BLOCKCHAIN QUARTERLY

9TH EDITION |JANUARY 1ST, 2020

9th Edition published by bqintel.com

FOREWORD

This document is the January 2020 issue of Blockchain Quarterly – a series of in-depth studies started in 2017 – and is undertaken on a trimestrial basis. Our report systematically highlights vital activities and trends of distributed ledger technologies (DLTs) globally.

To ensure comprehensive coverage, each issue of Blockchain Quarterly refers to the material contained in previous topics and elaborates on already-debated considerations – thereby updating views, introducing new solutions, and going deeper into the analyses.

In the present document, we discuss research, principles, and fundamental appreciations about the cryptosphere, as a whole. This includes the latest technical evolutions, updates on use cases, new regulations, etc., for the entire span of blockchain and other DLTs. The purpose is to reach a reasonably exhaustive understanding of crypto developments worldwide ultimately. Hence, based on this review, the reader should gain an educated view of the direction in which the industry is evolving. In particular, we aim to identify the current underlying forces that are driving DLT-based currencies and token markets, to identify possible scenarios.

As time passes, each exercise becomes more complicated to conduct than the previous ones, as the blockchain environment is evolving quickly. All information presented herein is considered to be accurate at the time of publication, but as a disclaimer, 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; we explicitly do not provide any investment advice in any edition of Blockchain Quarterly.

If, despite the care taken in gathering accurate information, some errors are found, contact us on research@bqintel.com.

TABLE OF CONTENT

Blockchain Quarterly - 1st Quarter 2020

EXECUTIVE SUMMARY

The bullet points below summarize the main points from the studies and research presented in this, the ninth edition of Blockchain Quarterly:

• Cryptocurrency markets are consolidating further after the spring price hike, on relatively reduced volumes, and with a continued high correlation of crypto asset classes, amid an over-extended expansion phase of industrial stocks.

• On the legal/regulatory front, steps are increasingly being taken by several central banks to issue some blockchain-based traditional fiat. The legal acceptance of managing securities on a blockchain is also making good progress. Otherwise, stances taken and laws passed regarding pure cryptocurrencies are systematically restrictive, if not hostile. Cracking down on KYC/AML is routine, but the prohibition of exchanging crypto for fiat is in question and not accepted in all countries

• Industrial use-cases continue to be researched. However, not many full-scale systems are ramping up or on the way to full implementation. We are still mostly at the stage of robust testing of pilot projects. The initial enthusiasm for disrupting ecosystems is over; professionals now believe that most of the potential gains will be made by automating interfaces and developing value transfer accounting applications. These are operational gains, at best, and will solve some issues, but will also introduce new kinds of hurdles. More and more, we are observing that industries are adopting ecosystem-wide approaches to define standards and protocols for decentralized infrastructures to be built, and for compatible systems to be built on top of these.

• On the cryptoccurrencies adoption front, not much is moving, not even with the benefit of the Lightning network. Even Libra has been under such intense scrutiny and criticism that its realization is now in question. More time is needed to devise and propose user-friendly apps.

• From a technical development perspective, there is still a long way to go to solve scalability. Some proposals, such as MimbleWimble technology, are being criticized and questioned; consensus mechanisms are being researched more intensely than ever, with no sign of a clear winner. The actual deployment of PoS by Cardano and Ethereum is on ice. In general, not much progress has been made to resolve the current technical limitations of blockchain, which has disappointed observers, stakeholders and investors/speculators.

Blockchain Quarterly - 1st Quarter 2020

1 GLOBAL MARKET UPDATE

EDITORIAL: GLOBAL STATE OF THE DLT ECOSYSTEM

Please note that the present report covering Q4 2019, is issued as Q1 2020 starts, as will be the case from now on. This issue of Blockchain Quarterly is somewhat light, compared to previous editions. Overall, the material that has emerged from this review shows an incremental evolution, rather than disruptive developments. To an extent, this slowdown in important news is proof that a moment has been reached in the growth of the technology and its business cases when the development of products and services takes some time.

Our deep impression, when performing press reviews, is that there are still many theoretical, forward-looking, almost philosophical articles being published, mostly accurate, but with relatively few success stories hitting the headlines. The hype, which had picked up in the first half of 2019, is now at its lowest again, with worrisome positions taken by some countries, and no real technical progress, or proof, or public adoption to counterbalance this.

COMMENTS ON CRYPTO-ASSETS MARKETS

Prices

Cryptocurrency prices have gone through some turmoil during the last three months.

The crazy, impulsive move seen in the spring was too good to be true. It was too much; the surge in prices was unreasonable. In that respect, the current retreat can be seen as a stabilization within a more significant trend.

It is always challenging to explain recent movements in financial markets; and somewhat easy to find reasons for past behaviors, but as we will detail chapter by chapter in this Quarterly, there has been a shortage of fundamentally positive news in the crypto world.

As outlined in our previous issues, all categories of cryptocurrencies are not behaving in an entirely similar manner. While Bitcoin has held some of the gains it made in 2019, this has not been the case for smaller-platform native currencies, let alone ICO tokens which are continuing to collapse, in what looks to be the middle of the crypto-winter, for them.

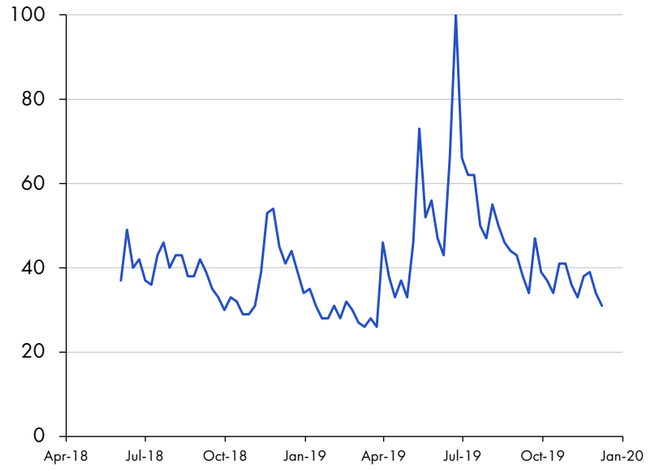
Correlations

The correlation between crypto assets has significantly decreased for the last year.

This decorrelation seems to be indicating a maturing sector as crypto-assets have very different natures.

FIGURE 1:

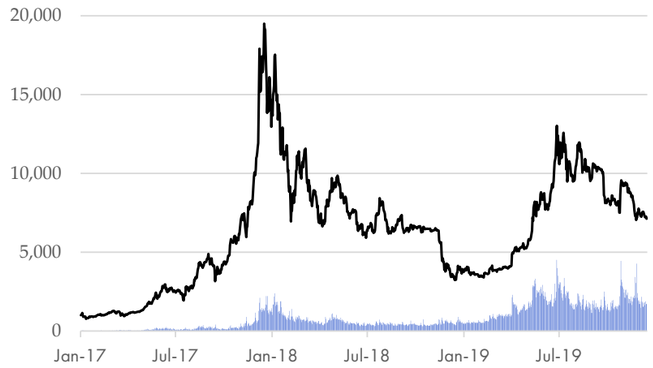
INTEREST IN BITCOIN RELATIVE PICK LEVEL (100)



Source: Google Trends

FIGURE 2:

BITCOIN PRICE AND VOLUME



Source: CoinMarketCap

Exchange volumes

Exchange volumes declined significantly in September compared to this summer. Data gathered from exchanges remain unreliable, so it is challenging to assess genuine exchange volumes worldwide. Still, the figures indicate that, overall, there is no sign of volume fading.

