FSUG reflection paper on crypto-assets

Introduction

Blockchain is a new technology which can support a wide range of applications. It is essentially a record of transactions but different from traditional ledger as it enables to create and maintain (in a very secure manner) a distributed ledger (or database) among participants in a network who do not necessarily need to know each other or resort to a centralized third-party to manage the ledger or, more importantly, verify the transactions entered in the ledger.

A blockchain just orders data into "blocks" and then "chains" them together securely. Each transaction is also time-stamped so as to ensure that transactions are added in the right order. In this case the verification comes from the secure links so established between subsequent blocks and the consensus of multiple users, indeed all users have a copy of the entire block chain, so any tampering of the links between block is easily identifiable.

Specifically, blockchain is a protocol/software which handles the recording/verification process of a database also in a decentralized manner, which is very important for digital records that should not be copied or edited freely such as financial transactions and balances. It is indeed virtually impossible (at least for the time being) to modify/tamper the data recorded on a blockchain ledger (namely the link established between subsequent blocks) without leaving a trace and/or being detected by the users of the ledger. From this point of view blockchain ledger is able to create trust.

Blockchains can be classified into two main types:

1) **private permissioned blockchains:** no new regulation or issues exist since there is a centralized or well identified entity that has control over the blockchain (the set of computers that maintain the blockchain);
2) **public permissionless blockchains**: there is no centralized or well identified controlling entity.

Private permissioned blockchains have some advantages compared to more traditional centralized databases like increased security, accountability/transparency for an organisation's records, possible interoperability with other organisations' databases. Also, existing regulation can apply to these blockchains. For any existing company, adopting a private blockchain is akin to changing the software responsible for managing their internal databases/records. The company remains liable to make sure that these records are safe. If that company issues crypto-assets linked to that private blockchain, it also remains liable and all existing regulations apply, depending on the "type" of crypto-asset (see the section dedicated to crypto-assets classification).

Public permissionless blockchains, on the other hand, pose many issues for regulators, given their open source, decentralized nature, and the impossibility to apply liability via the traditional *nearest person* principle. The benefit they could provide is to become the underlying technology and payments infrastructure for a peer-to-peer open source "real" sharing economy of online or offline services with less third parties or intermediaries (the remaining intermediary being the blockchain technology itself, and the network of computers maintaining the blockchain called "miners" and "nodes"). There are also "semi-public" blockchains where a limited number of stakeholders control the blockchain, such as in the case of delegated proof of stake or some form of hierarchy in the mining protocols (examples include DASH or EOS).

Public permissionless blockchains have a feature which can be both an advantage and disadvantage. They cannot be easily stopped or censored and they are virtually tamper-proof, which also means that there is no central authority able to correct possible mistakes, undo a transaction or recover a lost funds or "private keys" (the credentials allowing a user to access his/her crypto-assets). Typically, in public blockchains, falling prey to hackers or losing your private key means the loss of the underlying crypto-assets.

Crypto-assets could be defined as "a digital representation of value that is neither issued by a central bank or public authority, nor necessarily attached to a fiat currency, but is used by natural or legal persons as a means of exchange and can be transferred, stored or traded electronically."[1]

Crypto-assets of public permissionless blockchains serve as the economic incentive for users to maintain the network (maintain a copy of the blockchain and ensuring that the blockchain database is up to date, that transactions are processed). Public blockchains typically require an underlying crypto-asset, the exception being relying on the community to voluntarily maintain the blockchain at their own cost. Private blockchains do not necessarily need crypto-assets since there is typically a centralized entity running the network of computers which maintains the blockchain. However, companies running a private blockchain may issue a crypto-asset if they wish to monetize access to their private blockchain in one way or another.

The **value of some public blockchain crypto-assets** like Bitcoin is mostly speculative and based on offer/demand, and real world use cases such as payment for goods/services (merchants accepting Bitcoin as a means of payment) remain marginal in determining the value. Some would argue that the value of such crypto-assets has a "floor" which is equal to the cost of hardware/electricity of miners and nodes maintaining the blockchain, since once the price falls below such a level, miners/nodes have no more incentive to maintain the blockchain. However, in such an event, it is also highly likely that the blockchain will purely and simply disappear and the value will go to zero, as has happened for many crypto-assets/blockchains in the past[2].

Other crypto-assets, especially "utility tokens", are designed to serve as a "voucher" allowing to purchase a specific decentralized online service. For instance, the blockchain project Sia allows anyone to rent unused space on their hard-drive or purchase space online from other users, creating a decentralized cloud service. "Sia coin", the crypto-asset underpinning the Sia blockchain, serves as the currency to pay and get paid for purchasing/renting space. Thus the value of this crypto-asset is linked to the balance between the willingness to pay (the demand) for decentralized cloud hosting and the willingness to offer unused space (the offer).

ICOs or Initial Coin Offerings are one method of securing funding for emerging crypto-assets projects (private or public). Developers of such projects trade so called "pre-mined" crypto-assets (an initial amount of crypto-assets created at the start of the blockchain) of the new project in exchange for existing crypto-assets such as Bitcoin or Ethereum (two of the largest crypto-assets in market cap at present). The developers can then sell those collected crypto-assets (Bitcoin, Ethereum…) to get funding for the development of their project.

Finally, there are two main methods used to secure a blockchain network:

1) **proof-of-work:** is the initial method devised by the creator of Bitcoin. It is simply a way to "prove" that a "mining" machine/computer has done the calculations necessary (work) to

[1] https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf p. 11.

[2] See a complete list of failed blockchains here: https://deadcoins.com/

have the right to attach a "block" of transactions to the blockchain. This method has been criticized extensively for the tremendous consumption of electricity and hardware;

2) **proof-of-stake**: it relies on individuals "locking" a part of their crypto-assets in a special wallet, and allowing these individuals to "vote" on which block of transactions should be the next one to be attached to the blockchain. If these individuals vote against the majority, their funds are lost (which gives individuals a strong incentive to collectively agree on the next block and "vote" responsibly). This method is still experimental and has only been deployed in a select few blockchain projects. However, it could significantly diminish the electricity consumption of current blockchains and increase the number of transactions allowing blockchains to scale more easily.

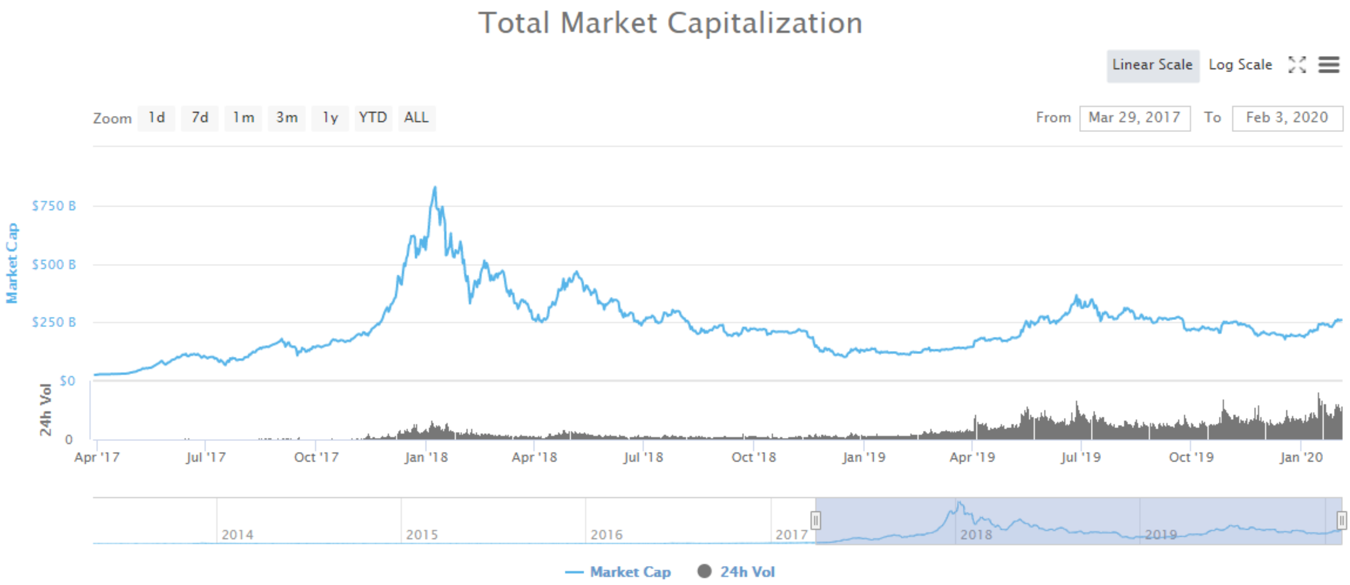
Rationale and scope

The Financial Services Users Group has a mandate limited to the protection of users of **financial services**. Therefore, it is important to determine why the FSUG is examining the use of blockchain and crypto-assets within its remit. While many users have undeniably suffered detriment due to various reasons (see below, the section on the consumer perspective), the FSUG is not necessarily the relevant body to address these, unless crypto-assets and blockchain can fall under the definition of "financial services", financial instruments or financial products.

In this regard, the FSUG takes a broader view, consistent with the EBA and other European institutions. Crypto-assets are used by natural or legal persons as various types of financial services/investments depending on their specifications: either used as an alternative means of payment (Bitcoin, Litecoin, Ethereum, …), a means of payment for a specific decentralized service (utility tokens), or an asset which could be qualified as a financial product (a security). As such, all of them may fall under the scope of existing or forthcoming "financial services" regulation or anyhow their use may be more and more relevant from the point of view of protecting the users of **financial services** and so fall under the remit of the FSUG.

Overview of the current state of the crypto-assets market and use cases

On the 1st of February 2019, the total market cap of crypto-assets sat at around $260 billion, relatively steady since September 2018[3].

