Published by **bqintel.com**

BLOCKCHAIN QUARTERLY

1ST QUARTER 2019

PREMIUM VERSION

bqintel

6th Edition

FOREWORD

The following report is the latest edition of Blockchain Quarterly — a series of in-depth studies which began in 2017 and is undertaken on a trimestrial basis. These studies highlight key activities and trends within the blockhain industry globally and in key regions around the world.

In order to ensure comprehensive coverage, each periodical analysis refers to the material contained in previous issues and elaborates on already debated considerations—thereby updating views, introducing new solutions, and going deeper into the analyses.

In these studies, we discuss research, principles and fundamental factors about the crypto sphere as a whole. This includes the latest technical evolutions, use cases, regulations, etc. for the entire span of distributed ledger technologies (DLT). The purpose is to ultimately reach a reasonably exhaustive understanding of crypto developments worldwide.

Based on this review, it should be possible to have an informed view of the direction in which the sphere may evolve. In particular, we aim to identify the current underlying forces that are driving DLT-based currencies and token markets, in order to identify possible scenarios.

We would like to draw our readers' attention to the fact that each exercise is more complex than the previous one, as the blockchain environment is evolving quickly. All information presented herein is considered to be accurate at the time of production, but no warranty of accuracy is given and no liability in respect of any error or omission is accepted.

Any examples used are generic and for illustration purposes only. Any forecasts, figures, opinions or strategies set out are for information purposes only, based on certain assumptions and current market conditions and are subject to change without prior notice.

If, despite all the care taken in gathering accurate information, some errors or lack of precision are found, please contact us on research@bqintel.com.

TABLE OF CONTENT

EXECUTIVE SUMMARY

During the past months, blockchain start-ups—even the most serious ones—have been laying off staff, miners shutting down plants, and crypto funds reporting heavy losses. All in all, although there is not, strictly speaking, "blood in the streets," the situation is quite serious.

Application efforts in the various industries continue to fall short of reaching the production stage. Large groups continue to research the technology; they satisfy their boards by showing some limited gains in efficiency, thanks to DLTs, but real disruption will only come from start-ups, even though these are currently struggling.

Technically, there is nothing disruptive to be reported. However, there has been gradual progress in refining and adopting solutions such as MimbleWimble, the Lightning Network, and a bunch of initiatives in the decentralized application infrastructures segment. Competition is on.

In many jurisdictions, regulation continues to progress toward offering clear guidelines and converged legal frameworks.

In the short-term, although prices of crypto-assets are already low, they can still go lower, but probably not by too much. Investors, ICO reserves and holders have already suffered enough, and in a sense, they have not much to lose anymore. Most analysts are waiting for the downtrend to bottom, and no doubt "whales" will then re-enter the market when they feel that the bargains are too tempting.

There are many objective signs of a possible recovery:

- Volumes are increasing, both on-chain and off-chain; hash rates have also been increasing.
- The communities have no shortage of enthusiasm, conferences are still full, and actors in the ecosystem are more convinced than ever that the world is on the verge of change.
- Interesting solutions, such as the Lightning Network, are reporting an explosion in adoption. The activity on decentralized exchanges is booming.

Looking forward, and in the mid-term, the feeling overall is slightly positive. To be pragmatic, one must acknowledge that the road to general adoption is proving to be more difficult and is taking longer than initially expected. Both the monetary adoption and the decentralized application infrastructures are limited by scalability, volatility, and regulation, in addition to being difficult for non-aficionados to get into. It will take more time to see quality services emerge and to have a large enough pool of people knowledgeable of the technology before we see a significant move into the alternative world.

In this context, assessing the financial attractiveness of a decentralized project is going to depend on its ability to deliver the revolutionary system advertised. The qualifications and leadership of teams are relevant, of course, but it is also essential to be able to assess whether the expectations of the projects are reasonable, or likely to be disappointing.

GLOBAL MARKET UPDATE

UPDATE ON THE PAST THREE MONTHS

As 2019 began, observers and actors could only sum up the past year as a "crash" or "worst year ever in crypto." The bear market that was seen as early as mid-January 2018 and confirmed in February has proved to be a strong trend that is not yet finished, as there are no signs of a recovery in the crypto markets in early 2019.

Despite this, the demand for tech people involved in DLTs remains strong (see comment on "Blockchain talent" page 13). Over the course of the previous twelve months, a lot of people that had entered by chance, perhaps attracted by the hype, have lost their enthusiasm, or have drifted elsewhere. Nowadays, fewer amateur and inaccurate articles are found on the web. Only the knowledgeable and the serious enough have remained.

So, from a hype standpoint, crypto has declined, but the nuclear core is still very (radio)active and convinced. We believe that this community will not shrink any further, but instead, it will start to attract newcomers.

When surveying the remaining "core community" that is still working in the crypto sphere, we could sense that its people share a common feature: they are all passionate individuals who strongly believe in what they do, in the vision of the world that they hold and are trying to solve its actual problems. These individuals are not going to exit it anytime soon; they are going to pursue their ventures, whatever it takes.

There are a lot of clues indicating that embers glow under the ashes. We are going to uncover them throughout this report; one of these relates to volume considerations. Despite the decreasing prices of crypto-assets, the volume of off-chain exchanges, expressed in bitcoin (rather than in fiat), has increased steadily compared with one year ago. Furthermore, the number of on-chain bitcoin transactions has been constantly increasing since the low level of February 2017, to again, reach its highest levels ever. Add to that, there is still volatility in the markets, which proves that bitcoin is very much alive.

Less noisy but tangible applications keep appearing, with DLT-based applications now in production and delivering some measurable bottom-line results. The gains are not yet fantastic, but they are now proven, and companies will make logical decisions to implement the pilots. This is what we think should be carefully monitored, as it is here that we see a pulse.

Right now, the battle in the media between promoters and detractors of DLTs has stabilized. Detractors are no longer bothering to argue over a body believed to be dead, while promoters continue their efforts.

The present situation is summed up well by this quote from Jimmy Song, bitcoin developer and entrepreneur: "Bitcoin price going up can be a very big distraction for a lot of developers. When the price is going up, we're all thinking about how much bitcoin we

have and what we can buy, so it's very easy to get distracted when there's a bull market. During a bear market, you don't want to think about the price that much. Instead, you get down to work and build all sorts of goods and services that might be useful to people, and that's a good thing."

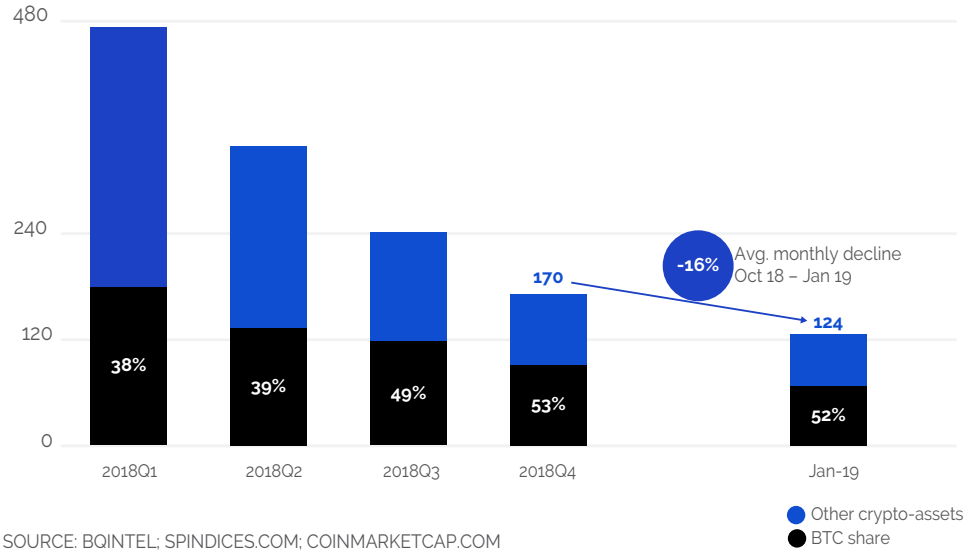
So, we will continue to pay a lot of attention to profitable application deployments, but overall, the DLT ecosystem is not in bad shape to begin a recovery sooner rather than later. The expectations of the public and CEOs have also come down to earth. This is a good starting point for a new and hopefully sane cycle.

ARTICULATION OF THE GLOBAL ECONOMIC SITUATION

The three-month gap between releases of this Quarterly is enough time for the global economic situation

FIGURE 1: TOTAL CRYPTO-ASSETS MARKET CAP

BN USD, % BTC MARKET SHARE



SOURCE: BQINTEL; SPINDICES.COM; COINMARKETCAP.COM

to evolve, and yet short enough for the evolution to be substantial each time. This time, though, we have sufficient elements to enable an accurate assessment of the situation.

In November, stock markets fell significantly, increasing the extent of the expected reversal, especially for technology-related companies. Apple fell from 230 in October 2018, to 140 in January 2019, and Facebook experienced a similar downturn (see figure 2). These are large capitalizations, so the losses for investors were considerable. Losses were reported in other sectors and, to a lesser extent, other countries. Nevertheless, the situation is the same regarding the trend reversal.

In our last report, it appeared obvious that some key resistance levels for stock indices were being tested; these levels have since been broken. This leads us to conclude that the uptrend is broken, and therefore, we have entered a downtrend. As before, the aim here is not to focus too much on the causes that may influence further moves in the world's stock markets, but rather to acknowledge that markets experience cyclical behavior, and we are heading toward further corrections: this view is now validated. The only unknown is the extent of the correction—the gravity of what lies ahead in the next eighteen months.

The fact that we have entered a downtrend in stock markets is important. Now, what are the implications for crypto-assets?

First, crypto-asset classes are evolving independently from other asset classes, including gold. And whereas some still pretend that precious metals are negatively correlated to cryptos: this does not appear to be obvious—maybe not yet—as clearly seen in figure 3.

The non-correlation of crypto and stock markets should continue. With the drop in the value of crypto-assets, the remaining value has shrunk so much already that, for holders, the difference between a write-off of 90 percent and 95 percent is not great, so a further shrinkage would not cause much pain if it were to happen. Currently, crypto-assets appear "cheap" compared to stocks, and hence the likeliness of a transfer of wealth from the former to the latter has increased.

This potential negative correlation would be in line with the initial purpose of cryptocurrencies; to be an alternative to the world monetary system—thereby benefiting when the adversary collapses. Although crypto prices react to news, they also react to fears of a collapse of the euro, the failure of fiat currencies, forks and other technically relevant crypto developments. However, they don't react to changes in interest rates and real economic indicators. A caveat: there is no history of cryptocurrencies existing during a bear stock market, so for this reason, any theory may hold.

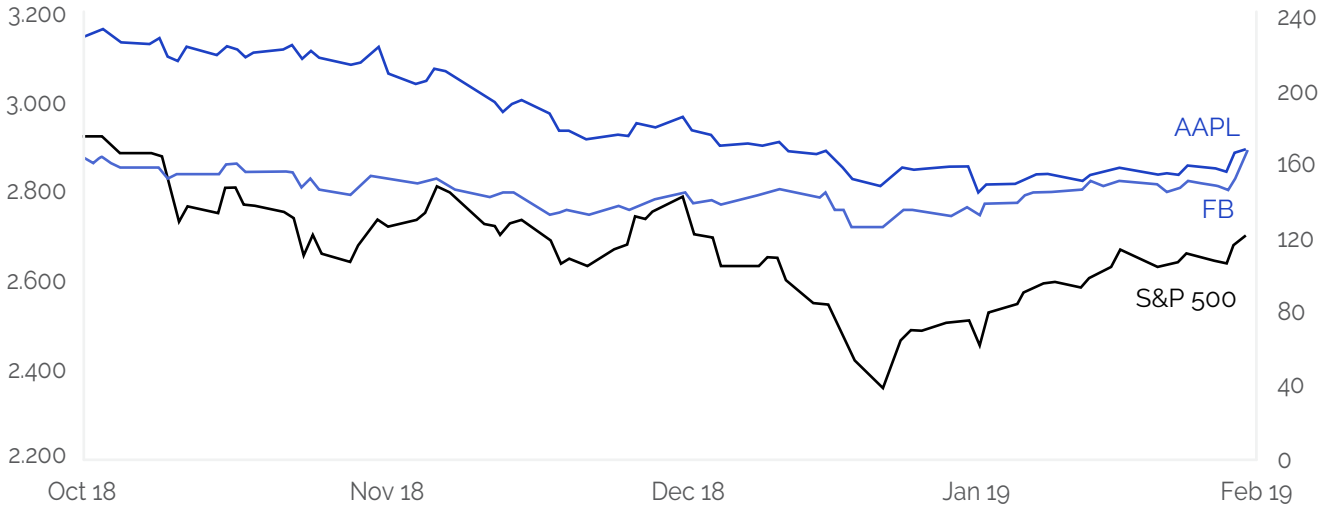
MACROECONOMICS

An interesting point that is never mentioned, but one that we believe is very relevant, concerns the impact of cryptocurrencies on macroeconomics. Cycles occur when monetary expansion results from the willingness of economic actors to initiate activities which require funds to be invested in projects, with the expectation of future positive cash flows.

When we see excessive creation of value, whether it be through bitcoin valuation, through altcoins appearing out of thin air—regardless of what they are homogeneous to—or very interestingly through stablecoins tokenizing fiat, we are looking at either a new "gold" resource suddenly being discovered (similar to the nineteenth century) or at new kinds of banks that want to act as money multiplicators.

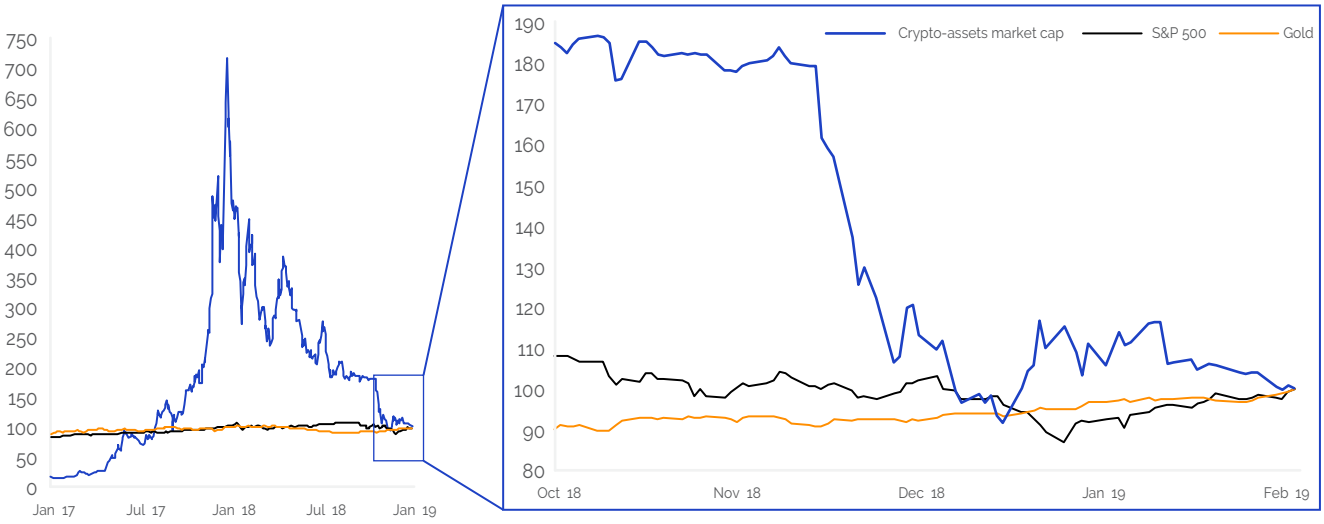
In the case of the crypto market, we experienced a monetary expansion outside of the control of a central bank for the first time since Bretton Woods ended. If this mechanism works, it has the potential to fuel an economic expansion in the coming years.