Volatility

When liquidity decreases, volatility can be expected to increase. Lately, this has been the case for crypto assets, because, as just mentioned, volumes are down. And indeed, we continue to see that whenever a market shock occurs with an increase in volumes, prices increase significantly.

Overall, observers expect volatility to continue, and indeed, there is no reason we can find to indicate otherwise, not before more adoption occurs.

INTERACTION WITH MACROECONOMICS

After a shaky 2018, stock markets are recording a positive 2019, which extends this growth cycle. As at the time of writing, share prices of American companies are pushing their all-time highs. Regardless of whether you regard this as total nonsense, or you see this as an effect of unprecedented advances in productivity thanks to robotics, internet platforms, and globalized competition, the fact remains that global markets, as a whole, have decided that stocks were not yet overpriced. How long it will take before we see a significant correction is unknown.

That's how it is, however, we have no choice but to wonder, what if it continues, and what if it crashes?

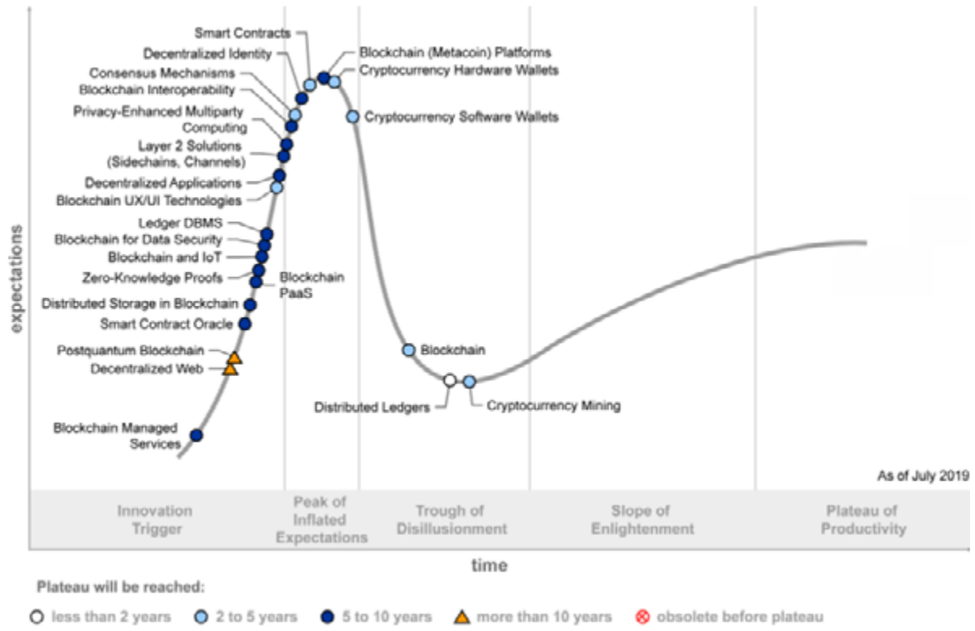
If stock markets crash in short to mid-term, reactions by central bankers are likely to be similar to those implemented in 2008: quantitative easing, increasing liquidity to prevent the economy from being short of funds. However, experts doubt that it will have the same impact it had after the GFC and may require central bankers to go even further with the level of money creation. In turn, this will dilute the holdings of individuals and companies who sit on cash, and this could negatively affect confidence in politically-influenced fiat currencies, which may then lead to a flight of capital to diversify into crypto assets, such as Bitcoin.

On the other hand, if stock markets do not crash in the short or mid-term, this would mean that companies are conducting good business and generating revenue for investors, thereby fueling investments in technology, among them, blockchain. It is entirely feasible that sustained signs of progress in solving current DLT issues, combined with an abundance of capital, could trigger, and then fuel, yet another crypto bubble.

An often-shown picture is Gartner's curve of adoption. It is indeed suggesting that blockchain still has a long way to go, and we are only just at the beginning of the journey on the road to widespread usage.

FIGURE 3:

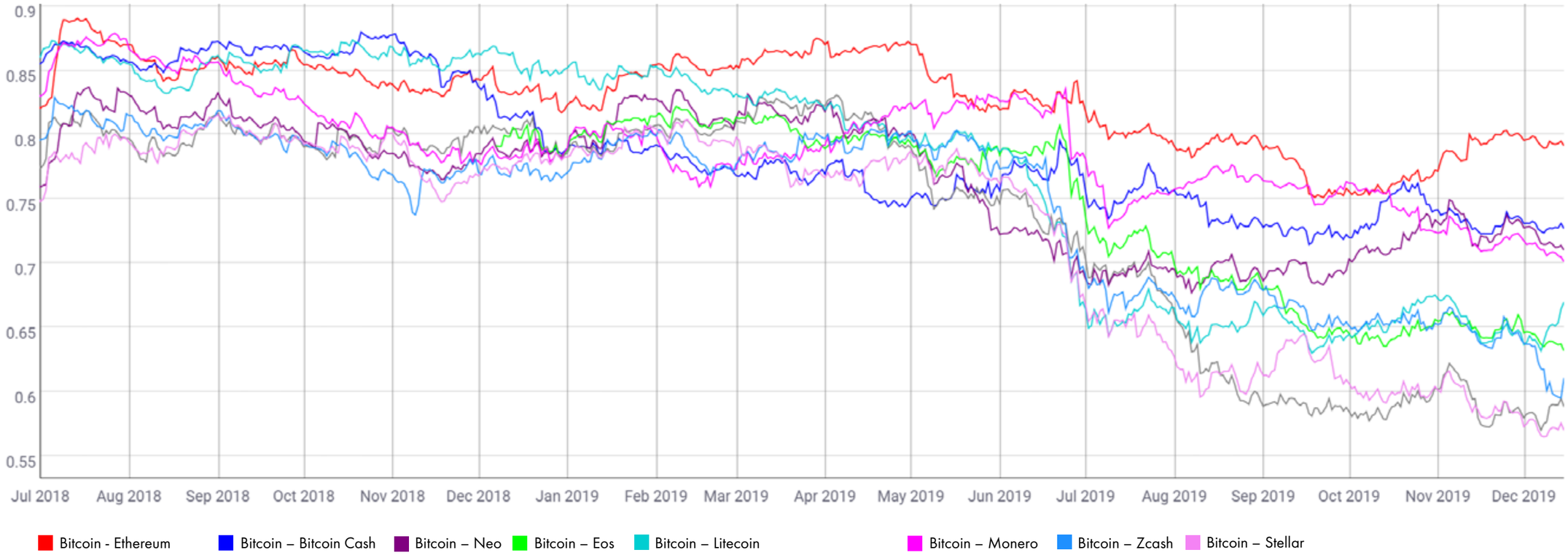
BLOCKCHAIN TECHNOLOGY ADOPTION CURVE



Source: Gartner

FIGURE 4:

CORRELATIONS OF COIN PAIRS OVER TIME



Source: Coinmetrics.io

Blockchain Quarterly - 1st Quarter 2020

2 UPDATE ON THE REGULATORY POLICIES

GENERAL APPROACHES BY GOVERNMENTS

Globally, regulatory bodies have been rather calm recently; we have seen relatively fewer media articles, compared to previous times. Interestingly, political crack-downs appear to be proportional to Bitcoin's price, which makes perfect sense.