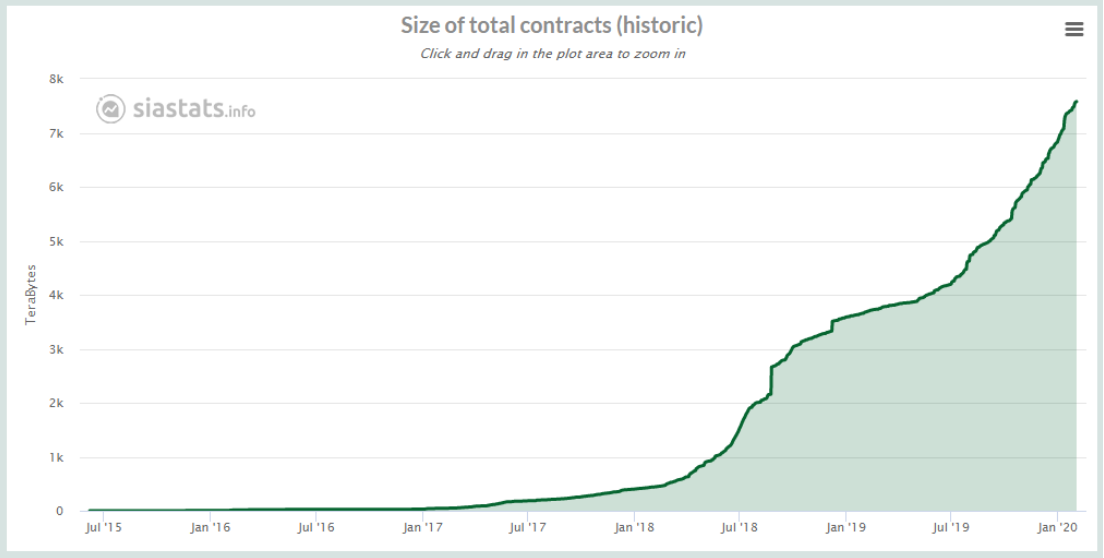


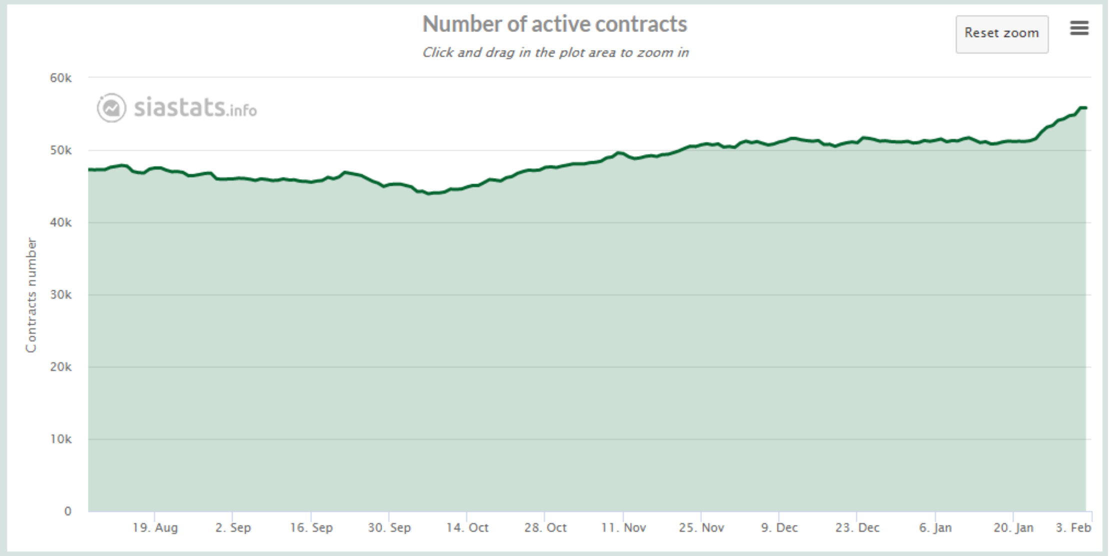
[3] https://coinmarketcap.com/charts/

Besides the total market capitalization, more importantly from the point of view of consumers, is to understand the degree to which this market is based on **speculation** or on **actual use cases.** Two blockchain projects with functioning products will be examined below: Siacoin[4] (a decentralized cloud service) and Steemit[5] (a decentralized blogging/social media platform). In addition, the three main "infrastructure" blockchain projects and decentralized applications use[6] will be examined (Ethereum[7], TRON and EOS).

Siacoin:

This chart shows the total size, in terabytes, of the contracts for decentralized hosting. The growth has been steady since January 2017 and has slowed down somewhat by the end of 2018, but picked up again in 2019. The chart below, looking the number of active contracts since May 2018, shows a stabilization in the number of active contracts, indicating a stable use of the Sia platform for decentralized hosting.





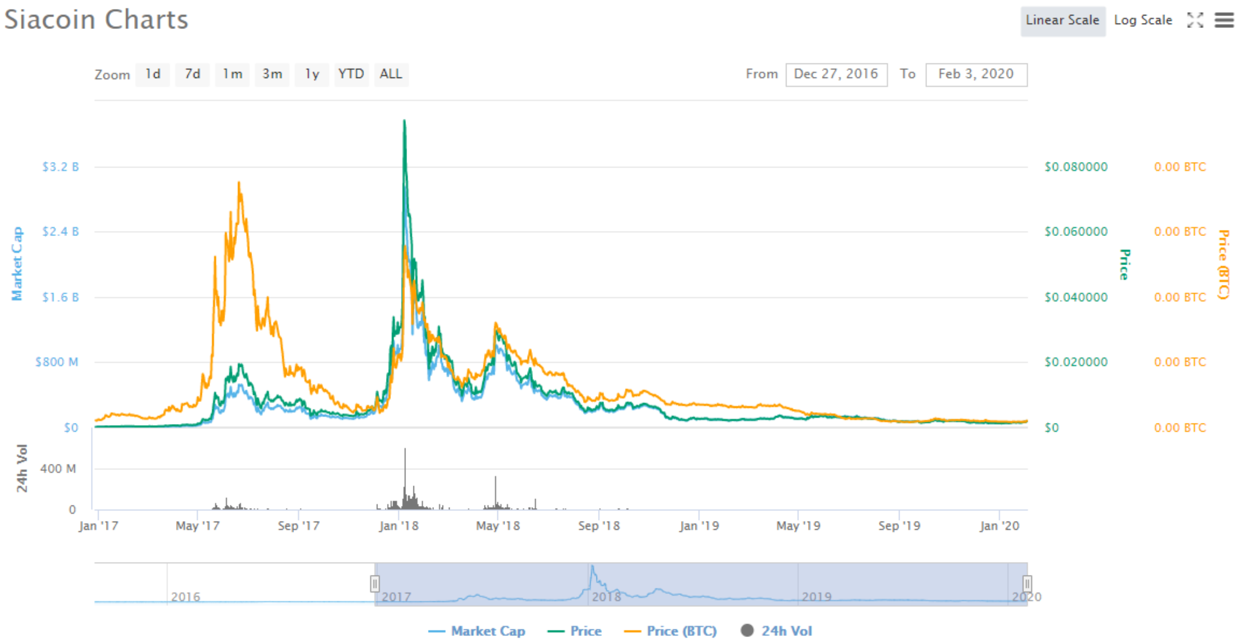
[4] https://siastats.info/contracts

[5] https://steemit.com/statistics/@arcange/steem-statistics-20191015-en

[6] https://dappradar.com/rankings

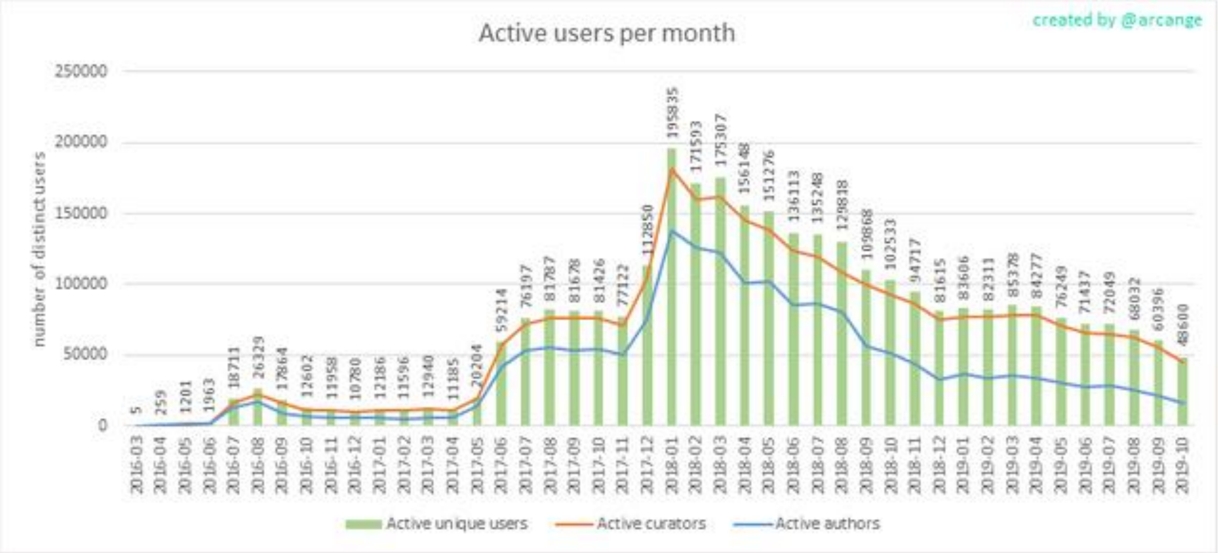
[7] https://dappradar.com/charts
https://etherscan.io/charts

However, looking at the valuation since January 2017, one clearly sees that valuation is disconnected from “real use case” indicators[8]. The value of Siacoin has mostly fluctuated following the global market trends of other crypto-assets (comparing Siacoin with the graph of the total market cap graph from above). The spikes in June 2017, in December 2017 and in April 2018 correspond to those of the total market cap. Furthermore, we see a gradual decline in the price of Sia while the use of the decentralized hosting has stabilized.