FIGURE 2: S&P 500, APPLE & FACEBOOK STOCK PRICES
SPX INDEX, USD



SOURCES: NASDAQ; SPINDICES

FIGURE 3: INDEXED VALUE OF CRYPTO-ASSETS VS S&P 500 & GOLD
FEB '18 – JAN '19, INDEX (100=JAN 31, 2019)



SOURCES: SPINDICES.COM; COINMARKETCAP.COM; WORLD GOLD COUNCIL; QUANDL.COM

UPDATE ON THE REGULATORY POLICIES

The following section discusses the major trends in the regulation of blockchain applications and crypto-assets globally. For more detailed updates by country, refer to "Overview by Country" section, page 43.

CURRENT GENERAL APPROACHES BY GOVERNMENTS

Overall, governmental action in the field of DLTs and cryptocurrencies remains on track.

A wide variety of approaches are continuing, with some countries still banning cryptocurrencies and ICOs, while some smaller countries are keen to propose forward-looking frameworks to attract innovative fintech businesses, however, most countries are active in issuing guidelines or monitoring the compliance of crypto actors.

As emotions have calmed down, there is less urgency for officials to act and clamp down on crypto businesses, as they once claimed they would. Central banks, in particular, have almost unanimously concluded that cryptocurrencies are not a threat and not something they should be engaging with any urgency.

As an observation, civil law countries deploy regulations faster than common law countries—in which case, more framework is likely to be better than no framework, as finance people are among the most averse to uncertainty.

However, every country agrees that the profits made in trading crypto-assets should be subject to taxation. An increasing number of countries are taking actions to tax private crypto-asset traders. Examples highlighted in the press lately include Bulgaria, Denmark, and others. These moves include obtaining information from the exchanges (located in their territory—at least for the moment) of holdings and the activities of private traders.

WORLDWIDE COORDINATION

The worldwide financial stability has confirmed the view that cryptocurrencies do not threaten the global economy. Arguably, the crypto sphere is too small, even more so now that the total market cap is back in the region of 100 billion dollars.

At the World Economic Forum gathering in Davos in 2018, the comments around crypto-assets and bitcoin were skeptical, but not completely closed to the emerging technology. This year, round tables and debates on blockchain were again held, and Davos participants have chosen sides. A lot of opposing views were expressed, and crypto-asset valuations were heavily criticized. The common ground found by panelists has been that the value of tokens will be derived from how useful the underlying protocol is. Hence wealthy, powerful people on the planet agree that what matters is the technology behind crypto, rather than the tokens themselves.

Responding to this consistent position of actors in the world economy, (bitcoin no, blockchain yes), Joseph Young

came up with a nice saying: "That's like saying: airplanes will go to zero while engines have potential!"

STATUS OF OFFICIAL INITIATIVES TO PASS FIAT ON DLT

Currently, it appears that officials have resolved this matter. Most countries have concluded that they will disregard possible sanctions at this time. The latest statement by the Bank of International Settlements says: "No central banks reported any significant or wider public use of cryptocurrencies for either domestic or cross-border payments in their jurisdictions. Usage of cryptocurrencies is assessed to be either minimal ('trivial/no use') or concentrated in niche groups." BIS member central banks believe cryptocurrency use "will remain minor" due to "low retail acceptance, compliance issues, better understanding by the general public of the risks involved and, for some jurisdictions, outright bans."

The worldwide financial stability has confirmed the view that cryptocurrencies do not threaten the global economy. Arguably, the crypto sphere is too small, even more so now that the total market cap is back in the region of 100 billion dollars.

Only a few outliers are progressing in the area, of which Russia, China, and Japan are the most significant.

KYC, AML, AND CFT

The status is still very much the same as it has been in recent months, that is: very stringent, with systematic and effective implementation requirements imposed on businesses that want to register, irrespective of the jurisdiction. A business starting in cryptos today cannot debate this: KYC, AML and CFT checks of its customers are compulsory to be able to operate.

A question worth asking is if all exchanges and cryptocurrency price movements are the under scrutiny of regulators, why is fiat cash still allowed out there? Probably a wider reflection about what people should be allowed to do without KYC compliance should be conducted.

One observation one can make here relates to the questionable actions undertaken by the United States. When a US citizen wants to buy an asset issued abroad, with a non-USD currency, from a non-US counterpart, there is still concern about how US law may apply to the transaction. No other country in the world adopts this extraterritorial approach with its legislation, and there is no reciprocity when a non-US citizen does business with a US citizen. This situation impacts the KYC process. As a result, businesses prefer to discard US citizens from their pool of investors and clients. This asymmetry is, without question, a form of protectionism on

the part of the US and is neither fair nor sustainable in the long run.

Platforms resistance

The problem is that KYC has some opponents, not the least being the exchange platform operators. Some claim that it is pointless implementing any KYC procedures, as everything is publicly available on the blockchain anyway. Others argue that the lengthy sign-up procedures and the tedious wait for KYC checks are an unacceptable violation of an individual's privacy.

One example is Kraken, which complained about the cost of compliance, stating that the "cost of handling subpoenas (not to mention licenses) is quickly becoming a barrier to entry." Rather than deterring criminals and increasing transparency, some argue that all KYC/AML does is financially exclude those who lack the documentation to prove their identity—a particular problem for the world's 1.7 billion unbanked, whose hope it was that DLT could help them to integrate.

The fight is just beginning, and of course, governments and states have a significant head start in this field. However, fears of hacks of KYC data from banks or exchanges are starting to show how preposterous this race for control is becoming.

On-chain authentication and identity management

A business case exists for providing authentication of users, thanks to distributed ledgers. The use case exists, of course, for on-chain applications (as users always sign what they are doing cryptographically), but also, why not for off-chain usage.

The concern for identity verification is stringent, primarily for exchanges and financial services providers, even if more advanced checks will be required, depending on the risk tolerance of the business service provider.

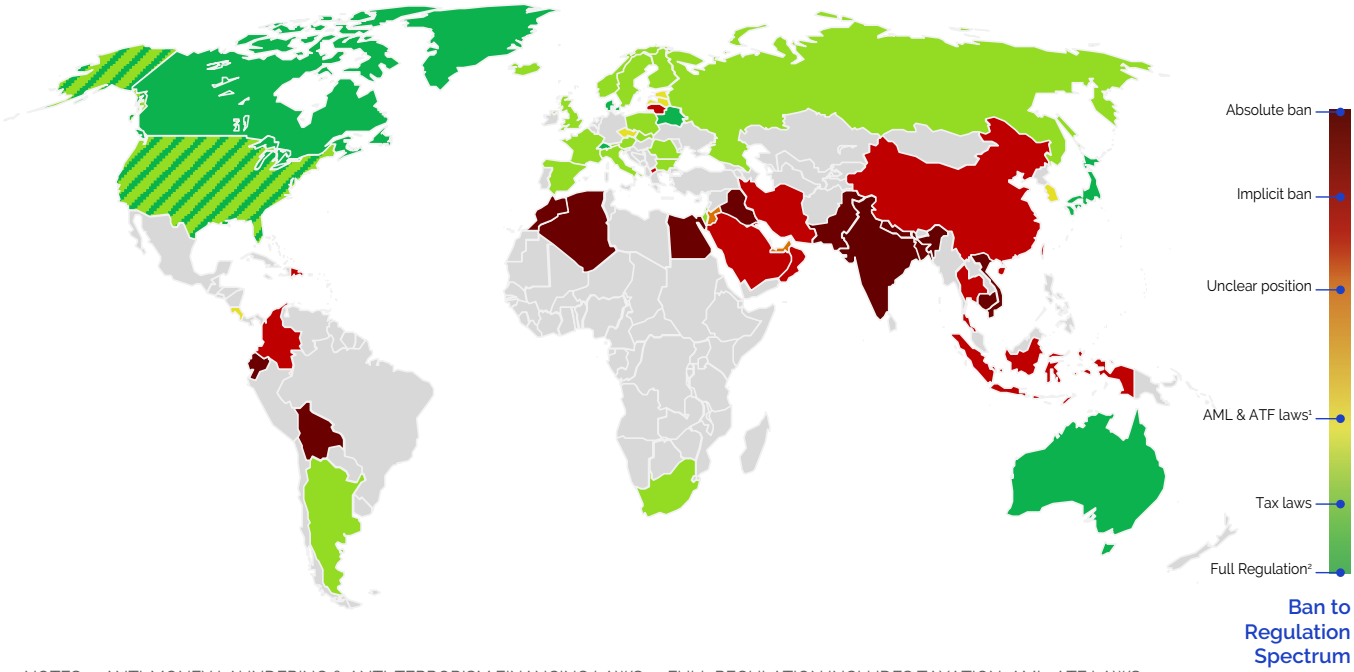
Hence, the facilitation of such an authentication service that complies with KYC (as well as AML and CFT) is necessary to make the onboarding of platforms users seamless and efficient—the opposite of what it is today. Ideally, performing the authentication service setup properly, once by the users and by any actors in the environment, could then be referred to and used to access various private offers.

Two directions exist in this respect:

- Independent initiatives have begun to propose such a service, such as Authenteq in Iceland.
- KYC can be incorporated into the blockchain infrastructure, as is the intent in NEO, Concordium, Belfrics, and others.

An efficient KYC service has not yet been implemented, but the sector is working on this. Let's hope that the efficiency achieved in this domain will further unlock the potential of DLTs. The ultimate in this field would, of course, be for zero-knowledge-proof mechanisms to be able to handle this service.

FIGURE 4: LEGAL & REGULATORY STATUS OF CRYPTO-ASSETS AROUND THE WORLD



NOTES: 1. ANTI-MONEY LAUNDERING & ANTI-TERRORISM FINANCING LAWS; 2. FULL REGULATION INCLUDES TAXATION, AML, ATF LAWS IN THE US, DIFFERENT STATES HAVE DIFFERENT BLOCKCHAIN LAWS AND REGULATIONS
SOURCES: BQINTEL; LAW LIBRARY OF CONGRESS; BITCOIN MARKET JOURNAL

REVIEW OF BLOCKCHAIN INDUSTRY PLAYERS

MINERS

News of mining plants closing or at least suspending business, continue to hit the headlines. For instance, Bitmain, the Chinese mining giant, has closed several offices (Israel, Netherlands, and Texas). Giga Watt in the US has also been forced to cease operations. This trend has resulted in the available bitcoin hash rate decreasing by 25 percent to 30 percent since October, despite the overall annual increase. In turn, this has an impact on the safety of the bitcoin network.

Only low-cost mining plants are today operating with a limited profit (the rest being unprofitable, see figure 6), mostly thanks to advantageous contracts with electricity providers. Even for these miners, unless mining difficulty level adjusts as a result of more miners unplugging, the threshold is 2,400 USD/bitcoin.

The consequences of this bear market are already being felt. China's dominance in hash power concentration continues to increase, thanks to its competitors being driven out of business.

Additionally, nobody is buying brand-new mining equipment, so business is also slow for mining rig vendors.

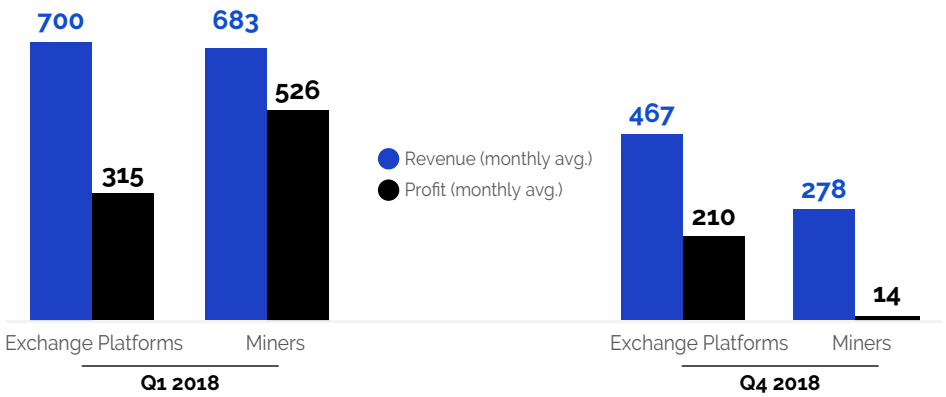
More positively, the decrease in hash power has reduced electricity consumption and consequently the environmental footprint of PoW for the time being.

EXCHANGE PLATFORMS

Centralized "off-chain" exchange platforms

Demand from ventures that issued an ICO for listing on the main exchanges (Binance, Huobi, OKEx, Kraken, etc.) is high. On the one hand, the benefits for projects that are listed on one of the main exchanges are significant, in terms of recognition, exposure, and access to liquidity. On the other hand, one of the business objectives of exchanges is to offer a maximum number of interesting tokens that they are confident will

FIGURE 5: EXCHANGES AND MINERS 2018 FINANCIAL PERFORMANCE
MN USD, ESTIMATED MONTHLY AVERAGE 2018



SOURCES: BQINTEL; BLOCKCHAIN.COM; ETHERCHAIN; COINMARKETCAP; DIAR; BLOOMBERG; DIGICONOMIST

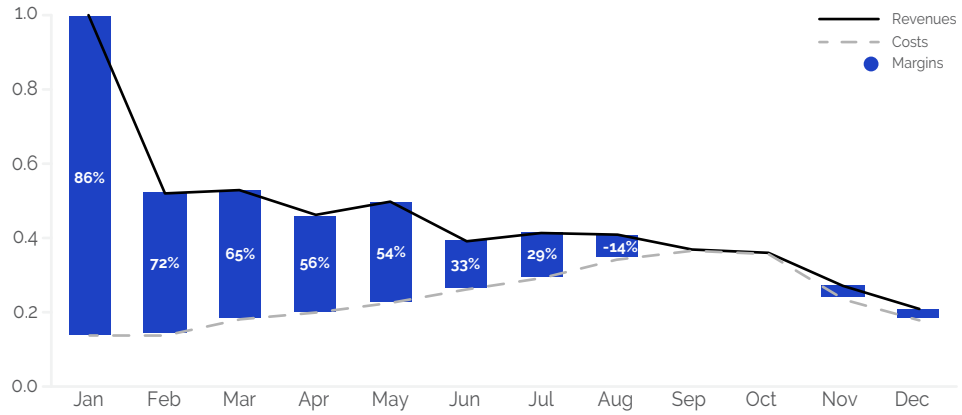
create a market that is active enough. Hence, some exchanges have implemented admission processes, including token information disclosure requirements. ICO details and success criteria are often analyzed by the exchanges as a proxy for evaluating the attractiveness of tokens. Their focus is on avoiding listing scams and weak projects that have a high probability of failure—they, of course, want to protect investors who are using their platform, from being trapped and having a bad experience. Very often, a voting mechanism is deployed for investors and users of the exchange platform to nominate (in priority order) which tokens they would like to see listed on the exchange.

Some exchanges, such as Coinbase, have begun proposing a custodian service; holding and securing crypto-assets for its clients.

A few agitators are trying to raise public concern about exchanges taking control of their crypto-assets, not the least due to repeated hacks of exchanges accounts. The attitude that "it's on the blockchain or it did not happen" or "if you don't have your private key, you have no bitcoin" is quite important. Movements have been launched to plan a bank run by coordinating the withdrawal of a maximum amount of crypto-assets from exchanges at the same time—to check whether exchanges indeed own the relevant amount of cryptocurrencies.

Another distinct aspect that is worth highlighting is the PoS business that exchanges might be engaging in. As they own a lot of native cryptocurrencies that work with PoS or DPoS, staking these assets would be very tempting for them, and they earn a reward while doing so. While the European Union has started to express the view that a custodian should not be allowed to stake assets in their custody without explicit agreement from their customers, the business of holding crypto-assets and managing earnings,

FIGURE 6: DECLINE OF BITCOIN MINING PROFIT MARGINS
BN USD, 2018



NOTE: COSTS ASSUME RETAIL ELECTRICITY PRICES
SOURCES: BQINTEL; BLOCKCHAIN.COM; ETHERCHAIN; COINMARKETCAP; DIAR; BLOOMBERG; DIGICONOMIST

thanks to staking in the name of clients, could be seen as a new form of banking. There is no reason why this will not occur at some point in the future.