Despite this, apparent calm does not mean that regulators have been idle. Our review of press releases indicates that the implementation of crypto or blockchain-related regulations is occurring almost every other day; for something like 200 jurisdictions on the planet, that's not surprising. But in general, we observe that the stances taken by officials and regulators have been in line with what they have previously indicated, thereby confirming their positions/views.

A few countries that had negative approaches are changing their tone, although not always with full acceptance of cryptocurrencies, they are at least acknowledging the potential of distributed ledger technologies; Indonesia is an example.

As for coordinated financial regulation, the Basel Committee is working on the prudential treatment of crypto assets, intending to reach an agreement on how much capital lenders should hold to cover the risks inherent to holding crypto assets. Compared to the usual critics of Bitcoin and the like, this is quite an exciting move – acknowledging a reality!

STATUS REGARDING OFFICIAL INITIATIVES TO PASS FIAT ON DLT

The most significant sign of progress has come from China, where a central bank-issued cryptocurrency is expected to circulate soon. While the infrastructure is believed to be quite similar to that of Libra, the intrinsic value of this token will be the Chinese yuan or renminbi. So, the release of this Chinese cryptocurrency should first be adopting blockchain support to emit the central bank money, then invite people to use it for representation and exchange of value. But many interesting aspects are yet to be clarified:

- How much of the currency will be released in this manner? And will it be accompanied by a destruction of equivalent paper fiat?

- How will it compete with the traditional currency transacted by commercial banks? Such a full-scale experiment is going to be very interesting to study.

- Will this money be available for payments abroad, including for foreigners to own and use, even outside of China? In this respect, the intentions of Chinese regulators are ambiguous, as they have actively sought to prevent citizens from taking money out of the country, while at the same time pushing for international recognition of the renminbi as a reserve currency able to compete with the US dollar, thereby also bypassing the western banking/financial system. In the eyes of Chinese officials, Libra's movements have no doubt stressed the urgency to move. Exciting times ahead!

Benoît Coeuré, a member of the European Central Bank, has been given the responsibility within the Bank of International Settlements to head the Innovation Hub, to foster international collaboration among central banks on innovative financial technology. Among the areas of focus for the assignment are the Central Bank Digital Currencies (CBDC), global stablecoins, and other payment innovations. The BIS also claims to be planning to look at "regtech", digitization of financial titles trading, and financial disintermediation.

The truth is, with varying willingness to publicly discuss it, most central banks are actively studying how they can do it, and what the impact would be. Examples are numerous: the European Central Bank has confirmed it is exploring the feasibility of a DLT-based euro as a retail and wholesale currency; others include Tunisia, Canada, Russia, and Sweden. Arguably, today no central banker can afford not to consider it, at least from a feasibility perspective, in terms of supporting their national currency. But the debate around possible changes to the circulation process, that is, controlling who is going to be entitled to possess and exchange it (licensed banks only vs. open) has not commenced.

THE MOST SIGNIFICANT SIGN OF PROGRESS HAS COME FROM CHINA, WHERE A CENTRAL BANK-ISSUED CRYPTOCURRENCY IS EXPECTED TO CIRCULATE SOON

REGULATION OF INITIAL CRYPTO-ASSETS OFFERINGS

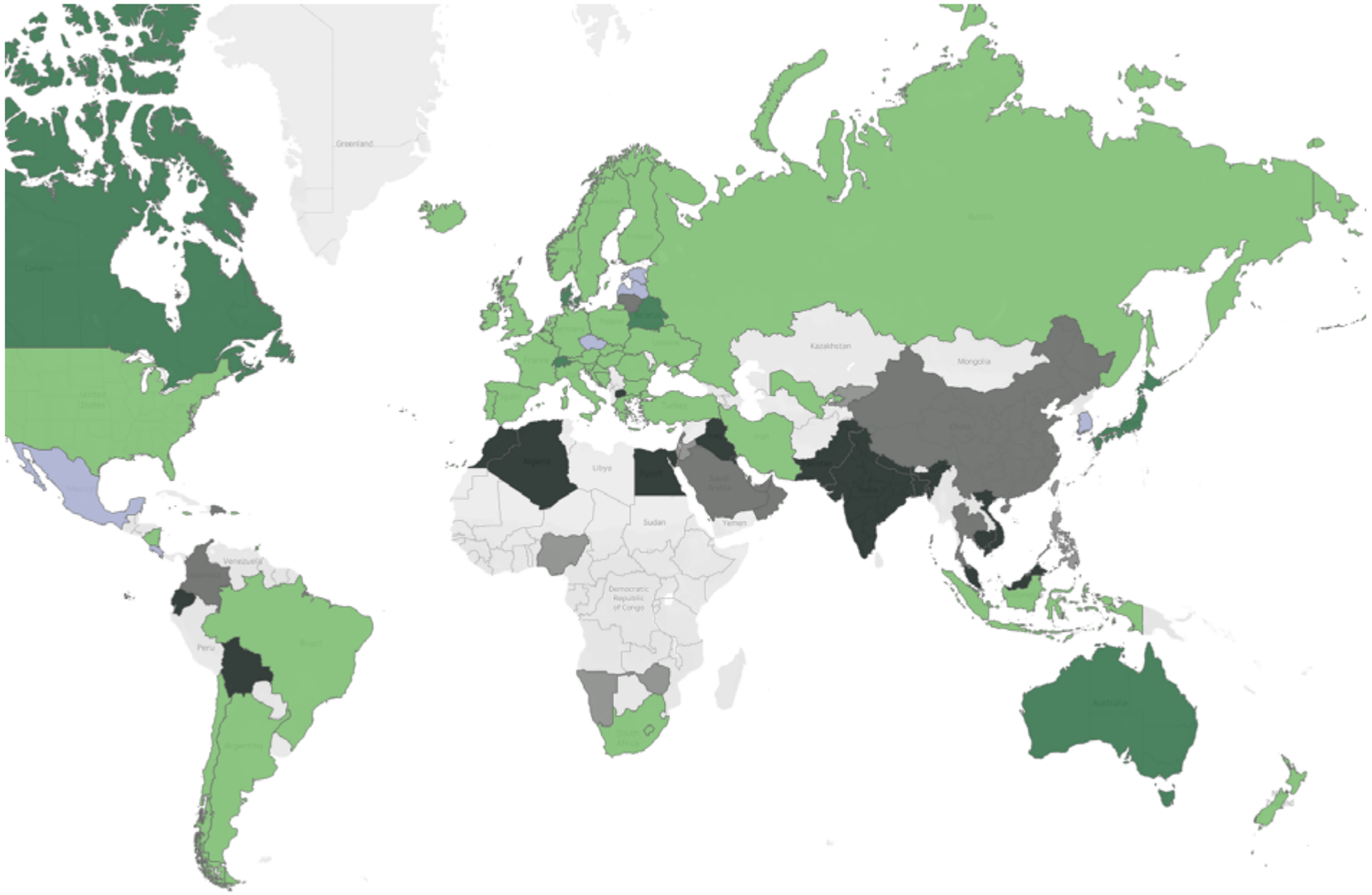
Fundamentally, there is not much that is new in terms of intentions to regulate ICOs.