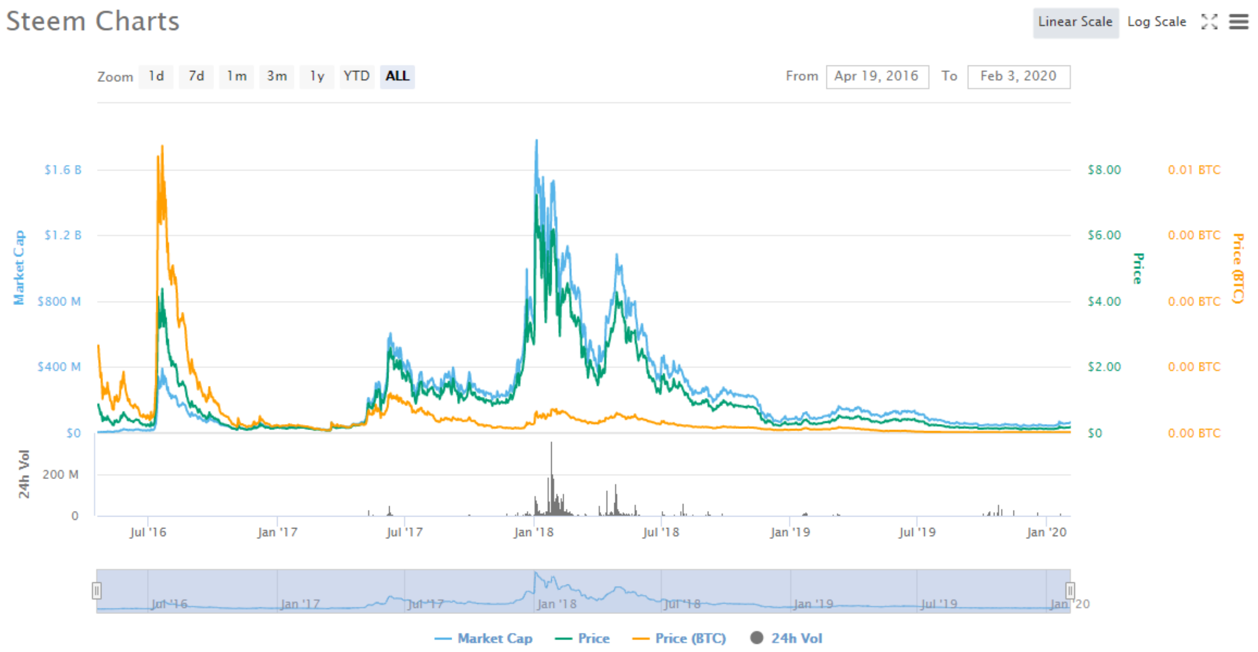


Steemit:

Comparing the chart of daily active users with the value of Steemit, the two charts match up better than that of the Sia platform. The initial “spike” in value of the Steemit token is purely speculative due to the launch of the platform/token, but the user growth does seem correlated with the two spikes in the value of the Steemit token (in May/June 2017 and in December 2017 and January 2018), followed by a steady drop in the number of daily active users as the value of the token fell during 2018-2019.

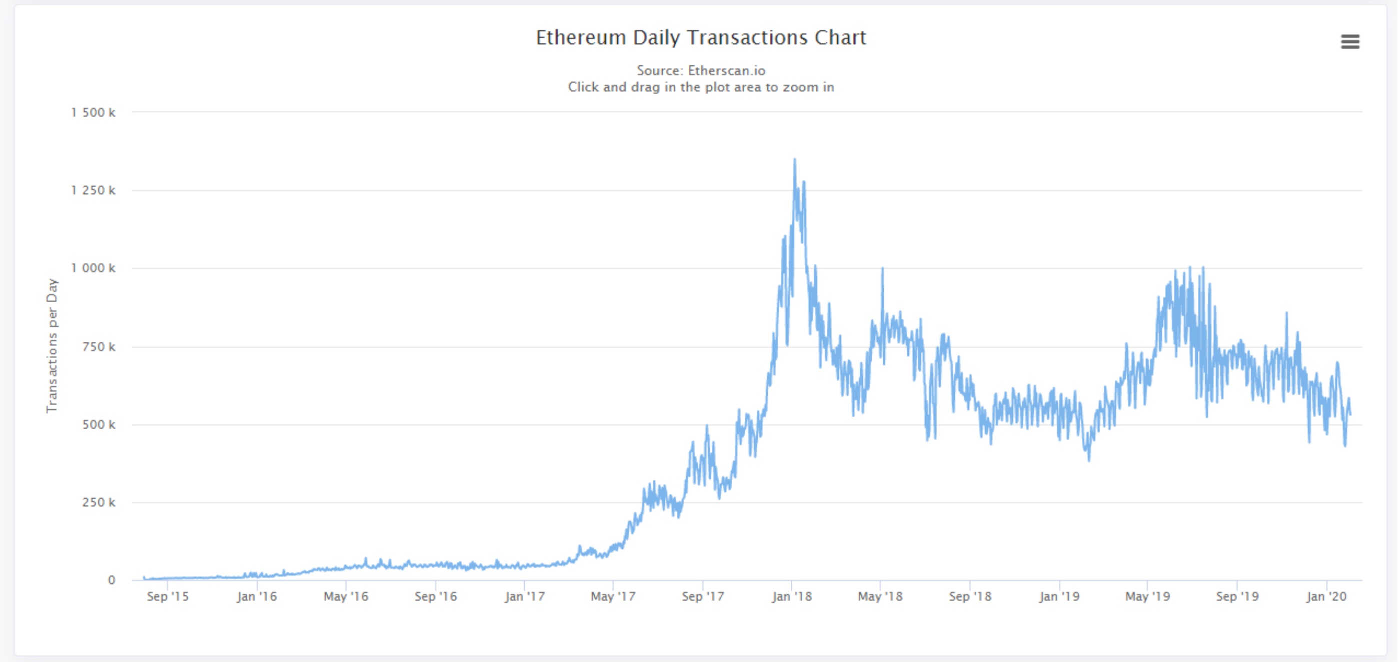


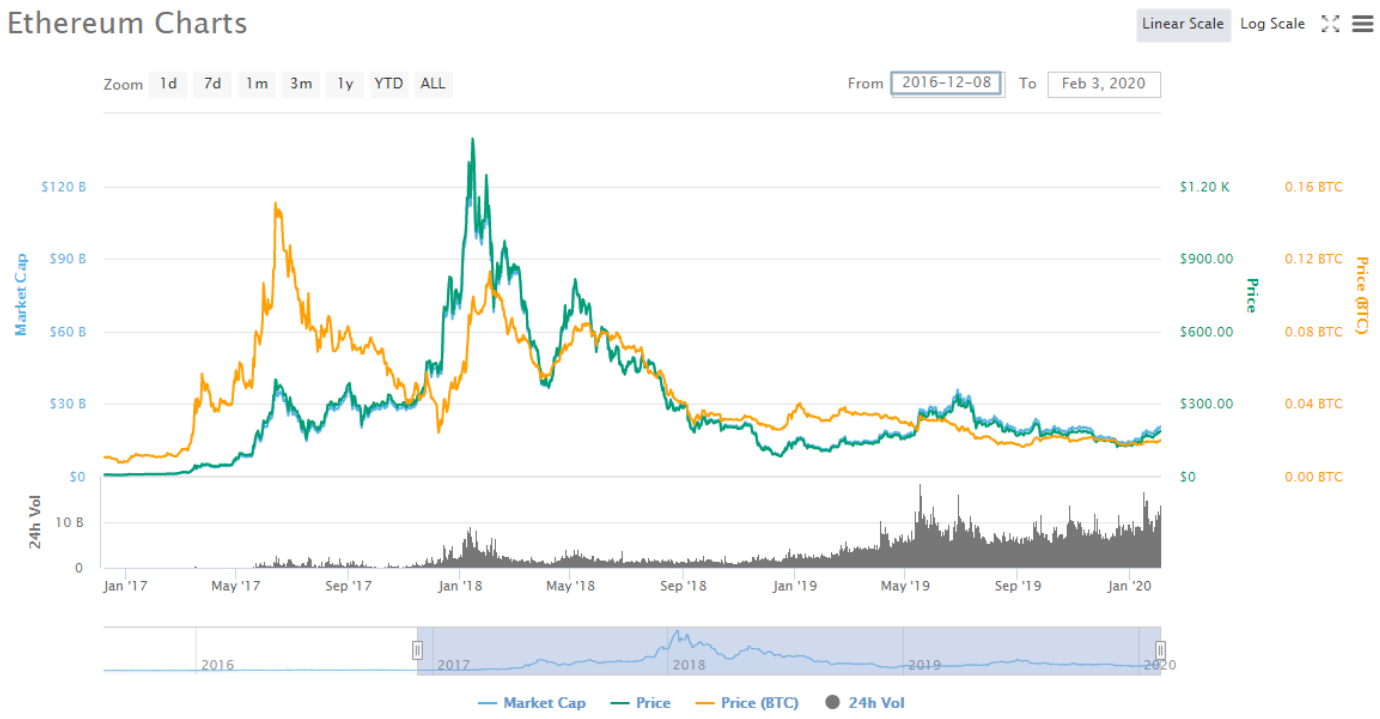
[8] https://coinmarketcap.com/currencies/siacoin/



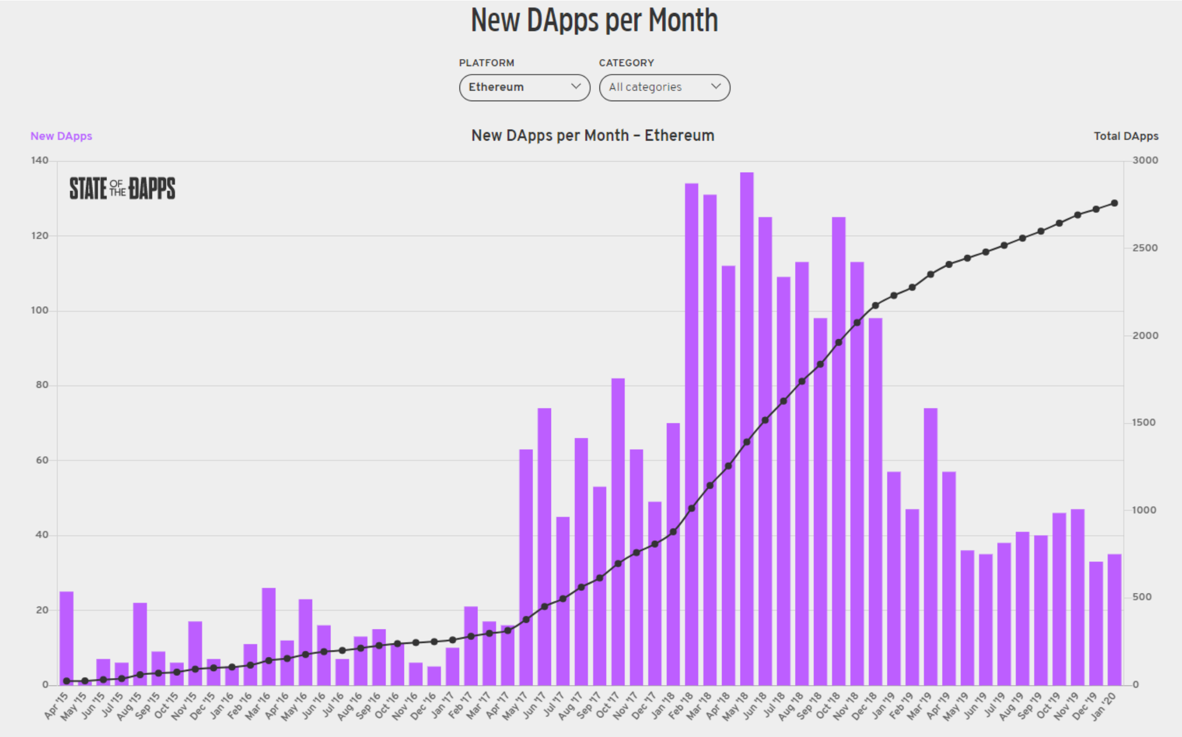
Ethereum:

The Ethereum transaction chart (number of transactions on the Ethereum network) and the value of Ethereum are highly correlated, suggesting that much of the transactions on the Ethereum network are related to buying/selling the token rather than about real use cases. The following charts, looking at the number of decentralized application users (dapps), which is one of the core use cases for Ethereum, confirm this observation.