Decentralized exchanges

Despite the noise decentralized exchange projects still make (they represent one fifth of total number of platforms), their relevance in the overall traded volumes is still negligible (see figure 7). The evolution of these figures will tell a lot in the coming months.

Some sources have highlighted that the rising cost of compliance for off-chain exchange platforms has resulted in decentralized exchanges having a competitive advantage.

Exploring this trend is, in fact, very interesting. Decentralized exchanges cannot be stopped; governments cannot close them, they are available 24/7 to any citizen on earth to use, with no identity check, no financial cap, and without questions regarding the origin of the funds. Hence, their use is likely to be prohibited by financial regulators, if not completely, then at least as far as their jurisdiction applies.

Despite the noise decentralized exchange projects still make (they represent one fifth of total number of platforms), their relevance in the overall traded volumes is still negligible

It is not clear whether individuals will take personal responsibility for acting on these exchanges, aware of the concern that ultimately when attempting to return funds to the controlled "real world," they may face difficulties in proving their legitimacy when questioned by traditional players and authorities. In turn, this may lead to a deepening of the separation between the legacy fiat environment and the new cryptocurrency environment.

Centralized exchanges are investing in the field of de-centralized exchanges—with Binance being the flag-ship of this move. What this means is that people will be able to exchange assets directly from their hardware wallets, thanks to a sort of over-the-counter facility.

BLOCKCHAIN CREATORS, ENTREPRENEURS AND APPLICATION DEVELOPERS

At the price level that cryptocurrencies have now reached, holders of BTC and ETH, and even teams holding their own coins, are down to a tiny fraction of what they raised. From this moment on, it makes little sense for them to exit or sell what they still have.

If it no longer makes sense sell out at those price levels, this means that the downward pressure on prices is likely to be almost exhausted.

In parallel, of course, ICOs currently going public are raising only a fraction of what similar projects were able to raise just one year ago.

Decentralized applications

Decentralized autonomous organizations (DAOs), or decentralized applications are sets of smart contracts that offer functionalities on publicly distributed ledgers, accessible to everyone. These are the most disruptive application of DLTs.

Even if progress has been slow and below expectations for decentralized applications that launched in recent years, there have been some successes, which should not be ignored or marginalized, including:

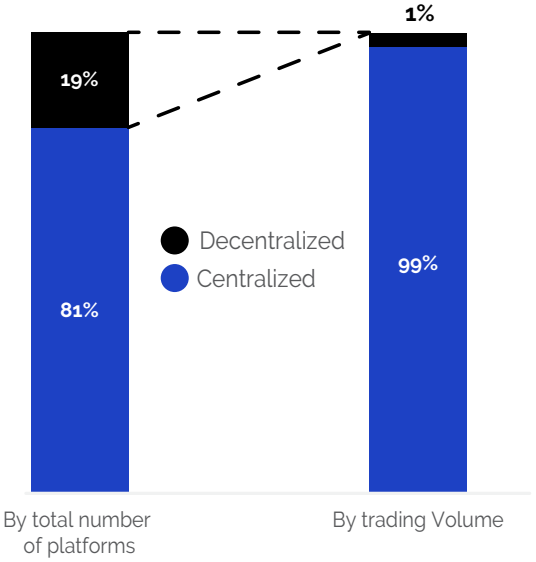
- Augur, the prediction market application is live and was used with success in the US midterm elections.
- Decentralized exchanges, IDEX and FordDelta, have witnessed very significant growth in terms of user numbers and trade volumes.
- Status, a decentralized messaging platform, has moved to a beta version.

All these services are not yet easy to use or scale, but they are still embryos of what we can expect. Nevertheless, some argue that decentralized applications have no chance of becoming mainstream any time soon because the required supporting infrastructure is still being developed. In this sense, a parallel drawn with the internet phenomenon would have to be based on the decade of the 1990s, rather than the 2000s.

The model for decentralized applications offers nothing less than a complete reshaping of how activities are

FIGURE 7: MARKET SHARE OF CENTRALIZED VS DECENTRALIZED EXCHANGES

% OF TOTAL EXCHANGE MARKET SHARE



SOURCE: TOKENINSIGHT

constituted, how money is raised, how stakeholders are economically rewarded, how financiers are attracted and compensated, how governance is expressed and enforced. So, considering that this ultimately has the potential to challenge even the status quo of capitalist profit-seeking companies, it is normal that the model is currently still in the very early stages.

Utility token ICOs

The failure of utility tokens has been well-advertised. Even if one wants to advocate for the system, it is difficult to regard it as successful at the moment. You could argue that the extreme crypto volatility was a paroxysm for utility ICO tokens, or that these price curves merely show that start-ups pass through very difficult downturns in their first year, which was not observable before when continuous trading in venture capital funds was not the practice.

However, it should be acknowledged that the utility-token-style ICOs currently being conducted are mostly based on highly dubious projects. Very few serious projects go that way, partly because not many new promising ventures are being launched during this crypto winter, and partly because the utility-token model has been roundly criticized, and credible new projects are currently opting for other, more traditional, alternatives.

Regarding estimating the worth of utility tokens, sound valuation approaches are scarce. One equation attempts to model the case: $M \times V = P \times Q$, where the total number of tokens in circulation, or Mass M (which equals the number of tokens × price per token) multiplied by their turnover, or Velocity V, in a given period will equal the Quantity Q of the digital service being performed in a given period on the platform, multiplied by the Price P of the service. This is straightforward, and from there, the token price can be deduced. This approach does not account for speculators holding the crypto-asset, and therefore the result can be regarded as a floor price. Be aware that applying this equation is difficult when a platform is still under development, or an early minimum viable product (MVP); it's all about estimating projections.

Security token offerings (STOs)

The regulations for offering and issuing securities are clearly framed in almost all jurisdictions. Regulations applicable to IPOs and public companies' capital management are usually quite constraining in terms of information disclosure, prevention of insider trading, accounting procedures, etc. All of this naturally applies to enterprises that wish to issue securities as tokens on blockchains.

A substantial number of articles have presented STOs as evidently the new way to raise funds, thanks to blockchain technology, which is bringing clarity to the "Wild West" that the crypto space has been. We would be cautious on that: while there is no doubt that STOs have a bright future due to the continuum in functions that tokens offer, as we have seen repeatedly, other categories of tokens also have a future. It is worth mentioning that small ventures—and ventures unlikely to attract venture capital—do not have the money to go through the costly process of an STO, and this is precisely the issue that ICOs were trying to solve.

We can conclude that, although the forest of projects still needs to be sorted out, security tokens are by no means going to be the only option to remain

on the landscape.

Airdrops

Airdropping is a practice by which the team behind an ICO or an STO, sends its token to the wallets of individuals—and mostly exchanges— for free. Wallet owners will then be motivated to sell the newly received token for any price a buyer would be willing to pay on the exchanges. If there is a market, then the tokens gain a market value, and the creating team can then sell some of the tokens they retained to fund their activity.

The biggest news in the world of airdrops is the TRON move to revive Bittorent and distribute BTT tokens to Tron holders every eleventh day of each month till 2025. The effect of this airdrop initiative is to strengthen the value of the supporting blockchain. People are likely to hold their TRON tokens in hopes of receiving airborne money on a regular basis, thereby locking out of the market a significant supply of the cryptocurrency—decreasing supply, and, in turn, supporting an increase in the price.

Interestingly, exchanges quickly claimed that they would support the airdrop, which confirms the view mentioned above that exchanges will play an ever-increasing role in managing the rights of token holders, which they in effect pool (see comment on "Exchange platforms").

Although the forest of projects still needs to be sorted out, security tokens are by no means going to be the only option to remain on the landscape.

Blockchain talent

News of former central bankers and other high-level executives joining boards of advisers and management of crypto-related businesses continue to hit the headlines regularly.

In most countries, the median annual salary for blockchain developers is on the rise, with developers in Switzerland routinely paid 15kCHF a month (15 thousand USD), due to the increase in wages caused by the scarcity of resources and the continuing demand for the competencies.

But probably the most interesting news item is the layoff of more than 300 people by Consensys: over 30 percent of the workforce—later declared to have been limited to 10 percent, mostly in support functions. Bitmain and Steemit have been reported to be reducing their headcount in comparable proportions. These are significant events in the industry.

In particular, Consensys had the reputation that Joseph Lubin, a co-founder of Ethereum, was willing to pay for his vision of the expansion of the sector, no matter what. It seems that Mr. Lubin's confidence has reached its limit; the fintech consultancy firm is shrinking by 80 percent, and incubating companies are encouraged to seek investors elsewhere. This could be a sign the bottom in crypto prices may arrive sooner than later.

INDEPENDENT INVESTORS

One interesting thing about crypto, compared to conventional analysis of stock prices, is that it is possible to scrutinize not only the volumes on the exchanges but also to have a perfect view of the movements on the blockchain. This is particularly true in the case of bitcoin; analysts can process the data available in the ledger to assess which types of owners are exhibiting which types of behavior.

For instance, some analysts claim that by looking at wallets that have been inactive for the past three to five years, it is possible to assess the willingness of these people to sell out. They think that selling is largely exhausted as of the beginning of 2019, pointing to what occurred in a similar case in 2014-2015. Interesting views, of course, even if this field of study is still young.

On a similar note, a study by Chainalysis earlier in 2018 estimated that 3.5 million BTC have definitively been lost. This amount represents more than

20% percent of the available bitcoin supply.

Below, we will explore recent activities of independent investors, or individuals acting for themselves: casual holders and "crypto whales".

Casual holders

In this quarter, it is particularly difficult to clearly express the general sentiment among average investors. Firstly, there is not much discussion these days. Secondly, among individuals active on social media, who claim to be crypto experts, the tone and feeling are primarily objective; dispassionate, but still quite positive. In summary, there is no real evidence of deep despair, which is typically present when markets bottom out.

Retail investors appear to be inactive, although probably, not many are unsettled at this stage. Most people who entered the market after November 2017 were individuals who invested a small amount of their wealth and can afford to lose the investment without being financially affected. These people are now, at most, at 10 percent of their initial investment value. They do not care anymore; they played, and they lost. However, before they consider getting involved again, the price needs to rise above their entry level to confirm their initial view, regardless of whether they held or not.

Crypto Whales

Since the advent of bitcoin, dominant cryptocurrencies have emerged in a fairly small environment, and those who have been involved since the early days—especially in mining—now own a disproportionately large amount of the underlying cryptocurrency. There are accounts, publicly monitorable on the blockchain, that contain fabulous wealth, and any movement involving these accounts (or the absolute movement of large amounts of crypto wealth) is carefully watched by the communities.

When the so-called "whales" move their assets, many think that it is a sign that "something is happening." Whether or not this is true, it is a fact that these people have such a large share of the cake that they could influence the market if they chose to. Interpretation of such on-chain movements, of which nobody knows the origin or the destination or the price at which the movement is valued, is open to question. A simple way to interpret this information is that these people are active and are dealing with their assets: they are either waiting, consider when to sell, or when it is appropriate to buy.

Whales have been active in recent months, e.g., on XRP and BTC. A huge transaction occurred on January 10, 2019: 130,004 bitcoins moved from one address to another. There is no way to know what this means, but a lot of addresses that have been inactive for years also transferred bitcoins back in October 2018.

INSTITUTIONAL INVESTORS

Private equity (PE) and venture capital (VC)

Many initiatives seek to address the financing issues of start-ups and are now working to deliver their solutions. Traditional players are continuing their business as usual and are probably more concerned about the tech stock market crashing than by a new entrant disrupting their business.

Private bankers and classical investment and hedge funds

Traditional investors continue to say that they trust stocks more than cryptos. That is what they have been specializing in, and it's no surprise they are reluctant to change. Bankers, in general, continue to be very averse to crypto-assets and are totally against the pure cryptocurrencies, which they see as a threat.

Regarding utility and company tokens, it is surprising that, to date, no private or investment banker has expressed the view that their perceived threat is irrelevant: stocks will be represented by tokens, but the core job of stock analysis and choice will remain the same, yet using a different supporting framework.

It is crucial here to discuss the subject of ETFs. Usually, when there are some noises in the US about the SEC examining a proposal for a bitcoin ETF, there is a huge

expectation and then a huge disappointment, which has a great impact on crypto-asset prices. This topic seems to be sensitive, especially since the SEC is continually rejecting proposals made in this direction.

So, why is there an interest in ETFs when people can buy bitcoin directly without going through a fund? And what would a BTC ETF change in the investing landscape?

An ETF is an exchange-traded fund, i.e., a security that tracks an asset or a group of assets; in our case, bitcoin. Therefore, it is traded on the classic financial market infrastructure, "off-chain," of course. And this is a big advantage; some people are unable to back up their photos, let alone their private keys.

Its aim, ultimately, is to provide investors with exposure to bitcoin in a manner that is more efficient, convenient and less volatile than purchasing stand-alone bitcoin. This means it is a financial instrument to deal with bitcoin in the conventional financial system.

So, the big hope for speculators is that offering bitcoin through an ETF would make it accessible to more people in a way that would be likely to trigger massive acceptance and therefore investment from financial institutions (traditional banks, investment banks, and asset managers). This move could contribute to triggering a potentially massive inflow of cash into the crypto sphere. If bitcoin is packaged in an instrument that investors are familiar with, pension funds may take a small position, and if it is a positive experience, they may progressively increase their holdings.

The supporters of a BTC ETF also claim that it could have the effect of reducing BTC's price volatility.

Now, what is preventing the inception of a BTC ETF?

One major failure was the Gemini attempt. The Winklevoss brothers concluded that the SEC was calling for more market surveillance and protections in the marketplace to prevent price manipulation. The security offered by ETF applicants has been deemed to be insufficient. Volatility also has been reported as an SEC concern.

Some reviewers of BTC ETF proposals have expressed the view that it should have been allowed, which indicates there may be some political pressure to prevent it. SEC officials are bound by their mandate, which is a political one. The place of fintech on the US landscape is being debated, with no doubt a lot of lobbyists around; the anti-crypto crowd seems to be in control.

Similarly, Japan has also been constantly rejecting proposals for a BTC ETF.

Traditional players are continuing their business as usual and are probably more concerned about the tech stock market crashing than by a new entrant disrupting their business.

Emerging dedicated crypto investment funds

Crypto investment funds have conceded that 2018 was a difficult year for the market and their funds. Pantera Capital is one of them, calling for patience, and expressing confidence that "digital tokens will achieve real-world usage." Its ICO fund (with investments in 40 projects, see figure 8) lost 75 percent during the first ten months of 2018. As bad as this looks, it is still far better than the overall market. Galaxy, another fund, was down 50 percent over the same period, while the management explained that "the asset classes show signs of maturing."

It appears that these actors are actively refining their approach by distinguishing the various types of crypto-assets, especially "utility" token assets relative to pure cryptocurrencies. This move is evident and sensible; they are taking advantage of the bear market to properly position their funds to attack when a positive trend re-emerges.

While some crypto funds have reported gains by trading short-term trends, it appears that crypto funds have taken very few "short" positions. This may be due

FIGURE 8: TOP 20 INVESTORS IN THE BLOCKCHAIN INDUSTRY
NUMBER OF CRYPTO-COMPANIES INVESTED IN VS. SHARE OF TOTAL PORTFOLIO

SOURCES: BQINTEL; CRUNCHBASE

to a lack of supply (owners unwilling to lend), or lack of shorting facilities on trading platforms, but it most likely reflects faith in the long-term success of the economic or business models of the various tokens, and that the market may be approaching the bottom.

And, of course, in the current market context, small and less robust funds have been driven out of business, earning no income and, also, suffering the loss of their subscribers.

CONCLUSION ON CRYPTO ECOSYSTEM CASHFLOWS

Where is the money that is entering the crypto sphere likely to come from and where is it likely to go?

- Miners that are still operating are not likely to sell their crypto-assets at the current prices if they can avoid it. They are likely to mine as an investment from now on. Exchanges are in a similar situation, even more so considering that they do not need the money in the short or medium-term.
- The prices are now almost low enough for whales to re-enter the market at a significant discount. This may prevent the market from falling much further.
- At the same time, it is too early for retail investors to return, or for institutional investors, who are likely to shortly face an economic downturn.