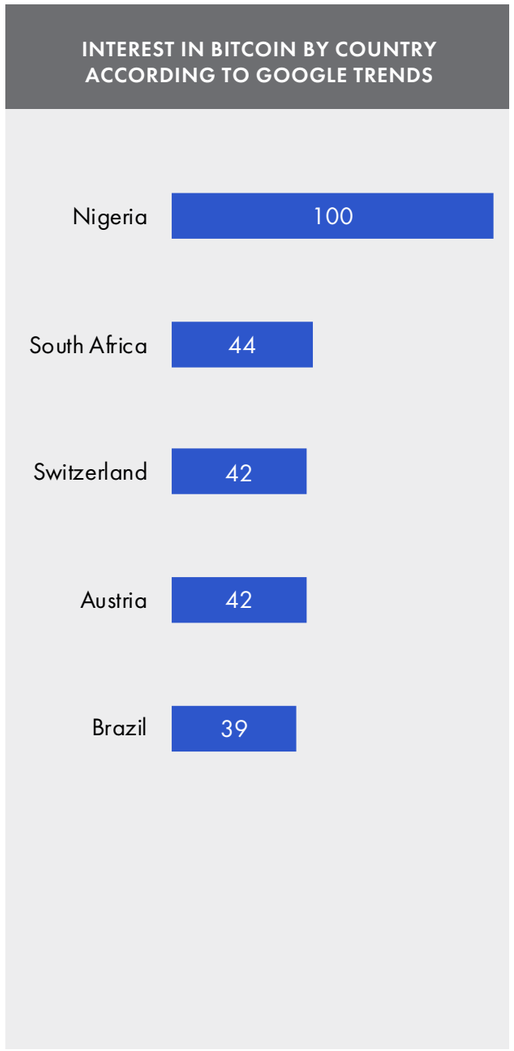
Capital raising via ICOs has shrunk drastically. This is all far less of a hot topic than it was in 2018. The prices of most ICOs had collapsed, down to their initial offering price or below, justifying the warnings of financial watchdogs around the planet at the time when ICOs were popular.

A correlated observation is that investors who lost money have not complained a great deal, clearly indicating they were aware of the potential risk of losing all of their investment (which mostly happened). This suggests that individuals who got (and continue to get) involved felt (and feel) responsible for the outcome, and generally were aware of the asset category they were getting into. Arguably, they were knowingly operating in this hazardous environment, showing that people can act

FIGURE 5:

LEGAL STATUS OF CRYPTOCURRENCY CIRCULATION BY COUNTRY





Source: BQ Intel, Google Trends

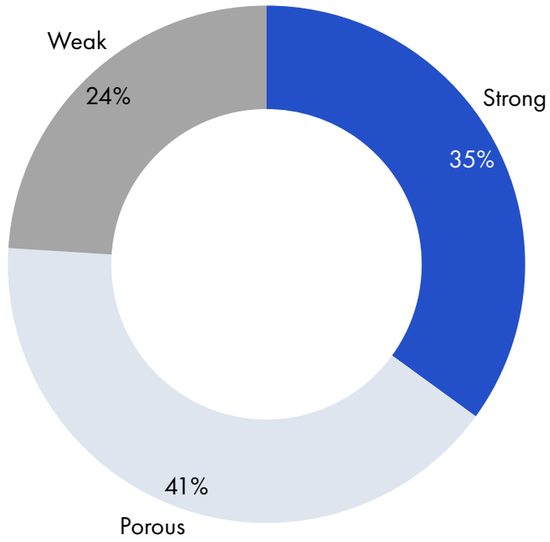
without being watched after / protected all the time by their governments.

Anyway, it all looks like a fire that extinguished itself before it became an actual problem for officials in charge. Currently, some ICOs are launching in jurisdictions that are comfortable with the nature of tokens, which are now clearly described in official documents, in addition to their whitepapers.

Investors are excluded if they are citizens of countries that have expressed opposition (or indeed, threats), and these ICOs are making an effort to apply KYC to subscribers – to avoid being accused of taking dirty money. Past ICOs that have not complied with this is potentially in trouble. However, there are very few actual cases of judicial action, just a few that are there to establish jurisprudence and scare others from bending the rules too far.

FIGURE 6:

CRYPTOCURRENCY AML REPORT RESULTS



Source: ChiptherTrace

Speaking of this, in this section, we usually present details of a US SEC case! This time, let's study the Telegram dispute. Telegram raised $1.7 billion in the first half of 2018 to build the TON blockchain, and almost 40 of the 171 investors were US citizens, who contributed about 25% of the total. However, Telegram did not deliver the GRAM tokens to its investors by the scheduled date in October 2019.

Some US investors complained and were unable to agree with Telegram. Importantly, the SEC did not dispute the characteristics or the legality of the token offering, as the issue was designed to attract experienced investors, and complied with the regulations. However, the SEC was concerned that a secondary market for the token was immediately available, where fewer experiences investors may not be aware of all the risks. It is not unclear how the SEC will move to address this concern: let it go or create new ad hoc rules.

Besides ICOs, irrespective of the type of investor associated with a token, especially for clear financial titles, we have observed that the applicable laws are generally deemed to be good enough by the regulators. In practice, however, existing regulations have to be adapted to allow for the new functionality proposed by DLT management, to be effectively used and leveraged (typically, the possibility to hold and transfer these assets more quickly). But the financial obligations of the issuer are pretty much the same, with a few exceptions. So, we are not seeing the appearance of new, specific pieces of regulation, but rather the incorporation of the original supporting medium of representing assets into the existing frameworks.

KYC / AML / CFT

More than ever, the position of regulators can be summed up, as Julie Myers puts it: "Money laundering, fraud and the financing of terrorism are serious crimes that have significant global effects. Any technology that has the capability to be used for these crimes must be regulated in some way to mitigate those risks."

Privacy / confidential cryptocurrencies regulations

Anonymous cryptocurrencies are built purposely to free people from controls, while on the other hand, officials and governments will never be keen to allow value to be moved anonymously in cyberspace. So again, frontal opposition is expected to lead to a fight. However, this quarter, we have not seen any concrete moves in that direction, probably due to the sluggish market for anonymous cryptocurrencies.

The only thing we see is that, for exchanges, the listing of privacy coins may ultimately be considered by regulators to be a breach of KYC, as these coins prevent any identification of the origin of funds. In anticipation of clampdowns, many exchanges have already been removing trading and custody of privacy coins, and at present, only around one-third of exchanges are proposing them.