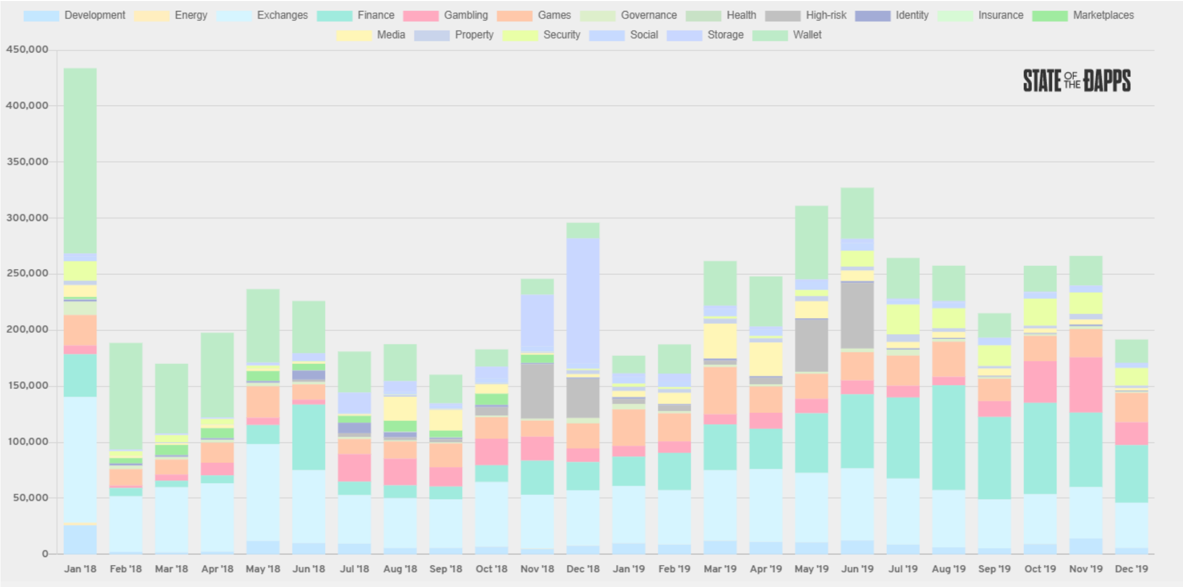


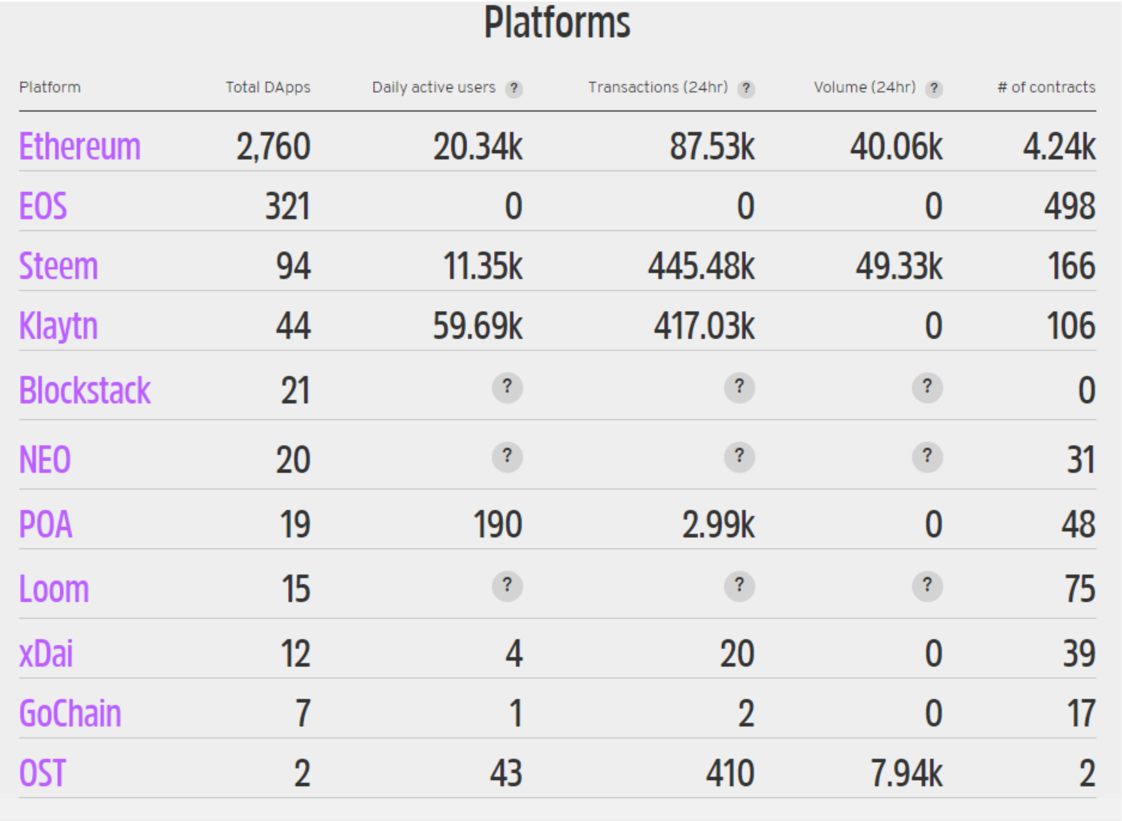
The number of dapps users stays relatively steady all through 2018 and 2019, even if the number of dapps grew[9]. There is little to no correlation with the value of Ethereum, suggesting a strong, albeit niche, dapps users community[10]. However, looking at the type of dapps, the two most used ones are exchanges and finance, which signals, again, use cases focused on speculation/trading, but with a clear diversification throughout 2019.



[9] https://www.stateofthedapps.com/stats

[10] Only about 20.000 daily users while the number of unique Ethereum addresses continues to grow and has currently surpassed 40 million.



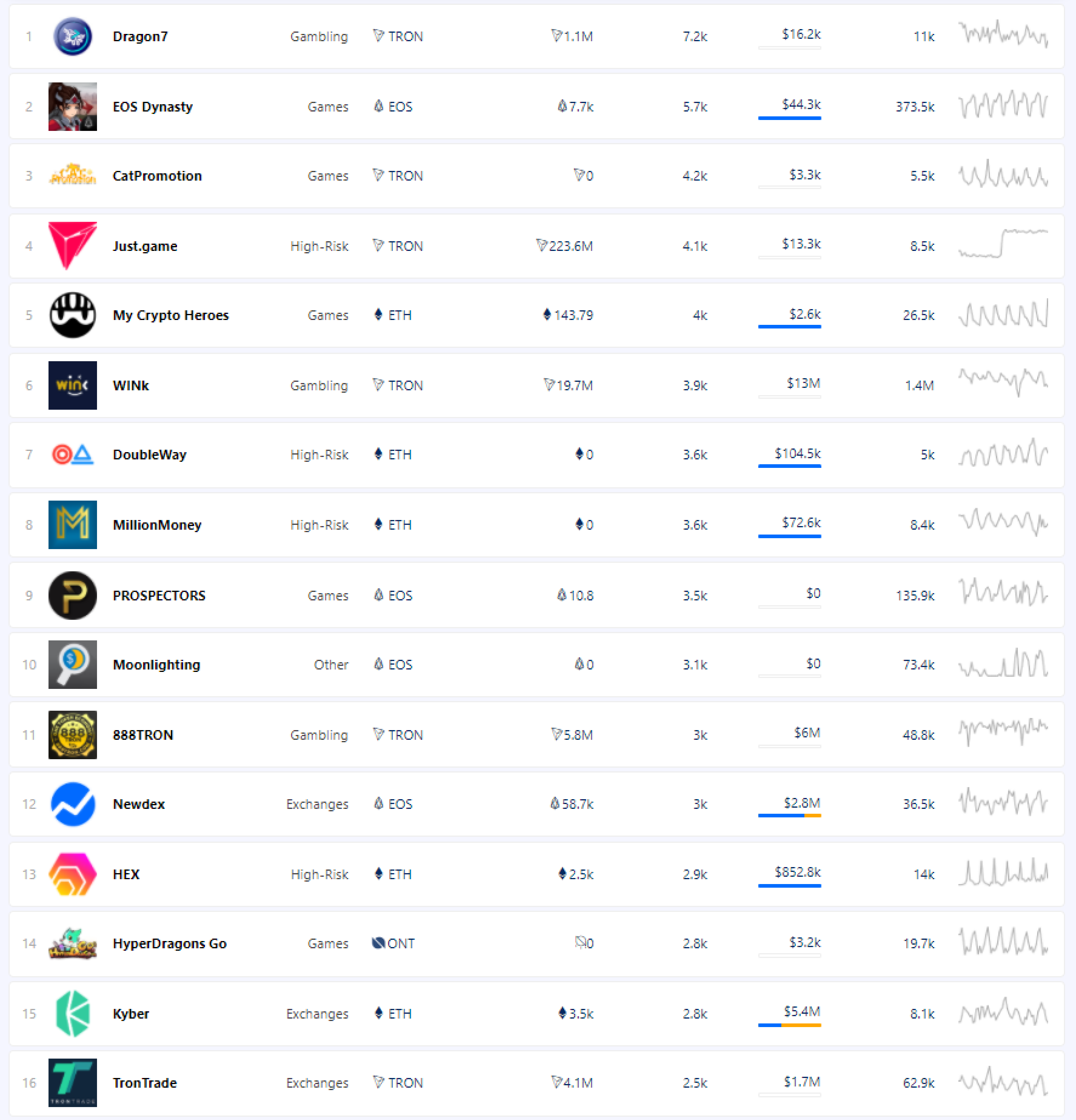


Platforms

Platform	Total DApps	Daily active users ?	Transactions (24hr) ?	Volume (24hr) ?	# of contracts
Ethereum	2,760	20.34k	87.53k	40.06k	4.24k
EOS	321	0	0	0	498
Steem	94	11.35k	445.48k	49.33k	166
Klaytn	44	59.69k	417.03k	0	106
Blockstack	21	?	?	?	0
NEO	20	?	?	?	31
POA	19	190	2.99k	0	48
Loom	15	?	?	?	75
xDai	12	4	20	0	39
GoChain	7	1	2	0	17
OST	2	43	410	7.94k	2

EOS and TRON

From the data available on the DappRadar website, one can see that usage of Dapps (be it volume or daily users) have been on a very slight increase, while the crypto-assets market remained relatively stable in the last year and a half.



