more clear idea on how this market is still in its infancy, given the elements described above. In this market overview is clear how the whole market

monthly trend could still be significantly influenced by the success of a single ICO (in terms of funds raised) having success during the year, with the biggest ICO ever reaching 4 billion dollars financing while the cumulative funding of the ICO market still being no more than 30 billion (at least by the time of this writing). What follows (with the same logic identified for chapter 1) is a brief history of the birth of ICOs as a sort of skeptical try by J.R Willet, to be considered the first person to conduct an ICO. The story of the first ICO is mentioned both due for the sake of completeness and for the interesting information it could give us about the “average ICO entrepreneur”, which is often a computer expert, a cryptographer, or anyway has technological background. Indeed, what is clear under this chapter is that the issuance process is more related to coding a proper smart contract rather than thinking about a good economic plan or to program sustainable development. One of the main important aspects of this chapter is the explanation of what happened with the failing DAO ICO, with one third of the funds collected through ICO stolen from the organization account just because of a coding error. What this case makes clear is that while ICO are an interesting new financing tool, it has of course many big issues to be solved to become a real competitor of traditional financing methods like IPOs and VC. The first conceptual part of this chapter ends by making a comparison with those two latter financing methods, with the main justification for a company to go for ICO instead of VC financing being:

- It didn't succeed to go for the VC option
- It has a Blockchain based business model which lets the project be more interesting for investors
- It wants to use it as a long term strategy to still reserve the option for IPO

For what concerns IPO comparison here are the main differences encountered:

- ICO reveals to be an entry strategy, while IPOs are traditionally seen as one possible way to exit from a corporate and cashing out an investment.
- ICOs tokens offered are not diluting the ownership of founders, whilst this is what happens with IPOs.
- ICO can compensate initial developers without giving them more control of the network than any other token holder.
- ICO provides the issuer with an early signal about consumer demand.
- ICOs provide a great amount of potential liquidity, which occurs when a cryptocurrency exchange permits trading in the new token. In many cases, the token is tradable for

cryptocurrency or fiat currency within a few days of the ICO. However, there are two caveats:

- Some ICOs offer or require lock-up periods, during which ICO participants may not sell their tokens.
- Many ICO tokens are never exchange-traded, and even if the token is listed, a holder may not be able to find a counterparty. Related to liquidity is the ability to take advantage of temporary overvaluation, a phenomenon that also exists in IPO markets.

The second part of this chapter starts with the most known “cryptocurrency” tools encountered up to now, being Metcalfe’s law. This law is stating that the value of a network should be approximately equal to the squared number of users. This statement has been used to consequently demonstrate that Bitcoin’s price (it was originally tested for Facebook revenues) can be described with a 93% accuracy by an ex JpMorgan employee called Thomas Lee. I summarized what I think of this valuation method being analyzed as follows:

1. I like to see this law as being the maximum value a network can have in the long-term, but not it to describe short-term trends.
2. A law fitting with actual numbers is simply a good outcome to be taken in consideration, but if we assume for a while that Bitcoin is a bubble, finding a good law describing it is only helpful to confirm a bubble, not to identify real value. We still can’t find reference to fundamental value.

The other two valuation frameworks identified as being mainstream for cryptocurrencies in general is that of Quantitative theory of money, which anyway reveals inconsistent with many token being issued for ICOs, given the unstable assumptions we have to make about many factors, velocity above all. The remaining valuation method being Network value to transaction candidates to be a proxy for what is P/E in traditional valuation, with few interesting fits with Bitcoin price and even traditional companies but still needing an adaptation in terms of predicting bubbles and not to confirm them only after they occurred.

The chapter finally ends up in defining the main factors driving an ICO success, which can be summarized as follows:

- The more the price per token in an ICO is high, the lower is the price at which this token is actually trading with respect to ICO event.
- Like with IPOs, the shorter the duration, the more the ICO could have chances of success
- Bitcoin price trend could result in an ICO going to be successful or not, being the market still dominated by that currency.
- Presence of the ICO details in developer's site GitHub

Chapter 3

This chapter wants to be just a way to figure out how traditional valuation methods could at least have sense to be implemented in a particular category of ICOs, which is that of companies issuing a token which could be considered as being a “security token”, thus having the same characteristics of an equity instrument. What I tried to do is to make a comparison with traditional valuation methods by applying multiple valuation methods to a use case being the Overstock's subsidiary tZERO, assuming that the security like characteristics of the tokens issued by the start-up are enough to treat these tokens as such. The only valuation multiple I could use was that of the EV/Sales because of all of the other indicators being negative, thus resulting in useless comparison. I then took a set of comparables and found an equity value accordingly, trying to divide for the exact number of token issued by the company, which is not officially confirmed but can be used as a reliable measure. What I obtained is that the value per token being issued by the company could even result undervalued according to the valuation which could be conducted with the few data available about the company. The main issue for this chapter was initially that of trying to avoid companies with no running business or at least to find listed companies already doing an ICO, so that I could try to find a correlation between the price at which the token traded relative to the price of the stock of the same company, which would have been easily connected to real cash flows. What I sustain in chapter 2 is that I think the market is ready to assist to a big listed company IPO, so that this reasoning described above could be finally implemented and result in a more thorough financial analysis. In the final part of the chapter I tried to apply a crypto-measure like the NVT ratio mentioned in chapter 2 to Facebook's price to see if the contrary was true, which is for cryptocurrency valuation about network values fitting “traditional companies”. The indicator is not precise, but it helps in anticipating times in which there is the possibility of an undervaluation of Facebook. This ratio anyway, only helps us ex-post in finding an additional signal of over/undervaluation, but it doesn't help in predicting the price movements of a stock for two reasons:

- a. The data with which is constructed (14 days moving average)
- b. There is no evidence of which is the “acceptable range” within which a NVT should be in order to be sure that there is an under/overvaluation.