Implementation by crypto actors

UK banks are looking at a blockchain-based solution relying on Factom and developed by the start-up, Knabu, to tackle their KYC obligations. Despite the incumbents' aversion to the blockchain, we expect more banks to embrace these systems, which will produce significant savings in operational costs to resolve their legal obligations.

MONEY LAUNDERING, FRAUD AND THE FINANCING OF TERRORISM ARE SERIOUS CRIMES THAT HAVE SIGNIFICANT GLOBAL EFFECTS. ANY TECHNOLOGY THAT HAS THE CAPABILITY TO BE USED FOR THESE CRIMES MUST BE REGULATED IN SOME WAY TO MITIGATE THOSE RISKS.

Meanwhile, a survey has concluded that two-thirds of the top 120 crypto exchanges had weak KYC policies.

Blockchain-based solutions

On-chain KYC management is closely linked to identity management. Please refer to the extensive coverage of this topic in the previous issue of Blockchain Quarterly.

Interestingly, managing KYC on-chain might not be technically complicated; what matters is that a credible authority can be created on-chain – or rather, that an existing official body can be given access to operate on-chain.

In general, on an open chain, anyone can propose the issuing of digital identities. Ideally, all of them being under the same format, to enable interpretation in the same manner by all applications that need to access them. But only real-world qualifying authorities (e.g. regulators, certified agencies, notaries) will, at the end of the day, be respected for financial KYC. Hence the importance of involving relevant governmental departments!

DATA PRIVACY PROTECTION COMPLIANCE

The European Union is spearheading regulation to protect data privacy; it has enforced the General Data Protection Regulation (GDPR). While this has had a massive impact on businesses, especially the internet giants, blockchain has fundamental issues when it comes to complying with the regulation. Let's dive a bit deeper into this topic.

In a nutshell, the principles of transparency and traceability of data entered permanently in an open ledger is a concern when it comes to operating in jurisdictions that intend to permit access, rectification and deletion of personal data upon request of the relevant individuals.

The European Parliament has issued a report titled, "Can distributed ledgers be squared with European data protection law?" In this paper, the researcher highlights the fundamental incompatibilities that appear, point by point. Very interestingly, blockchain complies with some GDPR requirements: transparency, accuracy and integrity is, of course, more comfortable to demonstrate on a DLT-system. However, the principles of purpose limitation and data minimization are not significant concerns; they are to be taken into account when designing the applications. So, the most worrisome questions interest, with no surprise, the right to erase private data – the right to forgetting – and the confidentiality / protection of private data.

However, the report falls short of proposing paths to solve the issues. So, let us consider this here. The approaches we envisage that can be pursued to try to resolve the problems, and use DLTs in a compliant manner are the following:

- In principle, we can state that a fully decentralized platform proposes a set of instantiated logic, available to anyone, with the developer having no liability.

- Going further, if an individual perceives an advantage in using an on-chain service/logic, and is required to share his or her data, then it is arguable that the benefit obtained from the platform should justify the publication, even forever, of the data. This justification is a practical one, not solving the core issue, but merely making it legally acceptable. Everyone then is free to participate in the system if they wish to benefit from it.

- It can be demonstrated that the handling of aggregated private data will no longer be private. Hence a service that handles the private data of several individuals off-chain, before aggregating it and inputting it on-chain, could be a potential business opportunity to comply with GDPR.

- Pruning can be considered a possibility to erase data from the ledger after a given period has elapsed (not upon request of users).

By the way, as a general comment, States are slightly schizophrenic when, on the one hand, they insist on tracking and controlling all financial flows via KYC, and on the other hand, they impose regulations on businesses to ensure confidentiality and self-control of data owned by corporations.

3 REVIEW OF BLOCKCHAIN INDUSTRY PLAYERS

MINERS

Market growth and profitability

Overall, the trend in the increasing hash rate is continuing, with, for the moment, continued mining profitability. Since November 2018, when the hash rate decreased, reflecting the crash in the BTC price, the growth has resumed, thanks to the material improvement of ASICs and new BTC investments. However, at the current price of Bitcoin, the curve suggests that mining activity is again reaching its limit. In November 2019, the mining difficulty decreased, similar to what happened at the end of 2018 (but online hashing power has since doubled), showing that some facilities have hit their mining operating costs.

A quote by Max Keiser expresses the point of view of miners quite well: "Price follows hashrate, and the hashrate chart continues its 9-year bull market."

Material

New special-purpose equipment continues to be released to the market, each time with improved technical capabilities. To quote an order of magnitude, a mining rig typically costs 3000 euros, capable of 70THash/s, consuming ~3000W of electricity.

Monero was upgraded again to counter the use of specially-built mining equipment. But note, despite the efforts to keep the protocol immune from specific hardware usage, ASIC-resistant chains have also been prone to 51% attacks.

The concentration of hash power

On September 23rd, 2019, the BTC hash rate crashed by 40% without any apparent reason, just a few days after reaching an all-time high of 102 quintillion hashes per second.

The biggest pool of miners is currently claiming 20% of the produced blocks, with a few other pools claiming 10-15%.

Environmental issue – electricity consumption

Still, on the subject of orders of magnitudes, Bitcoin mining currently consumes over 50 TWh per year. For, say, 650,000 BTC to be produced, ~75MWh is required per bitcoin. So, approximately 4,000 euros worth of wholesale power is consumed per bitcoin (depending to a large extent on the geographic location of the mining facility).

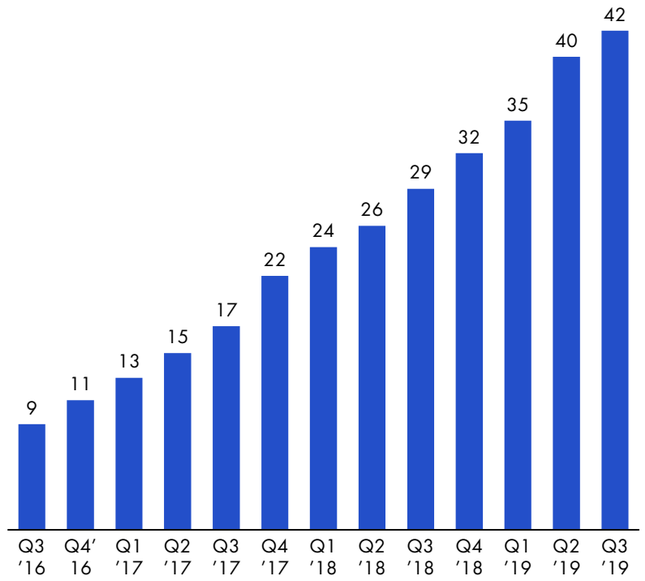
EXCHANGE PLATFORMS

Decentralized exchanges (DEX)

One of the main factors often quoted in favor of more decentralized exchanges is the potential to circumvent fiat currency. Since no control

FIGURE 7:

NUMBER OF BLOCKCHAIN WALLETS USERS (BN)