1	Dragon7	Gambling	TRON	1.1M	7.2k	$16.2k	11k
2	EOS Dynasty	Games	EOS	7.7k	5.7k	$44.3k	373.5k
3	CatPromotion	Games	TRON	0	4.2k	$3.3k	5.5k
4	Just.game	High-Risk	TRON	223.6M	4.1k	$13.3k	8.5k
5	My Crypto Heroes	Games	ETH	143.79	4k	$2.6k	26.5k
6	WINk	Gambling	TRON	19.7M	3.9k	$13M	1.4M
7	DoubleWay	High-Risk	ETH	0	3.6k	$104.5k	5k
8	MillionMoney	High-Risk	ETH	0	3.6k	$72.6k	8.4k
9	PROSPECTORS	Games	EOS	10.8	3.5k	$0	135.9k
10	Moonlighting	Other	EOS	0	3.1k	$0	73.4k
11	888TRON	Gambling	TRON	5.8M	3k	$6M	48.8k
12	Newdex	Exchanges	EOS	58.7k	3k	$2.8M	36.5k
13	HEX	High-Risk	ETH	2.5k	2.9k	$852.8k	14k
14	HyperDragons Go	Games	ONT	0	2.8k	$3.2k	19.7k
15	Kyber	Exchanges	ETH	3.5k	2.8k	$5.4M	8.1k
16	TronTrade	Exchanges	TRON	4.1M	2.5k	$1.7M	62.9k

Conclusion:

So far, while the decentralized services of these projects are operational, the valuation has been mostly driven by trading following market trends (speculative investment) rather than demand for the service by the users themselves. in the examples above, while the usage of Sia has increased, this has not translated into a higher valuation of the Sia crypto-asset. Only Steemit seems correlated with usage, showing a stable decline in users mirrored by the price of the underlying cryptoasset.

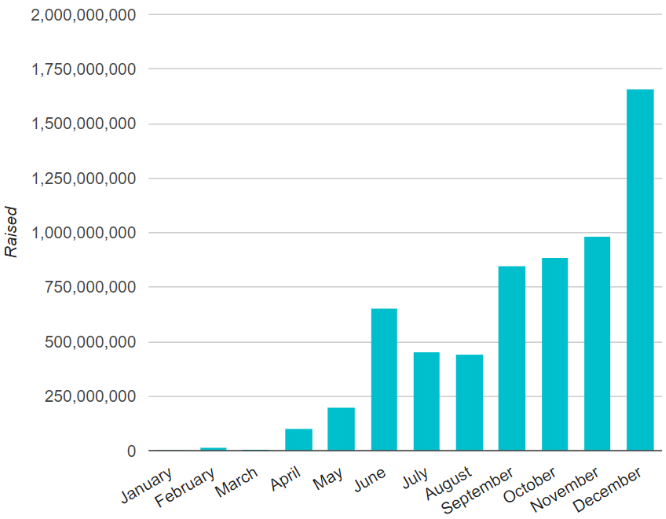
Overall, it is clear that the crypto-assets market is extremely young and that it will take time for its value to be correlated mostly with demand for the services/use cases of the underlying blockchain project rather than on speculative trading/investing.

Overview of the initial coin offerings (ICOs) market

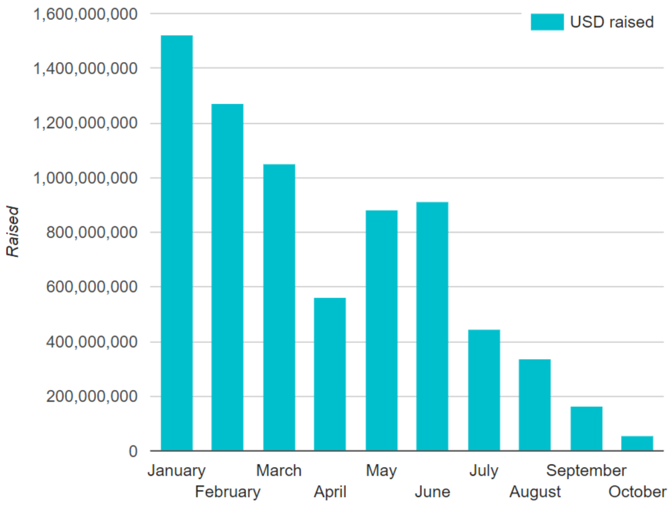
While the media and regulators focused, in the past year, on ICOs as a major risk for consumers, it seems that the "hype" has subsided, due to the state of the crypto-assets market in general, ICO "fatigue" (most innovative ideas for decentralized services running via a blockchain and requiring an ICO have already been exploited) and also due to user experience and data availability on how ICOs performed (nearly 80% of ICOs being scams, and at least half of the rest ending up failing)[11].

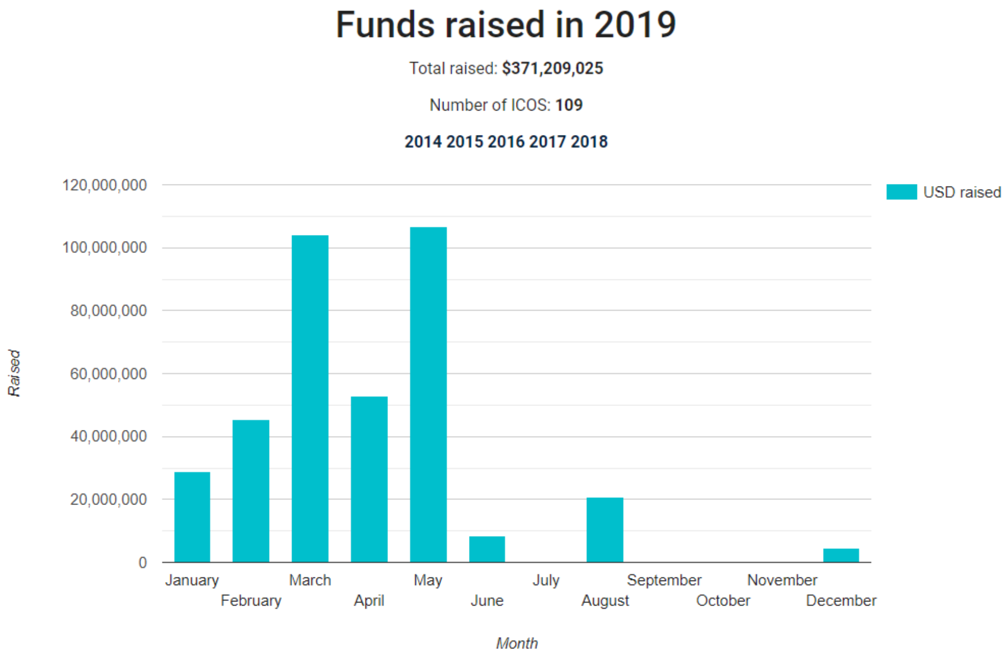
This slowdown is clearly evident from data on the funds collected by ICOs in the past three years[12], especially during 2019 where the total funds raised by ICOs went from $7.1 billion in 2018 to less than $400 million in 2019:

2017: $6,2 billion raised in total



2018: $7,1 billion raised in total





Funds raised in 2019

Total raised: **$371,209,025**

Number of ICOS: **109**

2014 2015 2016 2017 2018

[11] https://www.esma.europa.eu/document/smsg-advice-own-initiative-report-initial-coin-offerings-and-crypto-assets p. 7.

[12] https://www.icodata.io/stats/2018

Crypto-assets classification

As already briefly discussed in the introduction, not all crypto-assets of public blockchains serve the same purpose. While nearly all crypto-assets in public blockchains are created, originally, as an incentive mechanism for miners to maintain the public blockchain network, their use is extremely varied, which leads to an impossibility to impose a "one size fits all" regulatory approach.

There have been many attempts at classifying crypto-assets, an overview of which can be found in the paper from the cryptocompare platform[13], however there is not yet a common view about the most appropriate criteria to be used for their regulatory classification. For simplicity's sake, the broad classification made by the Swiss FINMA will be used in this paper. It divides crypto-assets into **three main categories depending on their function: payments, utility and security/asset.**

- The **"payment"** category includes projects like Bitcoin, Litecoin, Monero, Zcash, Dash (on the public or semi-public[14] blockchain side) and Ripple (on the private blockchain side). Payments are understood in a wider context, which includes not only payment for goods and services, but also for transferring funds. Ultimately, there are only a few characteristics which differentiate these projects such as: the transaction speed, the cost of transactions, the method the blockchain uses to maintain itself (proof-of-work, proof-of-stake…), privacy and transparency of the blockchain and governance rules.

  At this stage, any and all of these projects are still in their development and their value is fuelled mostly by speculation rather than "real world" use cases. Their long term value will depend on which payments/fund transfer project will become the most used and accepted for payments both online and in the real world. This depends greatly on regulatory developments and take up of one or more projects by consumers/merchants.

- The **"utility"** category is one of the broadest. Utility tokens can be seen as "vouchers" which users can redeem for some form of decentralized service. They are also akin to virtual currencies in multiplayer online video games such as World of Warcraft or Pokemon Go, which can only be used within the online game (online service).

  Some utility tokens are limited to a specific service such as Siacoin or Steem "dollars" in the examples above. Siacoin enables users to pay for decentralized cloud hosting or for hosters to be remunerated for sharing their hard drive capacity, while Steemit allows for users to post content on the decentralized blogging platform and get remunerated for their contribution depending on the audience's votes.

  Other utility tokens like Ethereum have a more "universal" use case, and can be used to pay for the execution of any type of code on the Ethereum "world computer". This can include the examples above. Any developer can, for instance, code a decentralized hosting or a decentralized blogging platform on top of Ethereum and use Ether tokens to pay for the execution of the various features of the platform (posting content, uploading content etc).

- The **"assets"** category relates to claims of ownership of certain physical goods, claims of ownership of a company, or promise of future cash flows or profits from a blockchain project.

[13] https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf

[14] Besides public and private blockchains, there are "hybrid" ones where there are certain restrictions on participating in the blockchain even though it is public. For instance, governance rules which gives some "nodes" more power than others over the network (see the Dash "master node" concept).

These are most similar to existing financial instruments such as equities, shares, bonds, futures, options etc and as such, can be covered by existing regulation.