So overall, from this analysis, the conclusion is, there is no urgency to act, even on BTC, regardless of the soundness of recent and near-term technological progress.

Some studies claim that in recent months gold has been favored by investors at the expense of cryptocurrencies. If true, that would mean that when these return, gold may suffer.

INVESTMENTS AND USE CASES BY INDUSTRY

Currently, start-ups are overall struggling in all areas, while consortia of companies are at work, making slow but continuous progress with dedicated resources. Each in their own sector, these consortia are thinking and developing "coopetition" frameworks as well as value and information exchange infrastructures. Their progress, successes, and difficulties should be closely monitored.

Some elements relevant to this discussion can be found in the section reviewing tokenized assets (e.g., real estate, refer to "O—Asset ownership", page 23)

INVESTMENT IN DLT TECHNOLOGIES

According to IDC (International Data Corporation), spending on blockchain is projected to continue growing exponentially, increasing from 0.8 billion USD in 2017 to 1.5 billion in 2018, to reach 12 billion in 2022. The US and then Europe will account for the largest spending, followed by China and Japan. In the same study, spending will be led by the financial sector. Manufacturing and retail sectors are also reported to be increasing their investment by 82 percent annually.

What this says, at the very least, is that corporations have not been deterred from continuing to invest in the technology and the development of related applications.

Start-ups also continue to receive funding. However, regardless of the current dynamic of ICOs, there is an important phenomenon related to ICOs issued in 2017 and early 2018: funds were raised in cryptocurrencies (BTC, ETH, etc.), and if the teams have not converted or hedged these financial positions, they are now sitting on one fifth to one tenth of their initial capital. While this hedging and spending on development has no doubt placed downward pressure on crypto markets, the actual funding of these initiatives must now be problematic for their executives.

BANKING

Banks were among the most active in trying PoC, with most of them starting early. As very few DLT-based systems are currently in production, it can be inferred that disillusion dominates blockchain teams within banks.

There are a number of ways in which the banking sector can be, and is, impacted by the inception of DLT. As we saw in another paragraph, there are many services needed for the custody of cryptocurrencies, including revenue management and payment itself, and most will probably be proposed by new kinds of banking actors. The impression we have right now is that large banks are turning to blockchain because they are obliged to. They found a couple of applications while optimizing their back-end functions, and their boards are probably relieved that it was all that needed to be done. Some go a step further by proposing a cryptocurrency brokerage service or tokenizing funds, in the most extreme cases. But there is no doubt that only start-ups that are native to the business will be able to propose disruptions comparable to the service that DLTs provide. Today's banks are just too cumbersome, have too many employees to pay, and are dependent on too many legacy systems, which they will never manage to decommission. Even if their inter-

bank settlement process is more efficient and faster, this will never improve their actual customer service.

Below is some relevant XRP news in banking:

- New partners continue to join the XRP network. The Euro Exim Bank is now using Ripple to provide financial services for export and import companies, for cross-border settlements.
- Ripple has invested 15 million USD in a Swiss producer of physical wallets (Tangem), as it has identified this as a key element in promoting the usage of cryptocurrencies; XRP in particular.
- One argument that is often quoted is that even if Ripple closes as a company, the XRP network will continue—SWIFT cannot say the same. And indeed, it appears that XRP is taking over from the SWIFT system. Today, this is the most obvious application of blockchain.
- The XRP community is also particularly active on social networks. This may indicate confidence, as this cryptocurrency has been resisting the downturn better than most in the past few months.

In other updates, Jerry Yang, co-founder of Yahoo, described blockchain as a "natural technology for banks and trading." He predicted that "if you look at US institutions and banks, the kind of infrastructure that is being developed has long-term implications. For the technology to succeed, the question is, can trust be built? That can open a huge number of doors."

At TenX, after Julian Hosp stepped down from his CEO position, payment cards were at last shipped to customers.

HSBC claims to have settled three million foreign exchange transactions and made payments worth 200,000 USD using DLT—a shared permissioned one. They claim that this use case is one that would not have been possible without DLT, and for them, it is a first of its kind. Regardless of whether this claim by the bank is correct, it appears that blockchain is finally being deployed full-scale in a company that is now benefiting from streamlining its processes. This is an example of a DLT-based solution performing better than available alternatives. Interestingly though, this is an accounting application, rather than a monetary application.

Spending on blockchain is projected to continue growing exponentially, increasing from 0.8 billion USD in 2017 to 1.5 billion in 2018, to reach 12 billion in 2022.

ASSET MANAGEMENT

Tokenization of assets is promising field with a potentially considerable impact on the asset management sector. Refer to "O—Asset ownership", page 26, for further details.

INSURANCE

We typically hear people saying, "Blockchain will not, in the foreseeable future, be replacing current insurance technologies wholesale; it's far more

likely to be used as a transport layer to move existing portions of policy administration data into a more efficient, accurate, and selectively shareable format." This means that, as in banking, the insurance industry is viewing blockchain as a means to improve the efficiency of their back office, as an additional layer in the architecture of their information systems, and in no way will they allow access to customers. While this approach of hiding the technology is correct, as the consumer does not necessarily care how the service is delivered, one does wonder if burying DLT so deep, as a framework, in a company's existing processes is not a little too easy for them, with respect to the disruption potential. And so, we still believe that suitable start-ups may arrive and conquer the market with packaged and easy-to-use smart-contracted insurance policies, where customers will have much more direct interaction with the underlying smart contract.

An illustration of the first phenomenon is RiskBlock Alliance (a consortium of more than thirty insurance companies), which is expanding its activities in Canada. In November, RiskBlock announced it would also chair blockchain standards for ACORD, the global standards-setting body for the insurance industry. The goal of RiskBlock's participants is to boost efficiency and reduce fraud. They are working on two insurance-based blockchain applications: (1) a "proof of insurance" application which shows whether customers have paid their premiums and are eligible for benefits, and (2), a subrogation tool that helps collect member payments and improve claims processing and accounting. The subrogation tool could help those filing claims to get paid faster through the use of smart contracts that automatically disburse funds after the insurance company has the proof of loss needed to process a claim. The whole framework is called "Canopy." B3I is also engaged in a partnership with RiskBlock.

We still believe that suitable start-ups may arrive and conquer the market with packaged and easy-to-use smart-contracted insurance policies, where customers will have much more direct interaction with the underlying smart contract.

An example of the other aspect is Etherisc, which has developed smart contract tools to create insurance policies on Ethereum. One of their applications, FlightDelay, enables users to obtain insurance against the risk that their flight will be delayed or canceled. Individuals purchase the insurance policy using a credit card, and, in the event, their flight is delayed by forty-five minutes or more, they receive an automatic payment without the need to submit a claim. Another application allows Puerto Ricans to insure their homes for up to $5,000 against the risk of hurricane damage. Under the policy, owners receive an automatic payout if their homes are damaged by a hurricane, as confirmed by an agreed-upon weather source. The developers of this policy are currently seeking investors to underwrite the risk—and this could very well be a huge roadblock that big players in the insurance sector will use to dominate the market.

SUPPLY CHAIN

The difficult path toward functioning traceability and a supply-chain ecosystem implemented on DLT-based platforms slowly continues. IBM's Hyperledger is focusing especially on this use case.

In particular, the shipping industry's development of solutions continues. The Israeli firm, Zim, has reportedly opened such a platform to all clients (in selected trades). The city of Veracruz in Mexico is also claiming to have switched operation to a DLT-based platform.

Ford has announced that it is tracking the origin of cobalt—a metal used in the production of batteries and is in high demand because of the ramping-up of

electric car production—thanks to blockchain. As 60 percent of the world's cobalt is mined in the Congo (DRC), often from inhumane child labor practices, an immutable audit trail of the supply chain from mine to smelting to shipping to Ford's factories has been implemented. Data providing evidence of the cobalt consistency throughout the process are to be recorded on the blockchain, thanks to smart contracts. However, maintaining a safe and reliable proof of the consistency of the metal during its entire journey is not easy. In the end, what will matter to the industry is being able to certify that materials used in production were from an ethical source, regardless of the actual cobalt (or commodity). Eventually, processing certificates of other key actors will be on the way.

Overall, big corporations are very interested in using blockchain in logistics and supply chain. Philip Morris wants to use blockchain to fight the counterfeiting of cigarettes. Nestlé is searching for ways to guarantee the origin of the cocoa used in its chocolate business.

Many start-ups are into the development of the solutions, platforms and IT of DLT infrastructure. It appears that fresh food product traceability may be a field where successful applications are the first to emerge. The availability of complete information about the origin and processing of food is today a "nice-to-have" feature that most people do not thoroughly check, but maybe with wide-scale availability, enhanced accuracy, and unquestionable reliability, it could become a point of difference.

It is crucial to highlight here that blockchain will in no way create miracles in traceability. Of course, the availability of a high-level tracking system is essential, but this only moves the weak point to other elements of the value chain. Humans, or robots controlled by humans, are still going to be responsible for entering data into the system. Regarding smart contracts, immutability can apply to errors or fraudulent information uploaded. Employees who are authorized to input the data can still be corrupted, or the goods can be physically substituted, or sensors can fail on the journey from production to consumption.

INFORMATION AND TELECOMMUNICATIONS

The Carrier Blockchain Study Group (CBSG), which includes worldwide telecom companies (from the UAE, the US, Taiwan, Japan, etc.) is aiming at developing an innovative blockchain platform specifically designed for telecommunications providers. The goal of the group is to provide telecom members and their users with different services, such as secure global digital payments, personal authentication, internet of things (IoT) applications, clearing and settlement, and other services, using blockchain technology.

SOCIAL NETWORKS

The question of whether Facebook will issue its own cryptocurrency is still open. Apple Pay and others that are taking steps into banking (such as GAFA) have been identified by large banks throughout the world as their greatest threat; as Facebook has not yet entered this field, a built-in crypto for WhatsApp, Facebook Messenger and Facebook itself is quite possible. Reports indicate they are working on a stablecoin and to do so they are recruiting all the DLT engineers they can find—reportedly a team of forty people led by an ex PayPal executive. India might be the target market to do exactly what WeChat did in China. However, some believe that to succeed Facebook would need what it lacks today; consumers' trust.

ENERGY

The U.S. Department of Energy has announced federal funding of up to 4.8 million dollars for universities working on R&D projects, including those related to blockchain. In July 2018, the department also awarded a grant of nearly $1 million to Colorado-based blockchain start-up, Grid7, in a move aimed at advancing the development of a decentralized energy grid.

Iberdrola, from Spain, is among the latest actors claiming to track so-called renewable energy from

production to consumption. The company is assessing the feasibility of delivering 100 percent renewable-sourced energy to its customers. The beneficiary of the experiment has been Kutxabank, with offices in Pais Vasco and Andalucia under the Caja Sur brand.

TRANSPORT

Initiatives to develop and use a common infrastructure across the shipping industry are emerging, in what can be considered as a typical case of sectorial "coopetition." This will no doubt be very interesting to monitor, as it is likely to be adopted by other industries (e.g., health care, distribution, and energy).

Initiatives to develop and use a common infrastructure across the shipping industry are emerging, in what can be considered as a typical case of sectorial "coopetition."

The Maersk-IBM initiative in the shipping industry (named "Tradelens") is supported by some major actors, including harbor authorities. Twenty-plus ports have joined, one of the latest being Algeciras in Spain. The network has now taken the name, Global Shipping Business Network (GSBN). Still, it remains to be seen if Maersk's competitors will join the movement on this infrastructure or if they will try to build their own. CMA-CGM, for example, is still considering how it can enter the domain.

The "Blockchain in Transportation Alliance" (BiTA), which was founded in August 2017, is gathering steam as members continue to join (500-plus members in twenty countries) from a variety of industry sectors, including freight, transportation, and logistics. The Alliance's members "share a common mission to develop a standards framework, educate the market on blockchain applications and encourage the use of those applications." This is another example of a consortium trying to organize itself, and one that will be interesting to monitor.

HEALTH CARE

Initiatives for managing personal health data, with users controlling the access permissions, continue to be discussed. CoinHealth is considering rewarding healthy behavior, thanks to wearables, which enable patients to earn rewards based on their measured activities. Some start-ups, such as MedCredits, even envision that telemedicine can be delivered on such a platform, with information being sent by the patient and the medic being able to send back a diagnosis, depending on images and a description of the symptoms.

In the US, the Drug Supply Chain Security Act requires the pharma industry to be interoperable; this means that when a drug passes from one party to another, there needs to be a way to record it. Blockchain is a natural candidate to deliver that.

Collaboration Hub for Life Sciences, a consortium of pharma companies, has partnered with SAP to fight the counterfeiting of drugs. This is both a supply chain and health care sector application, and another initiative that documents all steps in the production and shipment of a product. However, it seems that the ultimate destruction of the token (representing the drug package) is missing in the process, as otherwise it can easily be reused by counterfeiters.

ADMINISTRATION AND POLITICS

Litigation: Legal actors are looking into smart contracts because they realize that they may have to deal with these in the near future when working on cases, as the legalities of contracts can and do change.

Paradoxically, the main concern of legal professionals in this regard is the potential shrinkage of their revenue streams caused by the inception of DLT-based information systems. That is because smart contracts may eventually resolve much of the problems that, until now, have required lawyers to battle in the courts.

Legal records: Washoe County in the US state of

Nevada is offering digital marriage certificates stored on the Ethereum blockchain. A similar technique is used for birth certificates.

Voting: In South Korea, a system called K-Voting, built on blockchain, is being offered to small democratic communities (universities).

GAMING AND ENTERTAINMENT

In general, compared to centralized gaming "worlds," decentralized gaming platforms allow users to own their virtual asset of the game, and trade them on the platform. This enhances safety and provides all other characteristics of DLT tokens.

A promising example of a decentralized collectible dueling game that has been recently launched is World of Ether—that exists inside the Ethereum Virtual Machine. The game focuses on the collection, breeding, and fighting of monsters. Each monster is stored inside a contract and referenced by the platform. This appears to be a more elaborate attempt than Cryptokitties to have a gaming ecosystem exist on the blockchain—Cryptokitties which is still alive; however, with only a couple of hundred active users per day.

DecentraLand (still on Ethereum, and which ICOed in the second half of 2017) is an interesting attempt. The team is building an ecosystem of games with the aim of capturing value from this ecosystem through the appreciation of the MANA token. The ecosystem is a "virtual reality platform where users can create, experience and monetize their content and applications." The team builds the "metaverse" from Snow Crash; parcels of land are sold to users who can build a 3D universe of their own. The money within this world is the MANA, and the details of land ownership are also well maintained by a smart contract. This is, without doubt, a very interesting use case that is worth monitoring.

SOCIAL WELFARE

The most high-profile example of blockchain being used for social good comes from the United Nations World Food Program. It has switched the processing of spending accounts by food-aid recipients onto blockchain at its Za'atari refugee camp in Jordan. The camp's 100,000 residents access their accounts using iris scanners at food store checkouts, which confirm their identity and then reconcile the bill against their family's account using blockchain. The system has enabled the UN to exclude banks from these transactions, thereby reducing its processing costs by 98 percent, resulting in savings and the ability to deliver more humanitarian aid.

At the frontier between banking and charity is the effort by NGOs and blockchain start-ups in South Asia and Latin America to use blockchain to offer microloans to small businesses that don't have access to the existing banking system or face punishing interest rates.

On a more optimist initiative, "Indigen" blockchain was launched with the objective of protecting indigenous culture. As an ERC20 of Ethereum, with proceeds from the ICO serving to fund charity projects in developing countries, holders of the predetermined number of tokens will be entitled to receive rewards as dividends from future projects. However, whether remote and illiterate communities will embrace a specific cryptocurrency remains to be seen, let alone the clarity of where the dividends originate from.

TRENDS BY CRYPTO-ASSET CLASS

In the previous Quarterly, we introduced the concept of "Consensually Accounted Assets" (CAAs), in an effort to classify all the various kinds of available cryptocurrencies and DLT tokens, and to give a general definition and terminology to all the units of an account bearing value managed on a distributed ledger.