Source: Statista

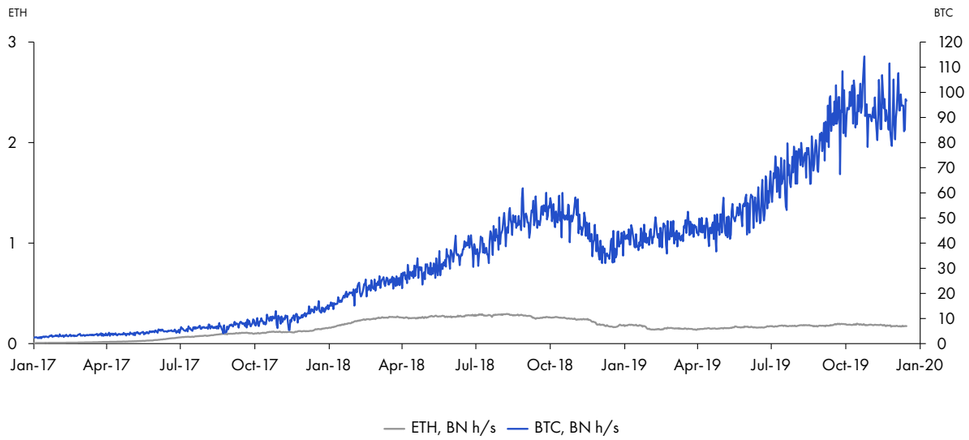
whatsoever is placed on them (which is the point...), convincing someone to take your assets in exchange for hard fiat is likely to be difficult; in particular, no bank is going to be keen to do that. So, the use of fungible stablecoins looks like the most promising way to go.

Off-chain crypto exchange platforms

Binance, Bitfinex Poloniex, and others are implementing geography-based blocking to prevent citizens of specified countries from accessing their services (especially for US residents). This approach is quite dubious: by using a VPN, anyone can pretend to be located in another country, not to mention the possibility of people traveling abroad. So, this is only a partial measure at best, and cannot be satisfactory from regulators, and cannot be seen as fair from the users' perspective. This is another paradox, to say the least, of trying to force cryptos into the existing frameworks of financial controls.

FIGURE 8:

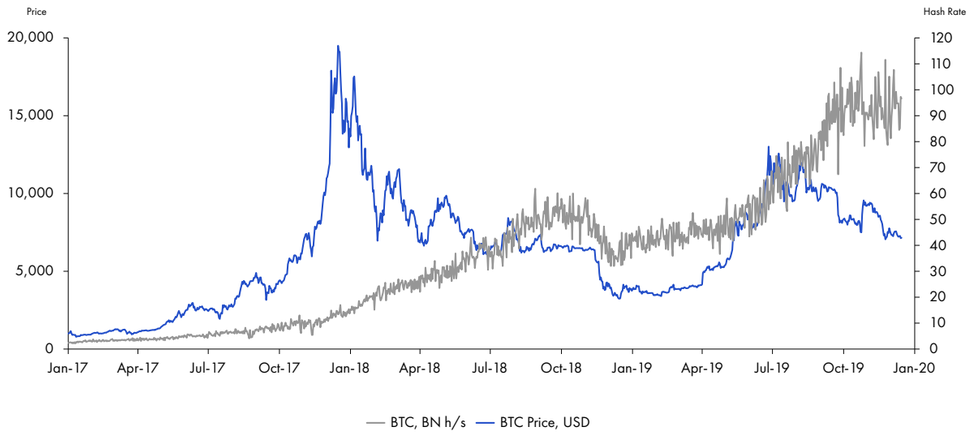
BITCOIN AND ETHERIUM HASHRATE



Source: Etherscan.io, Quandl

FIGURE 9:

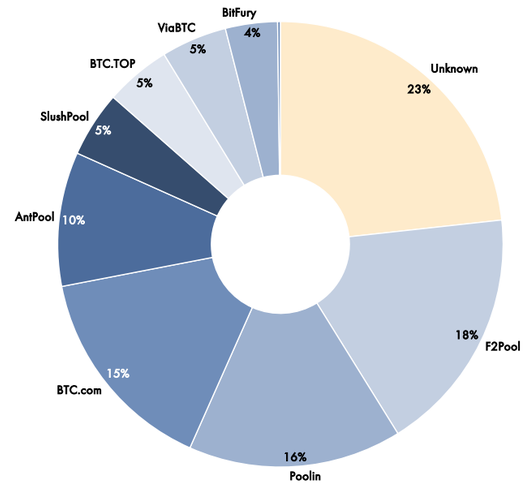
BITCOIN PRICE VS HASHRATE



Source: CoinMarketExpert, Quandl

FIGURE 10:

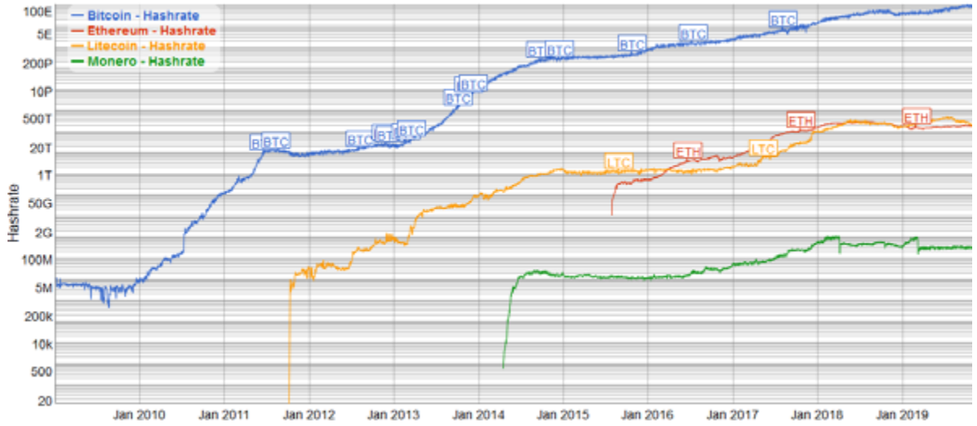
HASHRATE DISTRIBUTION



Source: blockchain.com

FIGURE 11:

BITCOIN, ETHERIUM, LITCOIN, MONERO HISTORICAL HASHRATE



Average hashrate (hash/s) per day

Source: blockchain.com

Legacy exchanges

The Chicago Mercantile Exchange (CME), which is already the first offer of Bitcoin futures, has announced that it intends to launch Bitcoin options as soon as January 2020.

CUSTODIANS

Simultaneously (if not before), the crypto assets custody sector has to build the management of financial titles on the blockchain before it can go mainstream, as the management of these assets for the public at large cannot rely just on private keys.