- Finally, the classification recognizes that there are **"hybrid"** crypto-assets which may fit into two or more of these categories. For instance, while Ethereum is a utility token, it has also been used as a means of payment. Some crypto-assets provide some form of governance rights over a blockchain project, similar to shareholder's voting rights.

Other classification rationales include sorting crypto-assets according to the economic properties of crypto-assets and which "industrial activity" they focus on: financial services; professional/scientific and technical activities; transportation and storage; arts, entertainment and recreation; information and communication etc.

One important dimension to add to classifying crypto-assets for regulatory purposes, and which in our opinion has been overlooked by all classification attempts so far, is to **examine whether a blockchain project is entirely self-sufficient in a closed-circuit, online environment, or whether it depends on or entails also offline interactions.**

This is absolutely crucial in determining the **risk for consumers**. A project which is self-contained in an online environment and does not depend on the "physical" world can be developed much faster and is less exposed to regulatory arbitrage and other risks inherent to the offline world. Such a distinction is also useful in determining the **enforceability of any regulatory measure** (as we will discuss when putting forward policy reflections). Concrete examples include the following:

- **Blockchain projects with a 100% online ecosystem**: Siacoin (decentralized cloud), Golem (decentralized computing), Musicoin (decentralized music platform) and Steemit (decentralized blogging/social media). These projects are entirely online and do not depend on any "offline" interactions or effects. Thus they can be self-sufficient and can quickly operationalize their blockchain project since they do not need for any authorization from a regulatory body to produce effects in the "offline" world.
- **Hybrid blockchain projects with mixed online/offline ecosystems**: Ethereum, EOS, Stellar Lumens, Bitcoin, Litecoin… Most blockchain projects are hybrid. They include both online only and offline interactions. To take a simple example, Bitcoin can be used to pay for virtual goods online, such as buying purely digital services like online music or images (100% online), buy physical goods/services via a decentralized peer-to-peer store (OpenBazaar, mixed online/offline), buy physical goods/services from regular, "centralized" merchants (buying a cup of coffee, a pizza or any other good, 100% offline). The latter is much more subject to the regulatory environment and the willingness of merchants to include such a payment option.
- **Blockchain projects dependent 100% on offline effects**: decentralized sovereign identity (DID), decentralized land registry, any crypto-assets which require interactions in the offline world (decentralized car sharing, flat sharing, smart contracts which affect real world assets, etc). All of these projects are much riskier since even if the "software/hardware" parts are stable and complete (an operational blockchain software running on a sufficient number of machines/miners), there is no guarantee that it will deliver the promised effects. For instance, any project aiming at decentralizing identification or land registry requires the cooperation of public authorities in order to ensure that their projects are recognized and validated inside their legal systems and produce real-world effects. These projects are therefore much more exposed to **regulatory arbitrage** since decisions from public authorities can directly affect their success/failure.

Risks from the consumer perspective

The EBA, in its 2014 opinion, listed a comprehensive overview of the different risks faced by consumers[15]. Overall, there are four main risks of engaging in crypto-assets:

- Falling prey to scams (either fake ICOs or fake exchange platforms offering a sale of crypto-assets);
- Lose a part or all of the value invested in crypto-assets[16];
- Have their crypto-assets stolen or lose their credentials (private key) which amounts to loosing the underlying crypto-assets;
- Engage (knowingly or unknowingly) in illegal blockchain projects or projects outside of the scope of current regulation[17], leaving consumers in a legal void and uncertainty (without any form of protection, and uncertain about the future legality of the projects they have engaged in).

Reflections on regulatory responses:

The reflections put forth will be based on a pragmatic approach stemming from the nature/classification of the various crypto-assets and especially, examining the **enforceability in practice** of any regulatory measure, in order to assist policy makers in developing regulation with strong consumer protection.

Liability

Before engaging in any regulatory initiative, public authorities must clarify where liability lies when it comes to public blockchains and how they intend to enforce the identified liability. For instance, the interplay between developers and miners in the public blockchain space makes it very difficult to pinpoint liability, since developers require the cooperation of miners to update any problematic code in a public blockchain to make it compliant with regulatory rules, and given that miners operate from all over the world, it is unlikely that they will agree to implement a regulatory requirement from one specific jurisdiction (like the EU) if it goes against their interests or threatens their revenue and investment in one way or another. The same applies to miners who are dependent on a more or less easily identifiable team of developers to adopt changes in the mining protocol.

Public authorities also need to clarify which regulatory regime applies when consumers are victims of scams or other fraudulent behavior. Such issues may fall under private/criminal law, as they involve relationships between individuals, since most public blockchains and the stakeholders involved in maintaining them (developers, miners), are not registered as a private business or corporation.

[15] https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf

[16] This can happen for a number of reasons including scams, developers leaving the project, a decision by the community/developers to initiate a fork or change the rules of the project leading for instance to a dilution of the crypto-asset, a critical bug leading to a hack of the project, a programming mistake which lead to the loss (of value or access) of the crypto-assets, or a failure of the take-up/adoption of the project by the wider public, regardless of the good faith of the developers behind the project.

[17] For instance, it is unclear how certain regulations will apply to blockchain, such as the GDPR, or KYC and AML requirements (which already apply to public exchanges), terrorist financing, copyright, etc. To give a concrete example, a decentralized social network powered by blockchain where there are no mechanisms for taking down content, can become illegal should some of its members upload illegal content: terrorism propaganda, child abuse material, hate speech, copyrighted material.

Reflections on self-regulation and co-regulation

For blockchain projects which operate in a 100% online self-sufficient ecosystem which depend very little on interfacing with the existing financial infrastructure, public authorities should consider combining self-regulation and co-regulation strategies which would arguably be more effective than regulation. Given the technical specifications and governance structures of fully decentralized blockchain projects, it would be hard if not impossible to implement/enforce regulatory measures given the global nature of these projects. Engaging in a discussion and dialogue with these projects to enable them to provide tailor made solutions to problems that the regulators flag might therefore be more effective and future proof, as it involves a continuous exchange and dialogue with these projects, than a regulatory approach.

It is important to underline previous attempts by policy makers at regulating similar online services. The clearest example is the case of **Napster and other peer-to-peer file sharing solutions.** Such services can be thought of as the "premise" of Blockchain technology, since their principle (peer-to-peer, decentralized) has been a source of inspiration for creating a similar system for decentralized, peer-to-peer "money" (the initial aim of Bitcoin, according to Satoshi Nakamoto's original white paper).

Public authorities successfully managed to close down Napster, given that the project's developer was known. However, this short term success was followed by the emergence of other similar software, where the developers remained anonymous, much of which are still existing today (the most prominent one being the Torrent network). Eventually, following a nearly two decade long fruitless battle, the music/film industry gave in and adapted their business models from selling individual music/film to setting up platforms which operated on the basis of monthly subscription fees (Spotify, Netflix, Deezer…) emulating some of the features of P2P file sharing platforms! One of the latest examples of regulatory failures was the French "Hadopi" law which was meant to penalize Internet users for illegal downloads based on a "three strike" approach. Only a limited number of cases of piracy were brought to justice[18] and users found many ways to circumvent the law by using Tor, VPNs, switching to streaming services, direct download platforms etc.

Thus the most effective way to curb piracy was to adapt the business model to consumer demand and new consumption trends (ease of access, convenience, instant availability, adapted pricing etc) rather than adopting a harsh regulatory approach and trying to "force" consumers to conform to outdated business models (buy music and films on physical support in physical shops).

With regards to blockchain projects, most of them already include a form of **self-regulatory mechanism** depending on the governance structure of the project itself. Looking at the Bitcoin network, for example, after the initial creator of Bitcoin ended his participation, a self-organized online community emerged comprised of volunteer developers on the one side, and "miners" and users on the other. This governance structure has been subject to a lot of criticism, especially for the preponderant weight that certain actors have in influencing the development, update and implementation of the Bitcoin's underlying software. One such figure is Jihan Wu, who is a co-founder of Bitmain (a special "mining" computer known as an ASIC) and head of a large Bitcoin mining pool[19], leading to complaints that the interests of "miners" (and their profits) came at the expense of the interests of users (for instance, using Bitcoin for payments rather than a speculative store of value). Disagreements between volunteer developers and miners/users has already lead to "forks" in the

[18] https://www.lemonde.fr/les-decodeurs/article/2018/08/14/hadopi-beaucoup-d-avertissements-mais-peu-de-condamnations_5342325_4355770.html
[19] https://itnext.io/governance-in-blockchain-part-i-the-bitcoin-experiment-a8c633791e6d

Bitcoin protocol, a situation where a part of the users/miners decide to adopt a different version of the software and thus create a separate ledger based on the Bitcoin one. In the event of a “fork”, any Bitcoin user now has an equivalent amount of “Bitcoins” in both ledgers. This is exactly what happened as Bitcoin split between Bitcoin “Core” (what most people agree is the “main” ledger) and Bitcoin “Cash” (an updated version of Bitcoin which addresses issues of scalability and transaction fees).

Public authorities could thus focus on **defining a set of characteristics, features and criteria for the governance structure of public permissionless blockchains in order to minimize the risks of power imbalances, collusion or monopolization/oligopolisation between the various stakeholders involved.**

Major blockchain stakeholders from the industry side have already started to issue their own voluntary codes of conduct (See the code of conduct of GDF – Global Digital Finance). These need to be examined carefully to ensure that consumers are adequately protected and monitor their implementation/enforcement[20].

The “incentive” that public authorities could provide to encourage public permissionless blockchains to comply with these rules is to **grant them Legal Personality as “Technological Arrangements”[21].**

This solution was proposed in the consultation document of the Maltese Parliamentary Secretariat for Financial Services, Digital Economy and Innovation of the Office of the Prime Minister[22] and is linked directly with the difficulty to enforce any kind of regulation on public permissionless blockchains.

Some examples of required features to qualify for this status include:

- Offering guarantees or insurance schemes that could cover possible damage claims (for instance, developing an internal insurance scheme in case of loss of crypto-assets within the core protocol of the blockchain and with a mechanism for releasing such funds)
- A governance structure which clarifies the powers, roles and responsibilities of each stakeholder in the development, update and implementation of the blockchain (users, developers, miners, nodes…)
- Leveraging the potential of multi-signature schemes and smart contracts, whereby public authorities would be granted special “powers” over a blockchain by holding a series of private “keys” which would be required to activate/deactivate certain features of the blockchain (for instance, release compensation funds, access certain encrypted information etc).