The CAA concept came as a follow-up on previous observations we made on utility tokens, published in our Q3 2018 edition.

Regulatory bodies, as well as traders, struggle to categorize these objects appropriately. The terms "cryptocurrency" and "coin" are hardly applicable to tokenized assets; and "token" does not describe accurately other cryptos like Bitcoin and Ethereum, amongst others. Not to mention that some are native to a DLT and some others are built on top of a native DLT.

We've received some comments that a more robust term would be Consensually Recorded Assets. And thinking about it further, a similar misuse of language has also led to the "crypto-asset" term. For the time being, and in the following sections, we will be using CAA and crypto-assets interchangeably in their broadest definition.

CLASSIFICATION AND ANALYSIS OF CRYPTO-ASSET BY FUNCTIONALITY

We introduce the concept of "crypto-asset class" classifying crypto-assets based on their final usage, functionalities or combination of functionalities.

These are summarized in the table below:

We introduce the concept of "crypto-asset class" classifying crypto-assets based on their final usage, functionalities or combination of functionalities.

The subsequent paragraphs offer comments and analyses on the identified crypto-asset classes, as introduced in the previous framework.

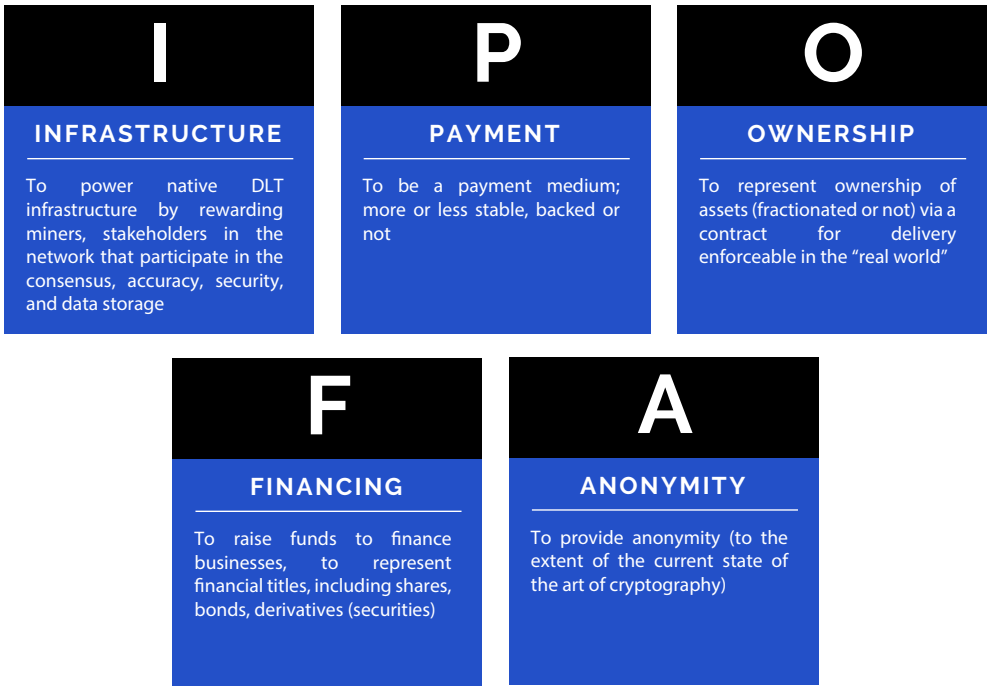
I—INFRASTRUCTURE FUNCTIONALITY

Following Cardano, EOS, Tron and other Zilliqas, there is no shortage of creative projects that claim to be a better alternative to Ethereum. They claim to differentiate on scalability (throughput rate), the consensus mechanism, management of private data, built-in KYC, and other compliance issues, with some that include identity management.

Not all of them are deployed DLTs or listed on coinmarketcap.com. Among those we have come across lately, it is worth mentioning a few:

DFINITY: "The Internet Computer," i.e. "a decentralized public cloud

MAJOR DLT TOKEN CLASSES



designed to host the next generation of software and services." The whitepaper describes a 4-layered consensus mechanism, relying on a verifiable random function decentralized among the nodes to elect the block's validation leader on the blockchain itself. The real innovation is the introduction of a 4th layer, to notarize information: by not requiring full network consensus at this level, they claim that this top layer is very responsive and can scale up.

Concordium: "Designed for business"; this Swiss-based foundation and the independent company relies on substantial cryptographic expertise, mainly from Aarhus University in Denmark. The infrastructure that Concordium built aims to address business requirements, in the sense that anonymity is eliminated, but the privacy of transactions are allowed. Regulatory compliance is built-in (KYC, AML, and revocable privacy). The consensus mechanism is based on a refined implementation of PoS and includes a finalization mechanism.

All these projects look very promising, taken individually. However, there are many competing projects, and

unfortunately, the success of infrastructure does not depend solely on its technical performance. In the forest of all the projects currently making noise, to get traction a given infrastructure must rely on good marketing and communication to build a community, to convince some proof of concepts to develop, and wait for systems to be put into production on it.

More than ever, the race to become the ultimate decentralized-applications IT infrastructure is on.

Enthusiasm and traction around a given DLT "infrastructure" depend heavily on its capacity to build an enthusiastic and working community around it and using it. While Ethereum is the clear winner at this game, we wanted to explore the size of these developer communities, and maybe characterize them.

A community is typically composed of:

- Developers of distributed ledger client software that agree on the protocol and its evolution;
- "Investors," i.e., speculators, arbitrageurs, market makers, and liquidity providers of the underlying cryptocurrency;
- Miners, where applicable;
- Developers of decentralized applications;
- Users of decentralized applications.

Ultimately, everyone needs to make a living. Developers of decentralized applications are likely to continue trying to get paid in the ecosystem that they create on top of the infrastructure. The application users will not care much about the underlying system that they will not even see.

The valuation of an infrastructure crypto-asset is therefore derived from either or a combination of the following: the cost of secure execution of applications and the monetary turnover and number of participants willing to rely on it for payment and value transfer.

By simple reasoning, we can infer that, if the cost of secure execution is higher than running a central database, then people will not use it; and specifically, scaling is about consistently reducing this cost. So, while an infrastructure may have potential, it may be quite limited. For example, consider Amazon Web Services. The company makes money, with an annual turnover estimated at around 50 billion dollars. However, if a crypto-asset is used for these transactions, and were turning over half the issued tokens each week, the monetary volume necessary in the ecosystem would be around 2 billion dollars; Ethereum is already valued at much more.

So, let's be clear; the secure execution of applications is not the primary factor to consider when valuing the infrastructure of crypto-assets, even disregarding the question of clonability of the protocols. Such crypto-assets are likely to earn value only if the users of the platform (at the lowest level, not the DApp level) use it as a vehicle to transfer or store value. In turn, this will only be possible if volatility declines. And if it does, then, of course, the more users, the greater the community, and the greater the potential for growth in value; in which case the turnover of fiat currency will be threatened, which is in the range of tens of trillions of dollars.

It turns out that the intrinsic value of an "infrastructure" crypto-asset will have a base value and an actual exchange value that remains quite volatile, preventing it, in the short term, from leveraging its real valuation engine: the monetary volume necessary for settlement (automated or not). Of course, if we envision that the tokenized fiats (or tokenized gold, or tokenized bitcoin) are going to be the currencies used on these networks, then, in the end, the community does not matter a great deal; Ether, Cardano and the like will be of little interest and value after all.

P—PAYMENT FUNCTIONALITY

This is the case for tokenized securities that are liquid enough to be used for daily settlements in businesses. However, collateralized crypto-assets to be used for bulk payments look quite far away, and a range of services will need to be

proposed before this is achieved.

Utility tokens are still a contentious class of crypto-asset. Despite their heterogeneity, the vast majority will fail due to the platforms, DApp, etc., not being built, or not being successful; but some teams might end up launching a distributed service where the crypto-asset will be alive and continue to exist. Such cases are highly speculative, of course, and each one will be specific, but a case for being good investments can still be made for some of these.

O—ASSET OWNERSHIP

Tokenization of assets is a whole subject by itself, and many of these can be readily used as alternative stablecoins. The following paragraphs offer a review of this space by asset class:

Real estate

The use of blockchain in the real estate business has gathered momentum lately since DLTs propose to solve the problem of large capital requirements, illiquid investments, third-party fee-grabbing intermediaries, and slow transaction times. Importantly, in addition to offering "digital shares" to investors, it can provide smart contracts, thereby automating payment of income for property owners.

A Consensys venture Meridio is addressing this segment. Their track record includes the tokenization of a building in Brooklyn. They list the advantages of their solution: (1) land title and deed recorded; (2) property sale and title assignment; (3) tokenized property ownership; (4) investor/tenant identity verification; (5) payment and leasing; (6) real-time accounting.

IHT Real Estate is an initiative that claims to tokenize real estate properties, offering individual investors an opportunity to purchase an interest. BitRent is another venture that collects and redistributes revenues from the features that are rented.

Commodities (including precious metals)

The demand for tokenized gold has increased, as people look for crypto-based safe havens. For instance, the capitalization of the Digix Gold Token market has increased linearly to 4 million dollars, which is still relatively small.

Many other actors are entering this sector, including Eidoo from Switzerland and GoldMint from Russia.

Royal Mint, from the UK, has been prevented by the government from selling blockchain tokens representing physical gold.

The valuation of an infrastructure crypto-asset is therefore derived from either or a combination of the following: the cost of secure execution of applications and the monetary turnover and number of participants willing to rely on it for payment and value transfer.

Securities

Of course, venture capital is the most immediate application, with a large appetite from start-ups as well as from investors and, especially in DLT-related fintech. We have already highlighted in a previous issue of this Quarterly, the extent to which this is changing the business model and jobs of PEs and VCs.

The adoption of STOs is gaining momentum, but it remains quite sporadic in the overall landscape: only a few dozen per month—although increasing exponentially. There is no doubt though; this business is headed for mainstream success in the short to medium term. But for the moment, burdensome regulatory requirements seem to be still discouraging small companies from going that way, while larger companies, due to their conservative CFOs, are so far, not diving into the pool either.

A whole ecosystem is in its infancy here. There are some asset tokenization platforms; some exchanges ("official" or private) that will specialize in security tokens; some

funds and investment bankers will package STOs into funds, shares, and derivatives; and some analysts and rating agencies will integrate them as well. We see a lot of enthusiasm and bullishness on the part of tokenization platforms and exchanges to push the adoption rate of STOs.

ERC20 standard from Ethereum is adopted by two-thirds of securities tokens, with Polymath's ST20 accounting for 25%, and the rest split between EOS, Waves, and others. ERC1400, a new Ethereum standard, has been specially developed to support securities tokenization.

Loyalty program points

In July 2018, Singapore Airlines started a tokenization program (KrysFlyer) for its membership miles, thanks to a digital wallet developed in partnership with KPMG and Microsoft. The airline is onboarding retail partner merchants to accept the token in Singapore.

Artists or athlete career

SportyCo, a platform that enables the public to bet on the career of athletes seeking funds, collapsed since its ICO one year ago.

Collectibles (art, luxury, and historical objects)

Everledger, which, some time ago began placing diamonds as non-fungible tokens on Hyperledger, is now expanding its concept to wines. Traceability is systematically highlighted in their use cases.
LVMH is working with VeChain; again, mostly with traceability in mind.

Maecenas tokenized, on Ethereum, and sold a 31.5% stake in Andy Warhol's painting, "14 Small Electric Chairs", to bidders who could pay with bitcoin, ether or its cryptocurrency, ART. In a survey, the European Fine Art Foundation found that 75% of auction houses, and 33% of intermediaries, intend to offer some blockchain technology within the next five years.

The adoption of STOs is gaining momentum, but it remains quite sporadic in the overall landscape: only a few dozen per month—although increasing exponentially.

F—FINANCING FUNCTIONALITY

CAAs are pure tokenized financial instruments; bonds, stocks, and all kinds of derivatives. They all have a value that can be estimated with traditional approaches and are of little interest for us here other than highlighting the fact that the support for these securities is poised to change and with it the jobs of many financial market professionals.

A - ANONYMITY FUNCTIONALITY

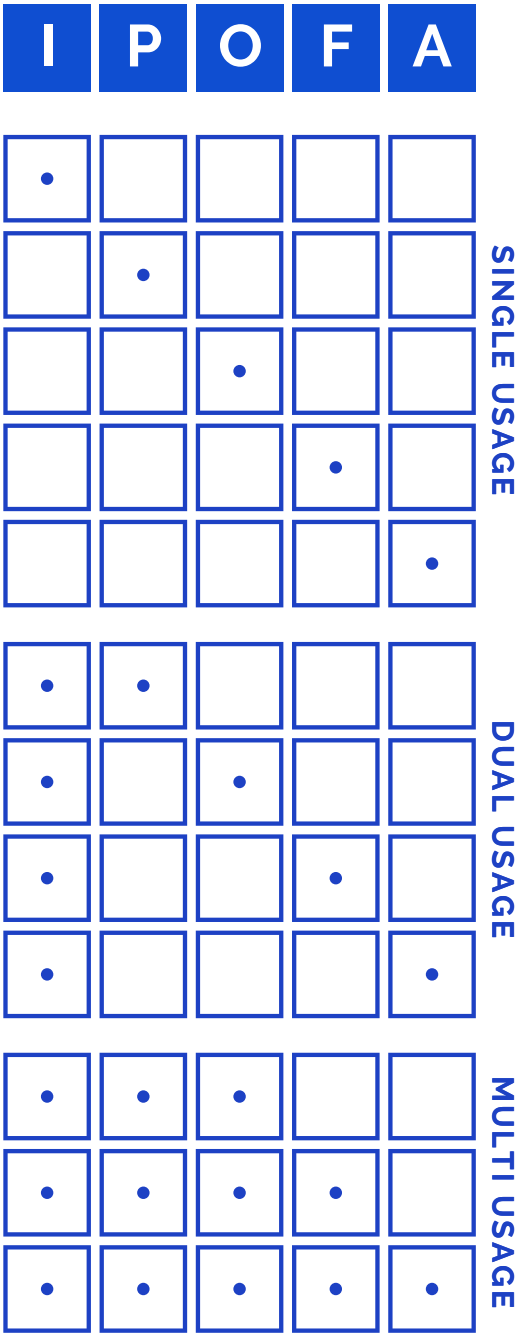
KYC/AML/CFT can hardly apply on these, and as such, we can expect that regulators will clamp down on them, while they will be favored by cypherpunks and their descendants.

Again, MimbleWimble-based distributed ledgers are getting traction in this field.

SUMMARY

In summary, all the functionality can be allocated single-, double-, our multi-usage features.
With five major functionalities usable to classify CAAs, we end up with a 5-dimension matrix; which is not very convenient to represent nor to navigate into. But since we have only two positions in each dimension, we have just 2^5=32 possible categories; and some of them are going to be irrelevant or non-existent (the blank one).

We will keep this matrix updated as we continue with our Quarterly reviews.