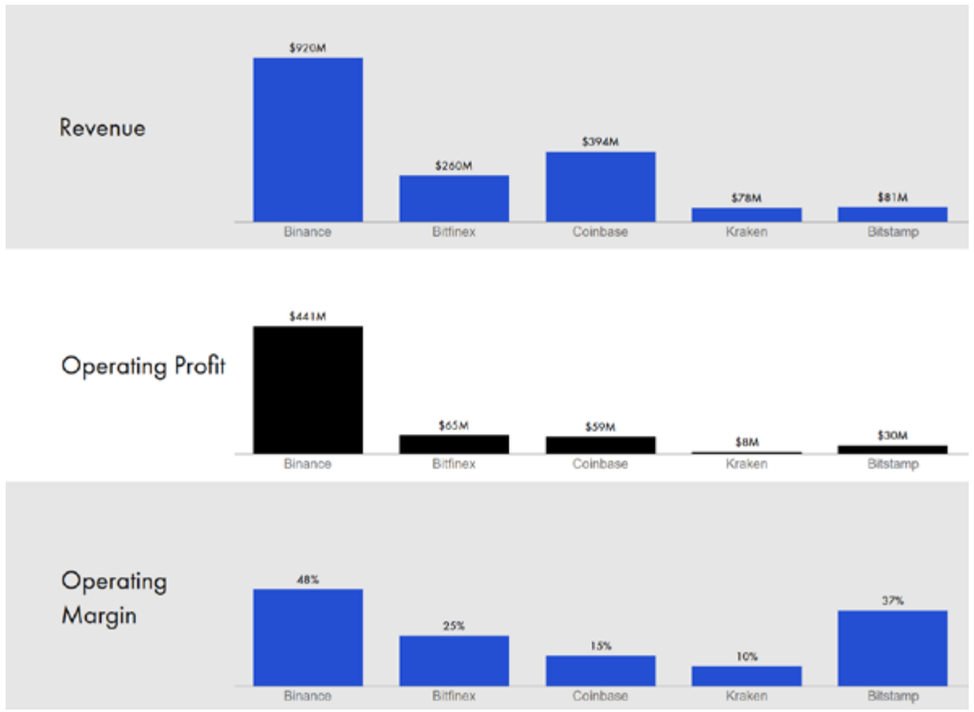
So, what we observe is that pure players are trying to gain momentum; Bitcoin Suisse, for instance, is spending a lot on advertising, while traditional players are working on stepping into the market, as they can justifiably see this as the evolution of their business. True, this is about providing a quality intermediary service, and the initial goal to empower users directly will still be possible, but custodians will have some competition in this space.

MONETARY EROSION

When professional custodians step into this space, we can expect that the loss of Bitcoin and other cryptocurrencies to be significantly reduced.

FIGURE 12:

REVENUE, OPERATING PROFIT AND MARGIN FOR TOP 5 CRYPTO EXCHANGES



Source: BQ Intel estimates based on internal modeling callibrated to publicly available data (more at bqintel.com/crypto-x-bench

BLOCKCHAIN CREATORS, ENTREPRENEURS

With depressed prices of cryptocurrencies and technical struggles, it comes as no surprise that more and more start-ups, especially those that initially raised millions on ICO-platform models, are closing their doors. The legal obligations they have to investors who own their tokens are not under the spotlight – yet. However, this may have to resolve, at least by the larger ICOs, and particularly those that scammed investors.

So, the crypto-winter continues for crypto-entrepreneurs. Weak and poor projects continue to die, exhausting their "war chest" of Ether and Bitcoin from their capital raising if they still any left before they terminate business.

INDIVIDUALS ACTING FOR THEMSELVES

Whales

A few "whale movements" continue to be detected now and then, "from an unknown account to another unknown account."

A recent one-billion USD movement was thoroughly discussed and analyzed after 94,504 Bitcoins were moved in early September. Questions remain as to who has paid who through this transaction. Was it weapons, drugs, a ransom, or just tons of cocoa beans? A mystery. Analysts of on-chain data have tried to track down the source of the coins. It turns out that they originated mostly from several Huobi accounts, leading observers to suggest that someone instructed a team to buy that many bitcoins via several accounts, and then to withdraw them discretely and mass them at one single address before making the transfer. The rest is left to your imagination.

Casual holders

At the time of writing, there are indications that most private individuals have withdrawn from actively trading the crypto market. This is likely to be directly related to the hype around the Bitcoin blockchain being down, and price movements being, not dull, but let's say, uninteresting.

The influence of casual holders is now almost insignificant, as prices now tend to move only when volumes increase. Control is now totally out of the hands of small individuals.

INVESTMENT FUNDS

PE/VCs

[Nothing new to report in this section this quarter.]

Private bankers and classical investment/ hedge funds

During the 2019 BlockShow Asia conference, a panel discussed "Unlocking Yield in Cryptocurrency Assets – Encouraging Institutions to Enter the Industry." A number of crypto leaders shared their thoughts on how to make emerging fintech accessible to mainstream financial entities. Speakers talked about what they believe is needed to onboard institutional players: "Custody, liquidity, and regulations are the top three petitions from institutional investors jumping into crypto."

Overall, the so-called institutional money is not pouring into cryptocurrencies – far from it. The only thing that has occurred in this respect is that a few clients are asking their private bankers to put some of their money into Bitcoin, and maybe a few experiments by maverick investment funds seeking to test the waters, but no further. Right now, there is no reason for this to change. Only when wider adoption has occurred will the large banks dare to look further. And not to forget, they will be under intense scrutiny and pressure from governments as soon as they decide to engage in this.

DATA AND INTELLIGENCE PROVIDERS

With the inception of distributed ledgers, an entirely new financial ecosystem was born. Data available on exchanges is a source of interest for data miners from many fields, who search for and extract patterns in various ways.

• Data services gather data from various platforms, compiling volumes and prices from across the globe. The most well-known is, of course, CoinMarketCap.com, but competition exists.

• The distinct value-added options likely to be offered will be similar to the services that have been provided for decades by, for example, Bloomberg and Yahoo Finance regarding company information and stock prices. (Interestingly, Yahoo Finance just concluded a partnership with CoinMarketCap to add cryptocurrencies to the list of assets presented). For crypto assets, some websites are now providing data sheets on crypto characteristics and project information for investors, even including an assessment of the respective technical teams, DLT performances, etc. Coming up with crypto indices is the next frontier in this respect.

• Finally, and more specifically, some services are offering on-chain data exploration and analysis. The ledgers are often public, and pseudonymization allows for research to be done to link activities with types of accounts; this kind of exploitation of the information on distributed platforms can provide an insight, for instance, on the origin of assets, a service that is currently sold mainly to exchanges and cryptocurrency custodians to make sure their clients are not involved in frauds – this is an area in which KYC can be extended.

UNIVERSITIES AND RESEARCH CENTERS

Recent press reports provide almost no indication that university courses are being launched, as was reported in our previous Quarterly. While this does not mean that universities have disengaged or that classes have been canceled, it does indicate that the popularity of the topic among students and academics appears to have declined.

Universities prepare the workforce to satisfy commercial requirements, and when industries boom, there is an immediate demand for skills, while the opposite situation leads to a moderation in academic engagement. Currently, the indications are that blockchain technology is going through a period of consolidation.

EMPLOYEES – TALENT

While the signals are still favorable for blockchain-intensive talent, which companies still are in search of and are hiring, the dynamic is clearly down compared with recent months. Having said that, Consensys, which has laid off staff in last months, is reportedly hiring again: times are hard, but all is not doom and gloom.