A practical example of using governance structures, multiple key signatures and smart contracts is in protecting consumers from fraud and failure of ICOs. One of Ethereum’s core developers, Vitalik Buterin, introduced the concept of DAICOs (Decentralized Autonomous ICOs)[23], allowing any contributor to an ICO to “vote” on the gradual release of the collected funds depending on the progress of the project. The funds are therefore “locked” and inaccessible to the initiators of the ICO and contributors decide when and at which pace the funds are released. Contributors further have the possibility to terminate the fund and be reimbursed (of all the funds or whatever is left over)

[20] https://www.gdf.io/gdfcode/

[21] https://chainstrategies.files.wordpress.com/2018/05/rtdf2018_1_doctrine_tendon_ganado_tap.pdf

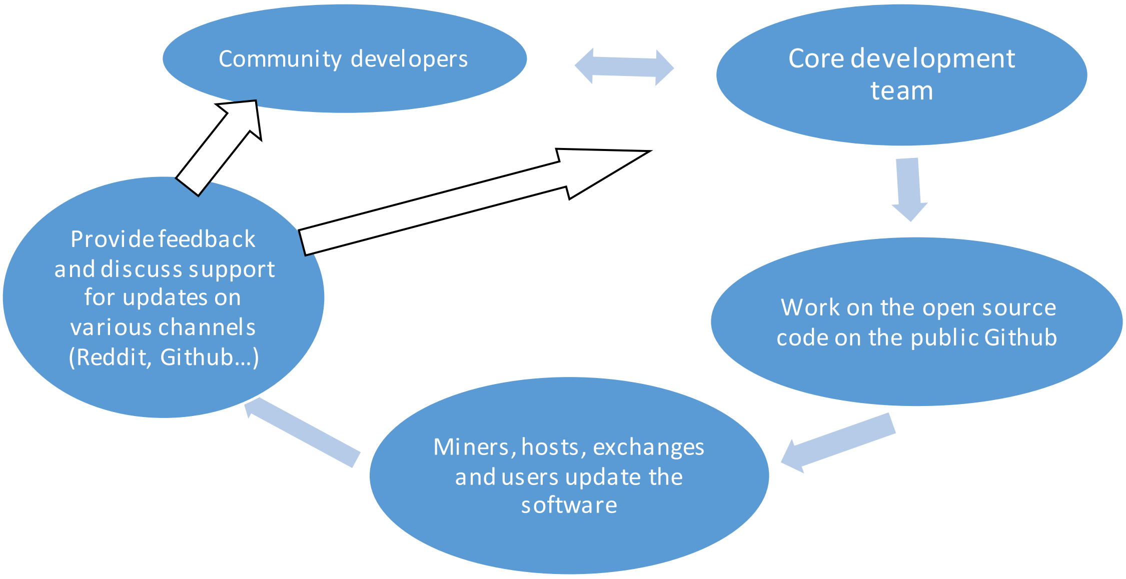
[22] https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF

[23] https://ethresear.ch/t/explanation-of-daicos/465

should the project turn out to be a scam or fail. This new form of ICO has been presented in January 2018 but has not yet been put into practice. In this regard, public authorities could prove instrumental in encouraging the testing and development of this solution by the Ethereum developers and wider community.

Addressing the internal governance of public permissionless blockchains could thus arguably be the most realistic option to reach a certain degree of consumer protection. It is recommended that public authorities and policy makers meet with the most active/influential individuals inside the governance structure of public blockchain projects in order to openly discuss issues such as consumer protection and the best way to remedy them.

Example of a public permissionless blockchain governance structure: Siacoin



Community developers
Core development team
Provide feedback and discuss support for updates on various channels (Reddit, Github...)
Work on the open source code on the public Github
Miners, hosts, exchanges and users update the software

Mandatory information to consumers

For public permissionless blockchains, given the difficulty to pinpoint liability, clear and understandable consumer information are a major challenge. As opposed to the "traditional" online services that consumers are more or less used to, public permissionless blockchains offer none or little remedy for common problems such as loss of a user password (a private key).

Several recommendations can be considered in this regard:

- Mandatory information to be presented on any "official" website of a public permissionless blockchain project, including information about the intended governance structure, description of remedy schemes (insurance, guarantees) in case of a problem, disclosure of all risks consumers face and which cannot be remedied given the nature of the project (impossibility to recover lost private keys, risks of exploitation of vulnerabilities in the code of the blockchain etc).
- Websites of ICOs should provide information about the control (or lack of control) contributors have over the funds raised by the ICO, and provide regular updates about project developments, including transparent disclosure of allocation of the funds.

More broadly, public authorities and consumer organizations could carry out information campaigns in order for consumers to better understand blockchain technology and crypto-assets. The main message conveyed to consumers should be to **only purchase crypto-assets which they intend to use, immediately or in the foreseeable future.** Investing in crypto-assets solely for the purpose of financial gain is extremely risky. Moreover, such a strategy can be directly responsible for the project's failure in the first place.

Drawing on a comparison which is understandable for consumers, buying a crypto-asset for a public blockchain that a consumer does not intend to use with the hope of selling it at a higher price, is akin to investing in a crowdfunding for a multiplayer online game where the investor receives virtual currency which may be used in the future inside the game (to purchase in game items, etc). The value of such a virtual currency will be directly linked to the success of the online game. If none of the investors intend to play it and simply keep the virtual currency for resale to a "potential" future player, their strategy might be directly responsible for the project's failure. The "wisdom" that generally applies to crowdfunding online should also apply for ICOs and crypto-assets: **do not invest in a multiplayer online video game that you do not intend to play or in other words do not invest in a crypto-asset that you do not intend to use.**

Gradually, consumers' ability to assess the value of a blockchain project should increase as the technology becomes more ubiquitous. For instance, no consumer would estimate the value of an online multiplayer game to be worth $4 billion in initial development costs[24].

Point of entry

Regulation has already been successfully applied to most centralized exchanges, especially compliance with existing AML/KYC requirements. However, this approach also has its limits. While centralized exchanges remain, so far, the most prevalent way to convert fiat to crypto-assets, there are many alternative points of entry which cannot be as easily regulated:

- **Decentralized exchanges**: these exchanges will simply consist of a piece of code running on a decentralized blockchain (such as Ethereum) and matches up buyers and sellers of crypto-assets, making the "trade" as soon as a certain number of conditions are met (a smart contract executing the trade once the buyer and seller have transferred the agreed amount of crypto-assets to a specified account). This means that regulators will not be able to ban any single crypto-asset since once a consumer successfully purchased one crypto-asset (for instance, Bitcoin), he/she will be able to easily convert it into any other crypto-asset provided that there is a market for it via decentralized exchanges.
- **Peer-to-peer direct transfer or cash payments**: alternative services to centralized exchanges are already available and facilitate a peer-to-peer trading system, for instance via SEPA transfers to a select account in exchange for Bitcoins, or even cash purchases[25].
- **Earning crypto-assets via mining or alternative means**: users also have the choice to engage in mining in order to obtain crypto-assets or participating in a blockchain ecosystem which provides them with revenue in the form of crypto-assets. These are becoming more and more prevalent. Examples include: earning BAT (Basic Attention Tokens) via the Brave browser[26], obtain crypto-assets by including a script on a personal website which takes control of the visitor's processor, obtaining crypto-assets by engaging in an online sharing economy type service (such as Siacoin, mentioned above), obtain crypto-assets by selling

[24] Such was the case for EOS, the ICO which raised a record $4 billion in crypto-assets.

[25] https://localbitcoins.com

[26] https://basicattentiontoken.org/

digital goods like music or art[27], or by participating in select decentralized social networks with a reward scheme (such as Steemit), selling a physical good/service against crypto-assets (notably via peer-to-peer decentralized stores such as Open Bazaar)[28].

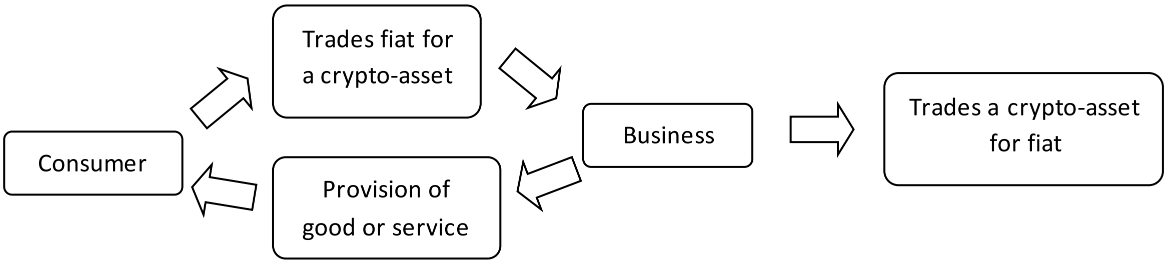
Mining

Regulation could address two core issues related to mining: the ecological footprint and the threat of centralization:

- Ecological footprint: the power consumption of proof-of-work blockchain networks has been mushrooming at an alarming pace. But this boom has been greatly exacerbated by **mining farms**; giant warehouses containing thousands of "mining" hardware, making a business out of mining. Policy makers should greatly discourage the emergence of mining farms, either via taxation or other regulatory restrictions (for instance, applying strong taxation for owning and operating a certain number of mining devices or going over a certain threshold in terms of energy consumption). Furthermore, policy makers should regulate mining hardware by obliging hardware manufacturers to embed heat recovery systems into their hardware (for instance, using the heat generated by the mining hardware for heating homes or other buildings).
- Threat of centralization: mining farms and mining pools are a growing concern as they threaten the security of public permissionless blockchains and create distortions in terms of governance (as explained above). Discouraging the emergence of mining farms and encouraging more distributed, decentralized mining is thus not only an ecological issue but also a security and governance issue.

”Payments” crypto-assets

Public authorities should clarify the difference between using crypto-assets as a means of payment and as an (speculative form of) investment in order to clarify whether they should be exempt of taxation. Regulation should specifically address the maximum duration for holding a crypto-asset meant for payments before it is considered an investment.


Trades fiat for a crypto-asset
Consumer
Business
Trades a crypto-asset for fiat
Provision of good or service

The liability and risks of using crypto-assets as payments in the case of relatively quick "in and out" schemes should be limited. For instance, in the diagram above, if a consumer only buys a crypto-asset prior to paying for a good/service and the business immediately converts this crypto-asset into fiat, there is nearly no risk in such a transaction. In Europe, thanks to the SEPA payments area in the Eurozone, there is little need for using crypto-assets as payments. However, for international payments, peer-to-peer international trade or remittances, crypto-assets remain an interesting alternative to bank wire transfer or using services like Western Union.