To conclude, I made a comparison between the DotCom bubble, finding that there are more analogies than differences between those 2 bubbles. The main difference is that the DotCom bubble was the result of the big amounts of money put at stake by institutional investors, ICOs are basically a sort of B2C or even C2C phenomenon in which everyone is allowed to participate, anyway the interest towards that instrument is rising also in institutional investors, putting cryptocurrencies like Bitcoin in their portfolio not to diversify a portfolio but to boost its returns. Coming to analogies, like in years 2000, companies in ICOs process show lack or absence of a real viable business model like it was for the Dot.Com bubble.

Conclusion

To sum up, ICO success as a financing method could be said to be extremely dependant on the following issues:

- The creation and implementation of viable use cases for Blockchain businesses: Blockchain’s speech is still all about potential application on real businesses with still too few ideas (but of course we have very interesting exceptions) on how to run a business which is based on this latter.
- “Blockchain not Bitcoin argument”: ICO success will be totally correlated to the success of Blockchain, what needs to radically change is the process of Bitcoin price news dominating the talk, and a downfall in Bitcoin price could also be seen as a good news for the Blockchain community, allowing people and entrepreneurs to focus only on real business purposes. By the way, the fact that we’re still in the “Bitcoin not Blockchain” trend, is also due to natural causes like the need to adapt existing technologies to the new one whilst Bitcoin being a ready-made application that could already exploit all of its value.
- **The role of cryptocurrencies as a competitor of fiat currencies:** For what concerns the future of cryptocurrencies, they’re here to stay and to let us remember that it could be time

to move from the old conception of paper money towards a new digital representation of this latter.

- The process of cryptocurrency adoption in member states will start with few first comer countries which will substitute their own fiat currency with its crypto-equivalent while maintaining ATM running for the exchange of those latter in other fiat currencies to be used towards fiat-currency based countries. The shift process will be longer with respect to what happened with Euro introduction, but with the same mechanism of retiring fiat-money to issue the crypto-equivalent. I expect those countries to be among the first countries by cashless transactions and digital innovation index, like it could be Sweden or Estonia. Or, to be preceded by hyperinflated countries in which the abandoning of the local worthless fiat-currency could be a booster for cryptocurrency adoption, given that it is well-endowed in technological infrastructure to support such a new economy. There are already interesting tentative of new emerging cryptocurrencies trying to beat fiat currency for its price stability, with the example of Tether being backed 1 by 1 with US.Dollar. For what concerns EU, regulators are prohibiting EU countries to issue their own cryptocurrency, but I think that this behavior will be soon abandoned if cryptocurrencies will become mainstream in some countries, with the clear need for regulators to at least accept this new framework to become legal.
- Consequent to the point above, it will be possible that since there are hundreds of cryptocurrencies issued, we could potentially face a situation in which different cryptocurrencies are accepted in a country as long as one of them reveals to be the best one, and then go for the adoption, or to choose to maintain this corridor of currencies competing with themselves.
- According to level at which Blockchain adoption will be in the future, it could happen that there will be not only competing cryptocurrencies for a whole economy, but for different services offered and for different privacy levels for example. In a phrase “there will co-exist different cryptocurrencies for different use cases related to privacy and utility”.

Coming to the future of traditional financing methods, it becomes clear for example how VC firms will be forced to change investment strategy by being no longer only financiers of start-ups but also

active investors in crypto financing startups. They won't disappear then, they will simply change the level playing field on which the funding mechanism happens. What will probably change forever instead, is not the type of financing used, but the way the same old financing mechanisms are built, with institutional investors (centralized institutions, then) decreasing their share over individual investors funding startups together in crowds.

For what concerns IPO future, they run the risk of being substituted by ICOs, which already accounts for nearly half of the total IPO funding this year and promise to overtake that amount soon. A possible scenario is also that of big multinationals doing their own ICO, in the so called reverse ICO process, and I think we can see something like Facebook or even more probably Amazon launching their own token within the next 2-3 years. What is clear is that future regulation about a practically unregulated environment could be the watershed for ICOs to become mainstream over IPOs too or to be doomed to failure.

For what concern the "bubble theme", I sustain that we have in place a process of creating a new one, and complete scams ICO raising hundreds of millions are, together with people buying "only in crowds" like it happened at the end of 2017 with Bitcoin reaching nearly 20 thousand Dollars, a sufficient proof for it but with the addition that we still don't have an idea of what is the intrinsic value on top of which we're letting this bubble grow. Therefore, we don't even know how big this bubble is and how big it could become. For sure regulators are hiding enough to let it grow, and they will be in part responsible of this latter to eventually burst. Technology speed can't be for sure overtaken by rules, but regulators should try to at least follow such a quick change instead of using the wait-and-see approach. What is worrying in here is how easily regulators let new instruments be used without arguing on the method.

By the way, ICOs are the demonstration that traditional financing mechanisms and financial models have to be at least re-thought to be adapted to this new type of businesses, not just because they passed from being reliable to be useless all of a sudden, but just because the assumptions on which they work are (at least for now) not applicable. What is indeed clear is that the way new emerging business raise money can't magically change the way they're valued, thus, a convergence between valuation models will occur in the next years and Blockchain panorama will start to correlate more with traditional financial markets.