I P O F A
SINGLE USAGE
DUAL USAGE
MULTI USAGE

	I	P	O	F	A	
1	•	•				Bitcoin, Litecoin
2	•	•		•		EOS
3	•	•			•	Monero, Dash, Zcash
4		•				Ripple
5		•	•			DigixGold, TrueUSD
6	•	•	•			Ethereum (actual state)
7		•		•		TenX
8				•		Gnosis

MAINSTREAM TOKENS

	I	P	O	F	A	
9	•	•	•	•		Ethereum (initial whitepaper)
10		•	•	•		Liquid pre-sales (e.g., wine)
11			•	•		Illiquid pre-sales (e.g., art)
12			•			Notarization services
13		•		•	•	Liquid fungible financial titles
14		•	•		•	Liquid fungible tokenized assets

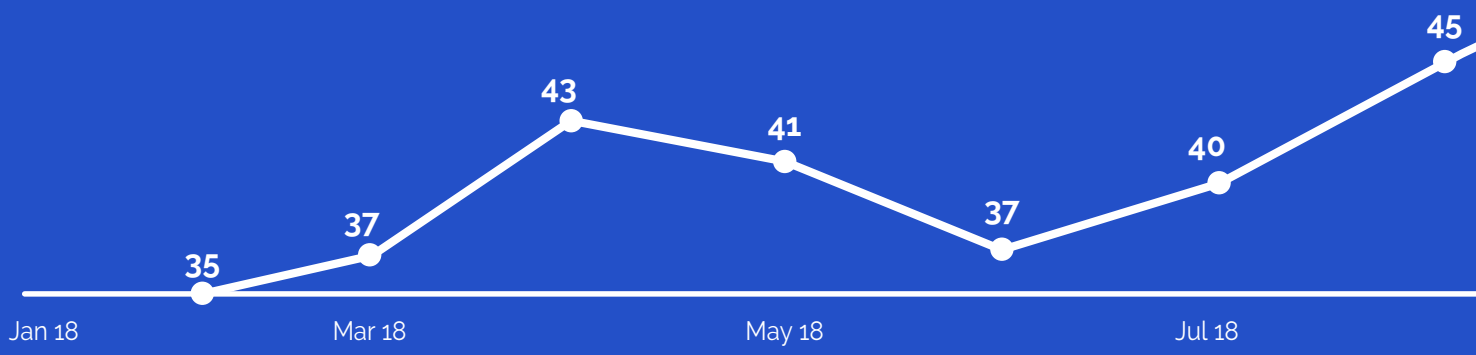
IN-DEVELOPMENT TOKEN

	I	P	O	F	A
15	•	•	•	•	•
16	•	•	•		•
17	•	•		•	•
18	•		•	•	•
19		•	•	•	•
20			•	•	•
21		•	•		•
22	•			•	•
23	•		•	•	
24	•			•	
25	•		•		
26	•				•
27				•	•
28			•		•
29		•			•
30					•
31	•				
32		•			

UNDISCOVERED TOKENS

A FOCUS ON BITCOIN

FIGURE 9: BITCOIN'S DOMINANCE IN THE CRYPTO SPHERE
% OF TOTAL CRYPTO-ASSETS MARKET SHARE



SOURCE: COINMARKETCAP.COM

Cryptocurrencies are now more than ever all linked to bitcoin, so it is worth focusing on BTC to check the overall health of the sector and the likelihood of a trend reversal.

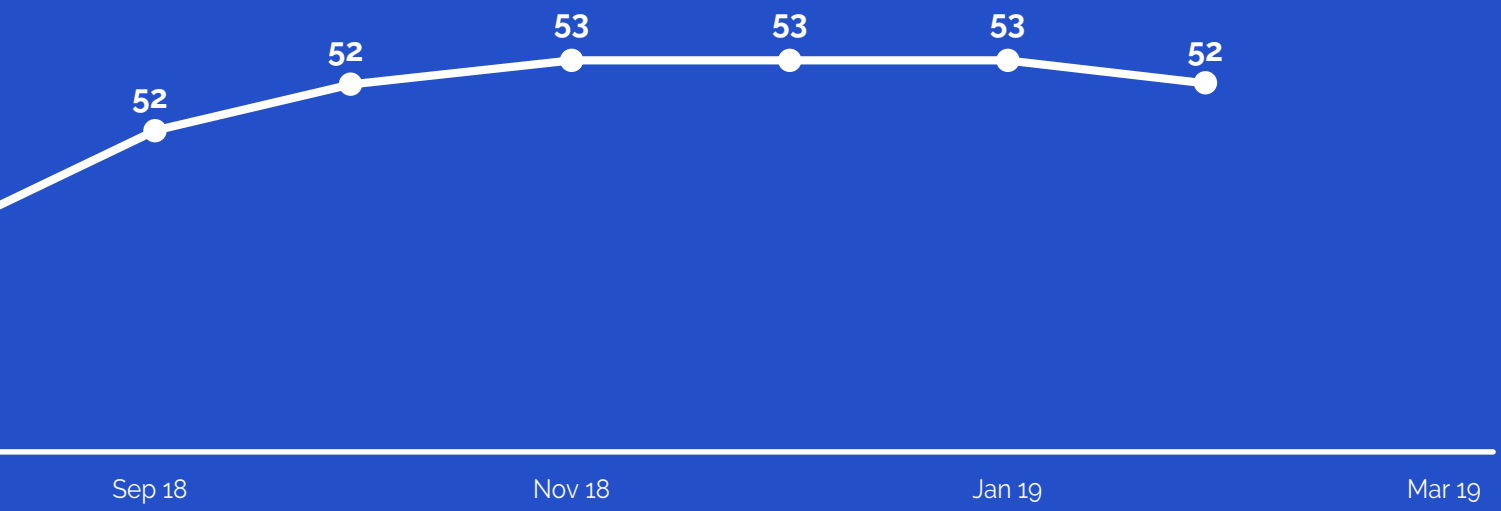
Bitcoin is incrementally claiming back the ground it lost to the emergence of altcoins throughout 2017. Its predominance had fallen as low as 30% and is now back to 55%. There are no indications that it will not continue to regain lost ground, and it is worth examining why.

Peer-to-peer money is still as cool as it was ten years ago. The value proposition is still to store, and exchange value using a means the government or large corporations do not control that. This view is still as attractive as it was in the beginning, maybe, even more, considering the measures regulators have taken to put more compliance pressure on exchanges (e.g., KYC)—thereby effectively ensuring a clear distinction between the "free world" and the constraint-laden, establishment-favored, tax-intensive world. More than ever, bitcoin is about providing freedom to whoever wants to conduct business without intermediaries or third-party surveillance. Therefore, cryptocurrencies that focus on anonymity have an exciting future; but as the legacy cryptocurrency, bitcoin is more than ever here to stay.

Almost unanimously, bitcoin holders and crypto pundits believe that a price bottom will occur in the first quarter or first half of 2019. However, even if this happens, prices would need to hold for another 9 or 12 months for this view to be confirmed.

Hereafter are some metrics on bitcoin's health:

- The hashrate has progressed from 18 Ehash/s in January 2018, to 40 Ehash/s one year later: this shows continued interest by miners, despite the profitability issues they face .
- Wallets containing anything from 100 to 1,000 bitcoins owned 23.3% back in September, whereas now they own 21.4% of all coins. Conversely, the five wallets containing anything



from 100,000 to 1 million BTC—which belong to crypto-exchanges (and their customers)—own today 3.3% of all coins, an increase from the 0.7% share in September.
- The average cryptocurrency payment in 2018 was 680 USD, while in 2017 it was half that, 340 USD.
- Bitcoin volume, expressed in bitcoin, increased drastically during 2018, as we saw earlier.
- Transaction fees over the network are back to their high levels.
- The number of bitcoin ATMs is said to have passed 4000 units, and the pace of installation is accelerating. ATM operators are currently living on the earnings from their business, which is already good progress.

A couple of other considerations:

- Some people have noticed that bitcoin's price witnessed huge increases on two occasions following the coin's block reward halving (in both cases, around a year after the halving occurred on November 28, 2012, and July 9, 2016). Whether it's related or not, the 4-year interval also corresponds to the inter-peak period of the price between 2013 and 2017. This may be an interesting fact to keep in mind.
- Bitcoin and its PoW consensus mechanism are still the best of what has been proposed in terms of security of the network to counter attackers. PoS scales a little more, but it is challenging to prevent new kinds of intermediaries overseeing the network. One should not forget that it all started to create a decentralized currency system.
- Even in the event of a 51% attack, the loyal bitcoin community would still be able to maintain a chain of valid transactions—but just.
- For scalability, one should note that it is always possible to tokenize bitcoin on another chain—paradoxical perhaps, but a potential solution, nevertheless.

Without a doubt, bitcoin remains "the king of cryptocurrencies," and its future seems as bright as ever.

LATEST ADVANCEMENTS IN DLT TECHNOLOGIES

It is still not clear which solutions will ultimately win widespread adoption, as far as scalability of the various current DLT alternatives is concerned. Some refinements appear to be gaining momentum, such as the MimbleWimble protocol, and zk-STARKs that are poised to replace zk-SNARKs. Also, DAGs seem to have received insufficient exposure up to now; but only time will tell which of these technical solutions will earn dominant implementation. As the example of Facebook shows, it is not always the best technical solution that achieves a monopoly.

To ensure further adoption of the various technical solutions, a user-friendly packaging is very much needed to allow the public to seamlessly enter the ecosystems.

In the following pages, we present a systematic review of developments in the technical aspects of DLTs. You will find updates on technological research and improvements in DLT infrastructures that build on previous in-depth descriptions and analyses of the critical issues. We will also explore topics that have not been thoroughly covered up to now in this Quarterly, such as the implications of quantum computing.

In this section on technical updates, we assume that the reader is up to speed with studies covered in previous Quarterly reviews.

CONSENSUS MODES AND GOVERNANCE

The consensus methods of DLTs largely determine the scalability of the infrastructure, and, in general, scalability features need to be implemented. Therefore, these topics should be discussed together.

Technical developments on consensus modes

Various teams are currently working on their implementation of PoS, DPoS, and PBFT, or a combination of the above, to improve scalability, rapidity and other features. We will cover some scalability aspects in this section. However, there is no breakthrough to highlight at this time. (Also refer to section "I—Infrastructure functionality" on page 23.)

This may be the time to cover a blind spot; even if it is not new. As yet, we haven't taken the opportunity to dive into the Federated Byzantine Agreement (FBA) consensus mode (used in particular for Stellar Lumens). Its specifics are interesting, and its impressive characteristics are worth looking at.

The FBA model (used in the Stellar Consensus Protocol), is an approach to the consensus that has nothing to do with PoW or PoS. This means that the network agrees on a statement if a majority of its participants agree on it; the threshold is usually 2/3 of loyal participants to counterbalance a

maximum of 1/3 malicious nodes.

With FBA, as opposed to Byzantine Fault Tolerant mechanisms, the list of validating nodes is not established in advance by a central authority. In FBA, anyone can join, and every node decides which other nodes they trust, which forms a "Quorum Slice." Quorum slices, by design, must overlap, together building the whole network consensus, and thereby gossip on positions by the node can spread across quorum slices.

To ensure further adoption of the various technical solutions, a user-friendly packaging is very much needed to allow the public to seamlessly enter the ecosystems.

In a synchronous distributed system—according to the FLP Impossibility Proof—at most, two of the three following properties can be achieved by the consensus method: fault tolerance, safety, and liveness.

Fault tolerance is the guarantee that the system will survive if a validator on the network fails at any time. Most consensus protocols choose fault tolerance as one of their preferred properties. The big tradeoff remains on the choice between safety or liveness as their second favored property.

Safety is the guarantee that nothing wrong will happen, like a fork. Liveness is the guarantee that transactions will always be processed. FBA favors security over liveness; whereas, in blockchains, liveness is favored. Hence forks are possible.

Periodically, the whole network goes through a cycle of validation. First, at the level of the Quorum slices, all participating nodes essentially go through continuous rounds of voting until they can agree on a statement. Once a consensus is reached in the quorum slice, voting then occurs at the higher level. Of course, every node maintains the same view of the ledger.

Consequently, transactions merely need to be passed to the network, and safety means that no confirmation time is required; this allows for fast transaction processing: in the range of 3-5 seconds. Another consequence is the removal of the risk of attack by considerable computing powers. The fee is reduced to the very minimum, which is mainly to prevent spamming the network; and therefore, not a lot of full nodes are running—due to lack of incentive.

Governance

All evidence points out that the governance of blockchains is going to be a growing concern. One indication of this is that Ethereum is delaying its Constantinople update, not because

the fix to the problem is not ready, but rather to have sufficient time to convince the community and to coordinate miners to ensure avoiding a hard fork.

But, as of now, this topic of tediously steering the blockchain protocol evolution is well below the radar, with scalability being the focus. Article writers and panelists in various discussions are identifying the issue, but only limited research efforts have been made to date.

Hard forks

In November we witnessed the fork of Bitcoin Cash, which gave birth to Bitcoin Satoshi Vision. Bitcoin SV claims to strive for address stability, scalability, and security. But for now, it hasn't changed much since the fork. Furthermore, they are somewhat self-contradictory in wanting to retain the original concept of bitcoin, yet wanting it to evolve.

SCALABILITY

Scalability in terms of transactions per unit of time

Bitcoin:

- Currently, 40% of transactions use SegWit - helping to decrease transaction fees. This is a failure of mass adoption of an easily implementable feature, but overall it is a minor consideration.
- The Lightning Network (LN) is gaining momentum: new records have been set in capacity over the network, namely over 500 BTC, over 5000 nodes, increasing steadily, and even more, channels are in the process of creation. To increase the adoption of LN even further, the community should concentrate on making the set-up phase easier. A few features are still under development to enhance the attractiveness of the Lightning Network. These include splicing to enable the size of channels to be adjusted after opening.
- The sidechain concept is competing with the Lightning Network. The most advanced implementation of it has been in development for three years at San Francisco's Blockstream, and is called "Liquid." As expected, users convert their BTC to LBTC, thereby totally pegging the new currency. The sidechain is a federated one, where partners (participants are big exchanges) are acting as third parties for each other. This is the fastest option, but bitcoin purists are not satisfied with it. It looks like we are witnessing the construction of efficient channels for—and within—a nascent industry about to replace banks.
- Meanwhile, as a side remark, Bitcoin Cash's 8MB block size has never been reached.
- Litecoin is also implementing the Lightning Network.

Ethereum

- The Constantinople hard fork has been delayed and is unlikely to happen before the end of February. A vulnerability has been flagged in the upgrade by a smart contract auditor, which required a rework. For details about the technical improvements included in this very significant upgrade of the protocol, refer to our previous Quarterly.
- The Ethereum Foundation has paid 5 million USD for the development of the Parity upgrade of the Ethereum node client.

Cardano is currently claiming it can handle several hundred TPS and is working to reach several thousand.

EOS has released an upgraded version of the code, which is 35% faster.

Stellar: As we have just seen in the previous paragraph, Federated Byzantine Agreement is very scalable and fast.

MultiVAC is a solution that has been progressing fast and is receiving increased exposure. The team describes it as a "high throughput, flexible public blockchain based on trusted sharding." By allowing nodes to accumulate their transaction power, they claim unlimited scalability for the network. A test in October showed 31,000 transactions per second for 64 shards. MultiVAC has the following features:

- The DApp designers can decide the tradeoff they want to adopt between decentralization, scalability, and security, rather than being limited to what the underlying platform provides.
- The sharding solution provides various dimensions of smart contract computation, including storage

and transmission of data.
- It uses Verifiable Random Functions (VRF) to establish in which shard a node is allocated, and which node gets to validate blocks.
- A Proof of Instruction Execution (PoIE) is implemented to eliminate the need for every line of code in a smart contract to have to execute on all nodes.
- Uses the physical discrepancy between computation and storage—existing in modern computers—to penalize malicious behavior and ensure security and efficiency.

Devvio: this initiative claims to be able to process 8 million transactions per second.

- Here again, the solution lies in sharding. The consensus mode is Proof of Validation. In short, on the blockchain's network (or shard), a validator is chosen randomly. It then gathers messages from the other participants in the network until reaching 51% of validators agreeing; the block is then passed to the blockchain, including the messages received from its peers.
- Devvio also claims that a transaction cost on their network is five orders of magnitude lower than on Ethereum.
- Every wallet is assigned on one and only one shard, and any transaction coming out of a wallet is processed by its shard. Then all the blocks from all the shards become inputs to a single shard, which handles all the cross-shard transactions.
- Of course, these performance claims have not yet been observed in real-life operation.

Unit-e: another group, mostly from the US and Germany, funded by Distributed Technologies Research (DTR, based in Zug) and Pantera, has been able to resolve the scalability issue for a globally decentralized payment network. The associated cryptocurrency is Unit-e.

- The group focuses on in-depth scientific research to achieve an increased throughput rate without sacrificing decentralization.
- They envision using PoS in an algorithm called Prism that would be "approaching the limits of what is physically possible in a blockchain."
- They are also researching a new sharding technique called PolyShard. The key being that nodes should not store replicated data; instead, they should store coded linear combinations of data, while still allowing for data recovery.