[27] See Artbyte or Musicoin

[28] https://openbazaar.org/

On the regulatory side, transactions and holding of clients' money has to be regulated under the Payment Services Directive. The ESAs have also issued a warning in using crypto-assets, which includes a broad overview of the risks that consumers entail[29].

”Utility token” crypto-assets

In the case of "utility token" crypto-assets, if they are granted on the basis of an ICO, regulation could be similar to that applying to **crowdfunding.** The FSUG therefore supports the further assessment of how regulation can be applied to this new phenomenom[30].

Utility tokens which are solely used to pay for online services in a closed ecosystem will essentially enable a **decentralized real "sharing economy" of online services.** Further regulation should focus, as already discussed, on the governance rules of the project. In many utility token blockchain projects, the barrier between "user" and "provider" is blurred. For instance, in the case of Sia, a person can rent decentralized storage while at the same time lending unused space on his own hard drive. While there is a core developer team, voluntary developers also contribute to updating the software and users/providers always have a choice in adopting the updated version of the software. The Sia "protocol" becomes the only intermediary between users/providers and thus pinpointing liability is extremely tricky. The continued success of the project rests arguably with **the community as a whole** which is why strong and sound governance rules is the most important feature to protect every participant in the project.

Crypto-assets as "securities"

For crypto-assets which operate in a similar manner to existing financial instruments such as shares, bonds, equities etc, the FSUG supports the suggestions put forth by the ESMA Securities and Markets Stakeholder Group (SMSG)[31], namely, **applying the MiFID regulation**.

An exception has to be made, however, for projects which are 100% online and include a profit sharing scheme or other scheme with features similar to a "security" paid out in the form of a crypto-asset. In that case, applying the existing regulation will prove extremely difficult (enforceability will be nearly impossible).

For projects which cover existing physical assets (tokenization of physical goods, commodities and other assets) or existing financial products (shares of a company sold as a crypto-asset), enforcement of MiFID will be less of a problem.

Legal certainty and regulatory arbitrage

While risks for consumers mostly focus on risks derived from the technology itself, there are also risks stemming from legal uncertainty and regulatory arbitrage (distortions in the market created by regulation or other decisions by public authorities like the support of one blockchain project against another). In this sense, the FSUG supports the positions of both the EBA and the ESMA SMSG in calling for a **common European position on the regulatory response to public permissionless blockchains and their underlying crypto-assets** rather than patchwork national regulatory responses.

[29] https://eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf

[30] https://www.lexology.com/library/detail.aspx?g=9bb042eb-51f7-40c1-9401-161f1926c57e

[31] https://www.esma.europa.eu/document/smsg-advice-own-initiative-report-initial-coin-offerings-and-crypto-assets p. 14-16.

Hardware

Hardware products interfacing with public decentralized blockchains are growing in number. The latest trend is for smartphones to include hardware wallets and running dapps (decentralized applications)[32]. This is a welcome trend which could make it easier for consumers to engage in the crypto-asset space, but also brings with it new risks such as hacking, theft and overall loss of the underlying crypto-assets. Regulators should take these developments into consideration and assess whether to regulate liability (how to identify who is at fault when crypto-assets are lost/stolen) and set standards to address the main risks of such hardware products.

Standards

As the technology progresses, public authorities should consider adopting standards of successful blockchain projects as a reference or benchmark against which other projects are to be assessed.

Such standards should include:

- Best practices in testing and deploying new versions of blockchain software. For instance, Ethereum is in the process of transitioning from a "proof-of-work" secured protocol to a "proof-of-stake" one. This transition, if not carried out correctly, could severely harm the Ethereum project and its community.
- Standards and requirements for select services or parts of the blockchain ecosystem such as centralized exchanges (in terms of security, AML/KYC, consumer protection, guarantees and insurances etc)
- Standards of successful governance balancing the power/participation of users, miners, nodes and developers.
- Standards on inclusion for vulnerable consumers. While the software, interfaces and tools developed for the core public blockchain cannot be subject to requirements such as accessibility, any centralized service which interacts with such public blockchains has to meet identical standards as other digital services in terms of accessibility and inclusion for vulnerable consumers (elderly, people with disabilities etc).

Addressing specific risks:

Below is a short set of policy recommendations to help address some of the many risks identified in the EBA 2014 paper on cryptoassets[33].

- User suffers loss when an exchange is fraudulent
    - In the case of a centralized exchange, regulators should make sure that all exchanges operating inside the EU abide by the appropriate rules to ensure that no such fraudulent exchange can open shop, set up a EU account and operate within the EU.
    - Regulators should proactively monitor, catalogue and block exchanges operating illegally within the EU, in cooperation with Internet Service Providers.

[32] https://medium.com/@bitassetglobal/5-blockchain-phones-for-crypto-holders-899a56c1cd8c

[33] https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1

    - A clear prosecution procedure of fraudulent centralized exchanges should be put in place.
    - In the case of decentralized exchanges, regulators will likely not be able to enforce appropriate rules. Co-regulation/self-regulation is advised in those cases, and regulators should issue clear warning to consumers engaging in trading on decentralized exchanges.
    - Prosecution of individuals running decentralized exchanges should also be clarified.
- User experiences drop in value of VCs due to (significant and unexpected) exchange rate fluctuation
    - This risk is inherent to the decentralized and especially, speculative nature of crypto-assets. Regulators (including ESMA and EBA) should issue clear warning to consumers about the risks involved in trading crypto-assets, maintain regular monitoring and use their intervention powers if need be. Another way could be to limit interactions to knowledgeable users, although this would be difficult to assess and certify. This could be on the basis of the "product intervention powers" provided under MiFID2 and the IDD.
- User suffers loss when buying VCs that do not have the VC features that the user expects
    - Indeed, many crypto-asset projects do not deliver the promised features, or fail to deliver them on time. Or more simply, even if they deliver, the user-base is not sufficient for those features to have any relevance. Many crypto-assets with great features such as low transaction fees or high transaction throughout end up failing due to a lack of community/user support. This is again an unavoidable consequence of the decentralized/public nature of crypto-asset projects, which have more or less serious/engaged developers behind them, and a strong community (especially miners/users). This risk is similar to that of funding an online multiplayer video game on crowdfunding platforms. Even if the video game has all the promised features, if there is no player base, then the features remain useless. Consumers should thus be advised to invest only in projects that they intend to use directly. Purely speculative investments increase the chance of such projects of failing.
- User suffers loss due to changes made to the VC protocol and other core components
    - The decentralized/public nature of certain crypto-asset projects makes it impossible to predict how the protocol of a crypto-asset will evolve. There are many examples of forks or controversial decisions made by developers which can affect end users or investors of crypto-assets (for instance, the Ethereum hard fork after the hack of a decentralized autonomous organization holding millions of euro worth of ETH or the decision by many crypto-asset development teams to embed an anti ASIC[34] code in their projects). It is again a risk inherent to the nature of public decentralized crypto-assets.
- User is in violation of applicable laws and regulations
    - The present risk refers directly to the point above on regulatory arbitrage. A clear regulatory framework for crypto-assets should be quickly put in place precisely to avoid legal uncertainty for consumers and those engaged in crypto-asset projects alike.
- User loses VC units through e-wallet/exchange theft or hacking
    - Regulators should set common, general industry standards in terms of security to minimize theft or hacking.

[34] ASICs are special types of hardware which are designed specifically to mine crypto-assets.

    - A difference should be made between cases where the consumer accesses his/her crypto-assets via a third party via traditional security methods (password, 2FA etc) and where the liability is with the service (such as an exchange), and situations where the consumer is in direct control of the private keys giving him/her access to the crypto-asset public wallet. In the later case, liability is with the consumer, except if it can be proven that the developers have committed a fault, in which case, the legal proceedings to remedy the situation must be clarified.
    - In the case of centralized exchanges, clear rules with regards to security, reserves and insurances to compensate consumers in case of losses must be established.
- User suffers loss when VC payment they have made to purchase a good is incorrectly debited from their e-wallet
    - A more accurate description of this risk is the uncertainty relating to the cost of a transaction and the difficulty in correcting mistakes (funds sent by error). Errors in transaction fees have been well documented and while they are a rare occurrence, they can cause a high detriment to consumers[35].
    - Regulators should cooperate with both merchants and miners (more specifically, mining pools) to help address these risks. Mining pools can refund very high levels of transaction fees if the person who paid them comes forward.
    - With regards to crypto-asset transactions, implementing a form of escrow service should be a recommended good practice in order for a facilitated way for consumers to delay or cancel a transaction within certain conditions.
- User is not able to convert VCs into fiat currency, or not at a reasonable price
    - There can be no guaranteed liquidity of decentralized public crypto-assets. Consumers should only invest in crypto-assets if they intend to use them directly regardless of convertibility to fiat (typically for utility tokens, where they want to access a certain service) or choose a crypto-asset with high liquidity levels (large market caps) if they intend to use that token as a means of payment.
- User suffers loss as a result of VC prices being manipulated
    - At present, the risk of price manipulation still remains high, given the enduring existence of so called "whales" which engage in pump and dump schemes to further consolidate their position and lure in consumers looking for quick gains.
    - Consumers should be advised to invest responsibly and engage with crypto-assets they intend to use directly (for payments, or accessing certain services). It should be made clear that using crypto-assets for investments or speculation is highly risky.

Conclusion:

Crypto-assets have been around for just over a decade. While the underlying technology is still in its infancy, consumers can finally find tangible and concrete applications in the public blockchain space, be it for international cross border payments/remittances, or for running dapps (decentralized applications). Nevertheless, the risks of investing in crypto-assets remains high, which means that only the most technically and financially savvy consumers can take full advantage of the opportunities of crypto-assets at this time.

[35] https://beincrypto.com/litecoin-transaction-fee-17000-mistake/

https://www.ibtimes.co.uk/bitcoin-user-loses-215000-by-mistake-due-transaction-fee-error-1629451

The emergence of “user friendly” third party services among which we find centralized exchanges is held back mostly by the technical limitations and problems on existing public blockchain projects and by legal uncertainty or ill-suited regulation.

The FSUG does not see a mainstream adoption of crypto-assets in the short term at the level of retail users and recommends that consumers are properly informed about the risks of engaging with crypto-assets and possibly inhibited from trading in crypto-assets, or at least in crypto-assets which do not comply with certain regulatory standards and criteria.

The FSUG recommends that European regulators should adopt sensible and enforceable ad-hoc regulation, adapted to the specificities of public decentralized blockchains, in line with the recommendations above, which mixes regulatory measures, especially targeting centralized entities or clearly identifiable third parties/intermediaries, and self-regulatory/co-regulatory measures encouraging crypto-assets projects to adopt internal governance rules and development standards which take into consideration consumer protection.