A significant effort is being made to ensure that Proof of Stake functions effectively, not the least being Ethereum's difficulty to switch from PoW to PoS. At this point, it is essential to mention the "Nothing at Stake" problem that exists in the PoS mechanism. The issue arises when two "forgers" (the equivalent of miners in the PoS consensus) arrive at the threshold that allows them to propose a block at the same time. In this case, a fork happens, and it propagates in the network. In PoW, miners will dedicate their effort to one of the two branches, and after some time, one of the competing blocks loses the race and is orphaned. In PoS, every person on the network may want a stake on both sides of the chain, so that they can ensure a higher reward for whichever block ends up winning. And then, the issue is that if almost all forgers do this, say 99% are on both ends; the remaining 1% may eventually decide the fate of the chain. In this case, an attacker would pass a transaction to one fork in the chain, and join the other fork, causing it to win, and in the process allowing the attacker to spend their cryptocurrency again. However, doing this would ruin the trust in the chain and would also impair the value of the attacker's stake. In reality, this problem is not observed, and of course, modern implementations can effectively resolve this.

Scalability in terms of ledger sizes

Bitcoin's ledger is now reaching 200 GB. The progression is now very linear and is not regarded as a concern if it continues. The low scalability of BTC has the advantage of having a "manageable" ledger size.

MimbleWimble has potential: with this protocol, most of the transaction data can be eliminated over time, without compromising security. As transactions are verified by checking that the amount of input corresponds to the amount of output, storing the proof of input is enough. Ultimately, this results in unspent transactions. Note that this is all made possible because the total amount of tokens is known in advance.

CONFIRMATION TIME: FINALIZATION MECHANISMS

To prevent 51% attacks from rewriting the blockchain story, some of the newer projects have implemented a finalization mechanism when validator nodes sign the appended blocks. These mechanisms ensure the endorsement of the chain that is being followed and immediately discard any stale blocks that are not on the longest chain (called uncles). This, in turn, avoids waiting for several rounds to be sure that the transaction has been accepted.

INTEROPERABILITY

Barclays has organized a dedicated hackathon centered on finding ways to connect Ethereum with made-for-enterprise blockchains (e.g., Hyperledger). The panel of judges included representatives from Barclays, UBS, HSBC, and Santander.

Otherwise, technically speaking, there is nothing significant to report on this topic.

PRIVACY AND CONFIDENTIALITY

MimbleWimble

The implementation of the MimbleWimble protocol continues to progress, adding to the ecology of anonymity-oriented cryptocurrencies. Grin, which is community-funded, is gaining momentum, and another has debuted: Beam, run by a start-up with the intention of handing over operations to a dedicated non-profit foundation.

MimbleWimble looks, even more, promising the further one dives into it. As of early 2019, it has generated a lot of enthusiasm within the community.

Please refer to the previous Quarterly for a technical explanation on MimbleWimble.

A few additional remarks about previous comments:

- Transactions jump from node to node before being recorded, which increases the difficulty of identifying the wallet a transaction request came from.
- MimbleWimble does not require addresses, so people have to interact in real life to enable communication between their wallets.
- MimbleWimble cryptos are fungible because of its design.
- MimbleWimble also marginally increases scalability in throughput rate.

Also note that the elegance and lightness of the MimbleWimble solution are competing directly with the burdensome, cryptographically intensive solutions of Monero, ZCash, etc., due to the computing demand of zero-knowledge proofs, in particular. In MimbleWimble, unless you were one of the participants, none of the transactions in any given block will be recognizable to you. If you view a block, you will not see a list of transactions. You will see one big transaction, in which everything has been mixed and merged—all that is left are the "list of new inputs, a list of new outputs and a list of cryptographic signatures created with the dummy above outputs." This makes it more anonymous than Monero and the like.

MimbleWimble has potential: with this protocol, most of the transaction data can be eliminated over time, without compromising security. As transactions are verified by checking that the amount of input corresponds to the amount of output, storing the proof of input is enough.

Apart from traceability, which is sacrificed to obtain fungibility, MimbleWimble-based chains are likely to achieve bitcoin's goals better than bitcoin itself. Surprisingly, projects using this technology have had little exposure, and money continues to flow to protocols like Ethereum. This may change shortly, as the framework is clearly in place for Grin, Beam, and probably many others to come.

Zero Knowledge Proof

While zk-SNARK has been among the most popular topics of discussion in the debate around anonymity implementation in blockchains, its method has been refined in a new application called zk-STARK (Zero-Knowledge Succinct Transparent Argument of Knowledge). The differences and main

advantages of zk-STARK concerning SNARK are:

- It does not require a trusted set-up phase.
- It is less costly, thanks to the reduced complexity of the arithmetic involved; of communication interaction; of the prover task; and the verifier task. We are talking here of an order of magnitude improvement, not just an incremental change.
- zk-STARK does not rely on private-public key pairing, and therefore it is not as vulnerable to the inception of quantum computing, as zk-SNARK is.

CRYPTOGRAPHIC ROBUSTNESS—QUANTUM COMPUTING EVOLUTIONS

The race towards quantum computing continues, with IBM recently announcing the release of IBM Q System One, the world's first commercial quantum computer.

Regarding post-quantum cryptography, the following, in broad terms, is a summary of recent developments.

Hash functions are partially vulnerable. As for finding a primitive for a hash, quantum computing is likely to be very efficient. But returning an original document hashed is still impossible.

Symmetric cryptographic algorithms are still relatively secure as they do not rely on the integer factorization problem, the discrete logarithm problem, or the elliptic-curve discrete logarithm problem. Provided the symmetric key size is long enough, symmetric encryption is still valid. Mathematics shows that doubling the key size is required to have the same level of safety post-quantum as it was pre-quantum.

The problem is that blockchains do not rely on symmetric encryption, but on asymmetric encryption to sign transactions. Asymmetric encryption that will not be broken by quantum computing is largely still at the research stage. Possibilities that are explored to find problems not easily solvable by quantum computers include:

- Finite fields of multivariate polynomials.
- Error correction codes, where the private key is the matrix used to correct, and the public key is a randomized version of it. A cyphered message is then the message with some errors included in it. This method is proven to ask the attacker to perform a prohibitive amount of work while keeping the legitimate user's work limited. The issue is that the resulting keys tend to be very heavy, especially compared to classical pre-quantum keys.

To summarize, methods already exist to create pairs of private and public keys to allow cryptocurrencies to continue being operational, but with more complex keys to managing. Meanwhile, there is still hope of finding more efficient suitable problems to generate more manageable quantum-resistant cryptography.

VOLATILITY

Analysis of volatility

The volatility of cryptocurrencies has reduced considerably in the past year, indicating that more actors are entering the crypto market and contributing mechanically to more inertia in price movements.

The volatility itself is not bad; it is how people react to it that comes into question. Some actors do prefer higher volatility.

Stablecoins

As applications design and development continues, interest in stablecoins has increased. A need for a more stable vehicle—without the need to hedge the exchange rate—to automate the transfer of value by smart contracts over the blockchain becomes more and more evident. The actual usage of stablecoins to settle the automated transfer of value is yet to be generalized, but we can be very confident this will happen as part of real smart contract platforms being put into production.

Evidence of this interest can be seen by the release on the market of various simple fiat collateralized cryptocurrencies, which include Gemini's GUSD, SmartValor's tokenized Swiss franc, Paxos' PAX and others. The value of these tokens has progressed in the CoinMarketCap rankings, as they act as a reserve of value for investors, while volatile cryptos continue to fall further. All initiatives line up and happily go through audits in the hope of grabbing Tether's place if the USD-pegged cryptocurrency collapses.

Huobi has also launched HUSD, which is a basket of pooled stablecoins pegged to the USD.

While it is easy to tokenize fiat, (the creation of self-standing mechanisms to maintain the pegged value of virtual currency), the real challenge for a stablecoin would be to offer a mechanism for a floating value, not linked to a particular fiat, yet that is overall stable.

STANDARDIZATION

At the moment, the early maturity stage of distributed ledger technology calls for a broad exploration of all implementation alternatives.

Only when the various known solutions have consolidated to produce optimized versions will "de facto standards" emerge, thanks to wider adoption. Ethereum's standard token types are the first attempt at this.

SYNERGIES WITH OTHER TECHNOLOGIES

IoT synergy

As a review, this is how the IoT will use DLTs:

- Two devices want or need to exchange something, which could be information, a commodity, a parcel, or anything else.
- Both have to run the same decentralized application.
- One (or both) must acknowledge its counterpart's identification on the supporting DLT, thanks to direct communication (sensors, Bluetooth, scanned QR code).

The decentralized application will have the framework for the intended interaction; including:

- On-chain acknowledgment of the identification of the two objects.
- Choice of a range of services or interactions, a range of steps coded in the process to get data, and its confirmation between the parties.
- Escrow of exchanged crypto-value or information.
- Feedback from one or both parties proving that the potential interaction took place satisfactorily, thanks to potentially independent sensors acting as oracles.
- And finally, releasing information and crypto-assets, as expected.

When it comes to the challenges of technology, machine-to-machine communication faces three challenges that can be solved by DLTs:

- Transparency: when communicating, devices use encrypted data that is not easily auditable. So, until now you've had to trust that the application would handle the content of the communication appropriately (typically not sharing information you do not want to share).
- Longevity: communication up to now has passed through the vendor's cloud, and if the vendor goes bankrupt or stops maintaining the devices, then usage can be discontinued.
- Trust: over a conventional chain, payment details are handled sensitively by a third party.

Smart contracts address the concern of transparency, since the logs are public, and it offers longevity because the blockchain is not stoppable and can be trusted, thanks to the disintermediation offered by decentralized applications.

However, DLTs must solve scalability, offer fast response times and privacy of exchanged information before claiming to be suitable for the IoT.

THE MOMENTUM GAINED BY DLT ALTERNATIVES TO THE BLOCKCHAIN

Direct Acyclic Graph (Tangle)

To the crypto world, it may seem strange that DAGs have not had more momentum given their elegant solution to the scalability problem in the field of DLTs. As they do not rely on blocks, are asynchronous to a large degree, have no time diffusion issues, less mining waste, lower fees, and there are no debates on block size or block frequency.

So, if it is faster, cheaper, more decentralized, not threatened by quantum computing, and in theory, has no scalability limit, why have we not seen any sign of

supremacy of Hashgraph, IOTA, Nano and the like?

Here are some possible answers:

- Without getting into too much technical detail, the "gossip-on-gossip" protocol—which is the basis of the mathematical demonstration of the reliability of truth recording on DAG ledgers against attacks—assumes sufficient traffic of transactions passing through the system. Therefore, a relatively high volume of transactions needs to occur on the tangle to maintain its security constantly. In other words, the tangle approach is eventually more vulnerable to attack than a blockchain system.
- Today, to avoid this trap, tangles are implementing "witness nodes," sort of central coordinators that negate the true decentralization of the system. Yes, the famous trilemma holds still, but as a result, detractors of DAG claim that it is centralized.
- Timestamping cannot be guaranteed as it is with a blockchain.
- DAG solutions struggle to integrate worst-equipped, worst-located network participants. The near-instantaneous processing of transactions by DAG means that far-away participants face the risk of disproportionately unconfirmed transactions. This will prove to be a 'real-life' limitation to the effective scalability potential of DAG.
- There are comparatively fewer developers working on DAG than on blockchains, and the inception of the concept as a competitor to blockchain is relatively new; nobody had this family of solutions on the radar before IOTA emerged in mid-2017.

There is not the same "global state" on DAG implementations as there is on the blockchain, which ultimately prevents participants from checking a transaction against the complete ledger history.

- Firstly, this is because the ledger changes with each transaction submitted to the network, and does not get gossiped at a constant pace, depending on the connectivity of each participant requesting an operation.
- As DAGs are designed for a high throughput rate, the size of the ledger can rapidly explode, hence pruning is commonly used (snapshot sum-up of states by epochs), deleting the history of operations—this again weakens trust in what is recorded in the ledger and empowers nodes that take charge of pruning.

The takeaway is that, most probably, both blockchain and tangles will have their preferred field of application where they will perform better than others.

Corda, Hyperledger and similar DLTs

Corda has on-boarded ING. The insurance giant has decided to use the technology to help streamline its back-office. BNP Paribas and Deutsche Bank are also among large corporations adopting Corda. Hyperledger is constantly hitting the headlines, with IBM promoting it in every project they sell to their customers.

Otherwise, there is not much to highlight technically regarding these solutions.

CRYPTOGRAPHIC KEY MANAGEMENT ON PERSONAL WALLETS

Samsung, in addition to Huawei, is proposing built-in secure wallets in their high-end smartphones; this is logical competition arriving to challenge the market for dedicated hardware wallets like Ledger and Trezor.

Sirin Labs, a company that launched dedicating itself to serve the smart-phone-for-crypto segment, has released its first products, which are available to the public through Sirin Labs' physical outlets.

In the same vein, a Swiss luxury watch company (A. Favre & Fils) has advertised a watch that has a built-in cryptocurrency wallet.

MALICIOUS ACTIVITIES

Double spending—the 51% attack

A 51% attack occurred on Ethereum Classic in early January. It was spotted by CoinBase and consisted of double spending coins to the value of $500k. This has been repeated than in the following

days on several transactions.

It appears that Ethereum Classic is now the chain where the DAO hack is still considered effective; this chain is particularly suitable for hackers to continue attacking with confidence, knowing that the community is not going to work to reverse the hack.

The takeaway is that small blockchains with a less hashing power are very vulnerable, as there is always someone who can have more computational power than everyone else. This is even truer because, as coins weaken, they become easier to attack—as, in a bear market, hashpower is turned off.

The vulnerability is not limited to double spending: once in control, an attacker can easily use the power to manipulate prices and build a short position. This is known as the Goldfinger attack.

Thefts

The latest cryptocurrency exchange for being hacked is Cryptopia, based in Christchurch, New Zealand. The hack, which occurred on January 15th, involved a few million dollars. The interesting thing here is that the tokens concerned have been identified as having been transferred to Binance, which took the conservative step to freeze them.

This incident sets a very interesting precedent. Except for privacy-focused cryptocurrencies, it is evident that this safety measure can be deployed for all sorts of cryptocurrencies and is a feature that can be easily implementable in the legacy payment system. Note that even if the thieves are not identified—and they may very well be, and easily—then the proceeds of the theft should be refused everywhere, thus destroying the profit from the theft, making it pointless.

Scams

Anonymous cryptocurrencies continue to be the currency of choice for kidnappers, scammers, and other criminals.

"Fake impersonations," for instance, of celebrities, through the creation of fake social media profiles account for a growing number of easy scams. For example, in a fake twitter account for technology entrepreneur and billionaire, Elon Musk, scammers promised to give away a total of 100 ethereum (ETH) to US President Donald Trump's followers after they send 0.2 ETH to a certain address. This may sound absurd, but people constantly fall victims of such scams. An analysis shows that 468 scammers have collected more than 8000 ETH in this way.

Fraudulent investment funds and Ponzi schemes

During and after the crypto bubble of 2017, an important number of crypto investment funds were launched. Some were not very well managed or made promises based on the astonishing returns observed in 2017. Hence, many are collapsing, and investors are using some for fraudulent promises.

Selfish mining attack

This strategy consists of a miner that discovers a block to mine, and then a second one with no competition, and if successful, a third one, etc. The miner then publishes this chain only if the main network is advancing at its level, then tries to broadcast its version of the chain fast enough.

It appears that no successful selfish mining has occurred recently on bitcoin. We can, however, report that such an attack occurred on Monacoin in May 2018, with damage of around ninety thousand dollars. Small chains are more vulnerable to this kind of attack.

Mining malware

With specialized mining equipment came specialized malware, which specifically targeted bitcoin mining rigs, asking for a ransom, with the threat of destroying the equipment by running it to the point of overheating.

OVERVIEW BY COUNTRY

The following section offers a collection of updates summarizing private and official positions towards blockchains in different countries and geographical areas.

ASIA

In Asia, more than anywhere else, the enthusiasm for cryptocurrencies and DLTs has anything but vanished. The blockchain is no longer the craze it was a year ago, but as people adjust their approach, and as the technological expectations mature, investors and start-up teams are more active than ever, in terms of the people involved, money spent, articles published, and social network activity.

Japan

The Japanese regulator has dismissed the idea of allowing bitcoin ETFs and futures, saying: "Taken it into consideration that it is difficult for us to find constructive and social significance of trading crypto-assets derivatives at present, we think that there is no need for trading crypto-assets derivatives at financial instruments exchanges where many market participants can trade."

A company linked to the internet group, Digital Garage, is investigating the issuance of a yen-pegged stablecoin.

E-commerce firm, Rakuten (often referred to as "the Amazon of Japan"), has announced the set-up of a new payments subsidiary that includes its cryptocurrency business. They aim to integrate and exploit the synergies between the prepaid card service and the crypto exchange that Rakuten acquired last year.

In Tokyo, there is the talk of experimenting with a blockchain-based consumer payment network for the Olympic Games in 2020, with a target processing capacity of one million transactions per second. The Japanese government is behind the project in an attempt to reduce the usage of cash notes and coins, which Japanese citizens prefer, but which are costly to maintain.

South Korea

In January, South Korea introduced some tax incentives for DLT development, by adding blockchain to the list of research and development fields that qualify for a tax credit. This move is intended to help the sector through a difficult period, which saw the price of crypto-assets decline.

Government agencies have conducted a security check on 21 South Korean crypto exchanges; two-thirds of the audited platforms failed the test.

Subsequently, the majority of South Korean exchanges are under threat from hackers—it appears that the government has identified exchanges that are the easiest prey.

More than anywhere else, Koreans used their life savings and took out loans to invest in the crypto market, and of course, they have been badly hurt by the decline in prices.

China

The Cyberspace Administration of China has introduced a new anti-anonymity regulation aimed at blockchain-related companies, pretending to "contribute to the healthy development of the industry." Any business that provides information and technical support to the public using a DLT is affected. The regulation allows authorities to access stored data, and to introduce registry procedures that require users ID cards or mobile numbers to be registered. Also, it oversees content and censors information that is prohibited by the Chinese government.

Officials stated: "The blockchain information service provider shall implement the responsibility for information content security management, and establish and improve management systems such as user registration, information review, emergency response, and security protection… If the user does not perform real identity authentication, the blockchain information service provider shall not provide related services."

The China Banking Association has launched a new blockchain-based platform for transactions. All major Chinese banks are part of the initiative, which is based on Hyperledger.

The Chinese central government is considering a revision of the income tax rules imposed on citizens. The implementation of a common reporting standard would make it more difficult for wealthy individuals to hide their wealth overseas, which could result in them buying cryptocurrencies as an alternative.

Hong Kong

Players in the industry regard the Hong Kong legal framework (SFC's "sandbox") as quite opaque and burdensome.

Malaysia

Starting in mid-January, Malaysia will regulate the crypto-asset sector as a whole. The Malaysian regulator has decided to classify digital assets and tokens as securities, without distinction. Those dealing in digital assets will be required to put in place anti-money laundering, and counter-terrorism financing (AML / CFT) rules, cyber security and business continuity measures.

Guidelines have been issued to establish criteria for determining the suitability of issuers and exchange operators, set disclosure standards and best practices in price

discovery, trading rules, and client asset protection.

Any person offering an ICO or operating a digital asset exchange without the approval of the Securities Commission may be punished.

Philippines

The securities regulator in the Philippines has postponed ICO regulation.

Thailand

The Thai stock exchange is reported to be planning the launch of a token trading platform.

India

Banks are still obliged to close customer's accounts that have cryptocurrency-related transactions. Indian citizens attempt to get around this by using small amounts and never mentioning the nature of the cash movements in transaction remarks.

India continues to lag in its official position, but rumors and press releases indicate that this may change. A new government committee has released a statement that indicates it is favorable to legalizing cryptocurrencies. Even though it refers to "strong limitations," the consensus is that "cryptocurrency cannot be dismissed as completely illegal."

There are reports that some of India's largest conglomerates have decided to "explore blockchain." It appears that private companies understand some of the potentials of the technology but are not able to fully embrace it because of current government regulations. Meanwhile, the huge Indian IT workforce is willing to embrace this new world, and large numbers of Indian developers are hiring their skills to foreign start-ups, to be part of the revolution.

Pakistan

A Pakistan-based microfinance bank has launched cross-border payments using blockchain technology from the payments firm Alipay. The main focus is Pakistanis working abroad who want to remit payment back to their home country.

Back in April 2018, though, Pakistan took a negative stance on cryptocurrencies by barring financial companies in the country from working with cryptocurrency firms.

United Arabian Emirates

Together with Saudi Arabia, the UAE is launching an official interbank cryptocurrency. The envisioned DLT will be private, and not accessible to the public. Quite paradoxically, it will be designed to allow transactions to be reversed, as central banks may need this feature. It is likely to be based on Ripple, Hyperledger or Ethereum.

Israel

Start-ups in the country continue to struggle, and many have closed for business or at least laid off staff.

Hamas in Gaza is asking supporters for donations in bitcoin.

EUROPE

Russia

Rather positive news has come out of Russia, led by Deputy Finance Minister, Alexei Moiseev, who stated that "cryptocurrency's age of pyramid scams" was now behind it—ushering in a new age of legitimacy. Another Russian source expressed the view that cryptocurrencies could have a place in a new world monetary system, where it would replace the US dollar. However, the official government policy remains blurred for the time being, as many different positions have been taken by various officials.

Anatoly Aksakov, chairman of the Duma's financial markets committee, has revealed plans to issue a blockchain-based version of Russia's ruble by 2022, fueling a revival of this debate in Russia. The crypto ruble would be just like the classic one, but on a new platform; this makes a lot of sense and changes little as far as the monetary system is concerned. It will be a very interesting experiment, and its impact on the banking system in Russia will be keenly observed.

Russia has been conducting crypto-assets tests: settlements using crypto instruments have occurred, the likes of which will be impacted by law to be passed at the end of February.

The Russian Deputy Finance Minister expressed the view that using cryptocurrency debit cards to pay for products or services does not contravene the local laws in any way. In other words, using a crypto card to pay for purchases is legal.

Rumors also have it that Russia is looking at investing billions into bitcoin, as a move to diversify from the US dollar, and with the prospect of further sanctions by the USA. It has already started moving its reserves to the euro and the yuan. Without a doubt, such a move would be an incredible legitimation of cryptos and would place huge pressure on demand, potentially driving prices significantly higher.

Ukraine

The crypto-exchange, Liqui, shut down due to lack of liquidity.

An important number of developers based in Ukraine (and Eastern Europe in general) have been actively offering development services in the field of DLT.

Germany

Exploring the bitcoin network, it is apparent that Germany is among the top countries for nodes, with around 20% of the total. It does not say much, other than the fact that the country hosts a vibrant community of crypto-enthusiasts.

Liferando.de, a food ordering platform, is now accepting payments in bitcoin.

France

Related to the "Gilets Jaunes" movement, some protestors have repeatedly suggested to participants in the movement that they should go to banks in numbers and withdraw their money (with the goal of creating a run, to reduce liquidity). The promotion of bitcoin by some demonstrators has been reported.

Italy

Italy has appointed a committee of 30 experts to develop a national blockchain strategy.

The European country has also made its first official statement regarding the legal framework of the blockchain, introducing several blockchain elements in

a new regulatory amendment, already approved by the Senate. It declares: "the recording of an IT document through the use of technologies based on distributed ledgers produces the legal effects of the electronic time validation referred to in Article 41 of EU Regulation no. 910/2014." That is, the recognition that blockchain notarization is legally acceptable.

Malta

Malta is consolidating its title as the "world's blockchain island" in a smart but natural move from the Mediterranean archipelago: 12% of Malta's GDP traditionally comes from the gaming industry (e.g., lotteries, bets, etc.). This business focus has developed thanks to the country's history of lax regulation and a low tax rate—as low as 5%—which attracted entrepreneurs of the sector. However, one must acknowledge that the gambling industry usually attracts various types of actors, some of which sometimes have links to controversial activities.

The economic growth in Malta is 6%, the highest in the EU. To a large degree, this is due to the arrival of the crypto industry on the island, the first of which was Binance.

Their November summit was a success, with 4000 participants being welcomed in the presidential palace.

Switzerland

Most people on Swiss streets have no clue what blockchain is or that a crypto-valley exists in their canton—the Crypto Valley of Zug. But currently, Switzerland leverages its position as a top-tier hub for finance, and consequently for fintech (and IT by extension). Talent is attracted by higher wages and a very good standard of living in the country. Jointly, with fantastic advertising designed to promote the country as a crypto-safe haven and vibrant community. Foundations and their operating companies register in the country (say, in the Zürich-Zug-Vaduz axis) both for tax purposes and for the support of authorities eager to address the concerns of this business, and who are forward-looking in their approach to provide a business framework for these companies.

As the most concrete and recent expression of the will of the Swiss to maintain their country at the forefront of DLT business development, the Federal Council has published a very comprehensive document titled "Legal Framework for DLT and Blockchain in Switzerland."

Swiss banks have issued a document describing accepted practices to address requests for banking services from crypto-related businesses, in a move to try to solve the problem of crypto-asset bankability.

All layers of the Swiss ecosystem are embracing DLTs. Not only are the regulators, start-ups, and banks working on it, but also universities, industrials, etc.

Liechtenstein:

The Principality is resolutely striving to offer the most favorable framework possible to attract DLT-related financial service providers. The small nation has just released a law on "transaction systems based on trustworthy technologies," thereby also proposing an alternative and an even more technology-neutral way to refer to DLTs.

The advantages of Liechtenstein compared to Switzerland are:

A supposedly easier process of opening a bank account to conduct crypto-related business.

Membership of the European Economic Area (EEA), which is about freedom of circulation, not only of people but also of goods and services. Switzerland, on the contrary, has kept border customs to manage the flow of goods and services. As such, it is supposed to be easier to serve the EU market from Liechtenstein than from Switzerland.

Also, Liechtenstein is also using the Swiss Franc and has a 12,5% tax rate, which is very competitive, even compared with the Zug canton.

European Union:

The European Banking Authority has urged the European Commission to examine whether unified crypto rules are needed across the region. For these officials, crypto-asset related activities do not currently fall under existing EU financial laws, and since it judges these activities as particularly risky, it thinks that appropriate rules need to be put in place to protect investors.

The European Securities and Markets Authority has published a report on crypto-assets and ICOs, which advises the EU Commission Council and Parliament on the existing rules that could be applied to crypto-assets, and specifies regulatory gaps for policymakers to consider. In particular, it states that some crypto-assets fall under the MiFID financial framework and need to be classified as financial instruments.

UK

Huw van Stennis, a Central Bank advisor, has expressed the view that cryptocurrencies fail fundamental tests for financial services, and are not high on the list of priorities: "I'm not so worried about cryptocurrencies. They're not a great unit of exchange, neither they hold value, and they're slower". In short, DLT tokens are not worrying about the UK central bankers. Brexit certainly is.

It has not been possible to verify rumors that English people would be dumping sterling to buy bitcoin. However, any turmoil in the fiat world is still, of course, supporting crypto usage.

NORTH AMERICA

United States of America

The government shutdown has been reported to have halted the progress of cryptos on Wall Street. The closure of the Securities and Exchange Commission and the Commodity Futures Trading Commission has caused additional delays in the operation of the US regulatory frameworks. This situation adds to the voices that raised concerns that the US is lagging in the DLT sector and has been slow to address the issue. Some may recall Bill Clinton's words in 1997: "The internet should be a place where government makes every effort… not to stand in the way, to not harm". Twenty years later, the philosophy in the US appears to be quite the opposite.

Gemini, the Winklevoss brothers' exchange, has paid for an advertising campaign in New York to raise attention and call for regulations in the US, claiming that the "revolution needs rules." This indicates that these entrepreneurs feel the need for firm ground on which to properly conduct their business.

The US Securities and Exchange Commission has extended the review period for VanEck's Bitcoin ETF to February 27th, 2019. This ETF, contrary to the previous attempts, is fully reliant on BTC itself, and not to BTC futures, which makes it more credible. VanEck is in the business of routinely underwriting

ETFs, so if it fails, it will hinder the future of BTC ETFs for probably quite some time.

The State of Texas is classifying stable coins as "money," according to guidance from the Department of Banking. This will require issuers of stablecoins to register for and acquire, a currency exchange license to operate in the Lone Star state.

The State of Wyoming has passed a bill to allow tokenized stock certificates to be issued.

The State of Colorado has introduced a bill with (limited) securities law exemptions for cryptocurrencies: the Colorado Digital Token Act.

Adena Friedman, president, and CEO of NASDAQ stated that cryptocurrencies "deserve an opportunity to find a sustainable future in our economy. Crypto thus stands at a crossroads, poised between one of two outcomes: (1) either the innovation finds practical utility followed by years of steady and sustainable commercial progress and integration into the economic fabric; or (2) the invention fails to achieve broad adoption and its commercial applications as medium of exchange are limited".

The Federal Reserve governor, Lael Brainard, said she was "monitoring the extreme volatility of crypto prices, particularly bitcoin," but did not believe that "crypto poses a threat to US financial stability." However, she "urged investors to exercise caution about the highly speculative asset class" and said the Fed would continue to investigate it.

Mexico

The Mexican government has announced plans to facilitate its first public blockchain-based procurement procedure.

SOUTH AMERICA

Brazil

Brazilian authorities have looked at the potential for blockchain to curtail corruption and overhaul Brazil's financial infrastructure.

Venezuela

President Maduro has unilaterally raised the price of the petro (fourfold, now worth 36000 sovereign bolivar). On January 14th, he proclaimed a "new monetary system." Experts and civilians alike have expressed their skepticism. There is still no sign of a crypto wallet for the petro, the links to download it don't work, and the Venezuelan government still strives to sell the digital currency and issue certificates of purchase to buyers. Venezuelans, meanwhile, are still fleeing the country's dire economic situation in the hundreds of thousands. Venezuela also filed a complaint with the World Trade Organization regarding executive orders and sanctions maintained by the US, which target Venezuela and the nation's oil-backed cryptocurrency.

AFRICA

There are indications that awareness and active usage has grown in Africa at a faster pace than anywhere else, with Nigeria, Ghana, and South Africa leading the pack.

South Africa

The central bank has proposed rules for crypto companies, which would impose various measures aimed at protecting the customers of these companies. The measures include compulsory registration, amendments to existing rules to frame crypto-asset management, and some KYC features, such as reporting suspicious activities.

A consultation paper was established to regulate and de-anonymize bitcoin transactions. The new laws would ensure exchange and wallet providers trace transactions and are held responsible for their customer's usage of cryptocurrencies, similar to the role banks play in today's financial environment.

Ghana

The SEC of Ghana is considering licensing cryptocurrencies to make it legal tender.

Cameroon

An English-speaking separatist territory is planning to launch a cryptocurrency as a tool to free themselves from the central government.

OCEANIA

Australia

The parliament in Australia has passed a shocking law: it states that backdoors should be implemented to all encrypted communications, to enable officials to monitor crypto activity. Even if this is not yet signed and in force, this statement would henceforth make blockchain technology non-compliant under Australian law.

New Zealand

Cryptopia, the Kiwi exchange, has been hacked and has been closed by the NZ authorities for investigation.

CONTACTS & REFERENCES

Alexandre Juncker
Research and Redaction Head, and Partner at bqintel
alexandre.juncker@bqintel.com

Halim Nader
Research & Marketing Manager at bqintel
halim.nader@bqintel.com

Danil Knyazev
Partner at bqintel
danil.knyazev@bqintel.com

For more information and updates, please visit blockchain-quarterly.com.
You can also email us at research@bqintel.com

Blockchain Quarterly is published by bqintel, a data and research company, providing blockchain intelligence & insights for businesses. Blockchain Quarterly is part of our yearly subscription service from bqintel. For more information on how to receive Blockchain Quarterly, request permission to republish content, or comment on content, please email research@bqintel.com.
Please see www.bqintel.com to learn more about our products and services.