Notably, crypto exchanges are heavyweights in the crypto job market. They are the ones making money, so no surprise there!

The current adverse climate can be explained by either over-optimistic expectations or too many pilots that delivered disappointing outcomes. Either way, this is another indication, in line with others, that the hype surrounding blockchain technology is plumbing new depths.

CONCLUSION ON WHICH CASH ENTERS AND LEAVES THE CRYPTO ECO-SYSTEM

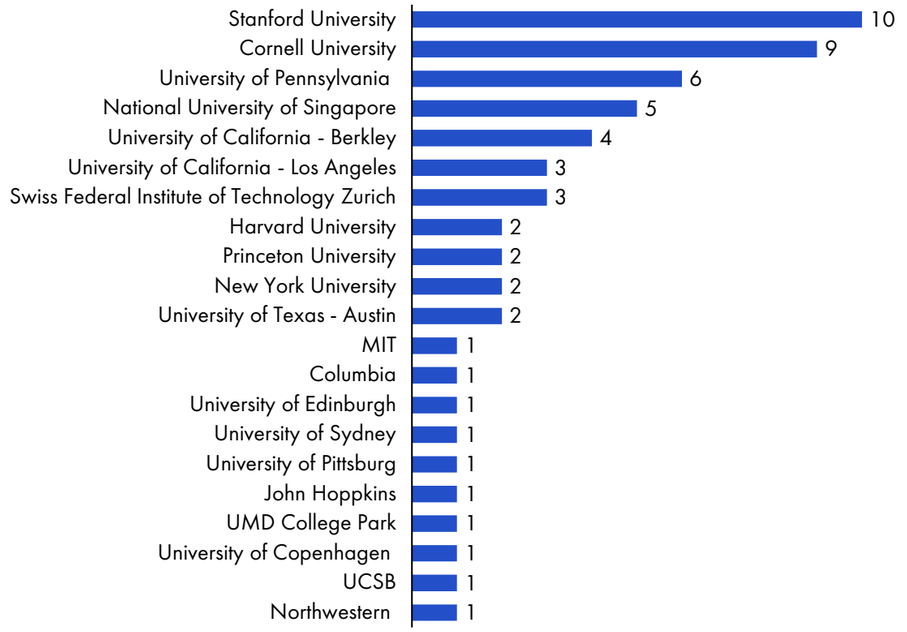
This quarter again, it is quite challenging to identify the money that is flowing in and out of crypto ecosystems.

ICOed start-ups are running out of the BTC and ETH they raised. Miners are supposed to be waiting for the halving, to sell their holdings at a more favorable price. Exchanges are seeing lower volumes. All these factors combine to indicate a relative stabilization of outflowing cash.

Most market actors currently have a wait-and-see attitude, with individual investors, in particular, having no influence on price action. Institutional investors are still not involved at all, and one can doubt the kinetics with which they might join.

FIGURE 13:

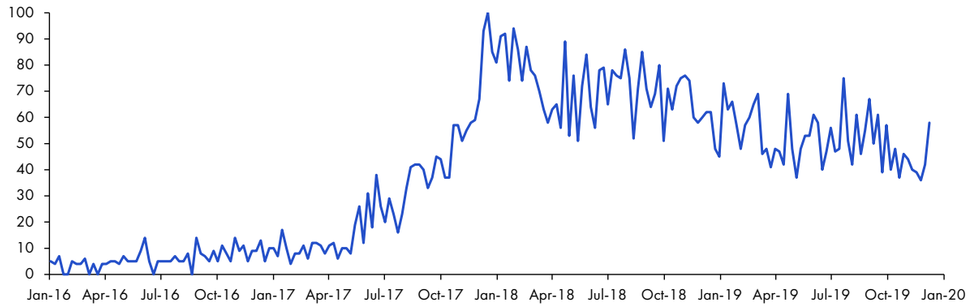
CRYPTOCURRENCY AND BLOCKCHAIN COURSES AT TOP UNIVERSITIES



Source: Coinbase

FIGURE 14:

INTEREST IN BLOCKCHAIN DEVELOPER POSITION (INDEX=100 - AT PEAK)



Source: Google Trends

4 INVESTMENTS & USE CASES BY INDUSTRY

Here are highlights of the latest DLT applications by sector. Note that this section has no intent to propose an exhaustive view, given the abundance of major projects going on.

BANKING

End-customer payments

A subsidiary of Ripple in Asia, in cooperation with a local banking company, has launched a money transfer service between Japan and Vietnam.

HSBC has announced it has completed two blockchain letters of credit transactions — one between firms in Saudi Arabia and Bahrain, and another between companies in Oman and Abu Dhabi. HSBC declared: "As the world's leading bank for trade finance, HSBC is actively supporting the adoption of technologies such as blockchain to make global trade faster, safer, and simpler." There is no particular technical prowess here, but to mention, the technology used is Corda.

Interbank settlements

Accenture and SAP have unveiled a Corda prototype for real-time gross settlement systems. Its promoters describe it as "another payment channel for central banks. And the idea behind this is to use tokens for settlement purposes." Corda is the platform used for the project: the solution will run alongside existing systems enabling tokenized payments to be received as regular payments by a non-participating bank. The distributed ledger technology component is integrated with the existing SAP Payment Engine.

The Swiss bank, UBS, is leading a team of four of the world's biggest banks in developing a system to enable financial markets to make payments and settle transactions quickly using blockchain technology. It will rely on a "Utility Settlement Coin" (USC), which is a digital cash equivalent of each of the major currencies backed by central banks, such as the dollar and euro. The USC will be convertible at parity to a bank deposit in the corresponding currency, making it fully backed by cash assets at a central bank.

Trading and settlement

Many initiatives that propose trading platforms for business continue to blossom. Enerchain is one for energy trading; VAKKT is another that was developed in Portugal for oil trading; DBS (a Singaporean bank) is also partnering with Trafigura to build a commodity trading platform. The objective is straightforward and the same with all of the proposed systems: remove manual processes, paperwork and reconciliation jobs, and automate accounting. We can be sure that such systems are the future for trading platforms.

Marco Polo is a project that is particularly interesting to highlight. Built directly by R3 since 2017 and running on Corda (though not yet in production), it keeps attracting new actors from all horizons, which lately include the National Australia Bank and Mastercard. Marco Polo differentiates itself from other blockchain trade finance networks, because it proposes integration with enterprise ERP systems, hence bringing trade finance options to the fingertips of corporate treasurers. Twenty-five companies are currently members.

One pain point that blockchain has the potential to solve, in addition to removing the middle man, is the pricing of commodities. A typical example is gold: the process leading to the fixing of the gold price is currently quite opaque, involving only a handful of well-identified trading offices that set the price and exclude all other market participants. In the twenty-first century, this is hardly understandable: the current system is surprisingly relationship-focused and prone to manipulation. Allowing for more transparency thanks to a DLT-based system would allow for much more efficient price discovery, more dynamically and accurately reflecting bids and offers.

Please also refer to the paragraph on the Ownership of Crypto Assets.

INSURANCE

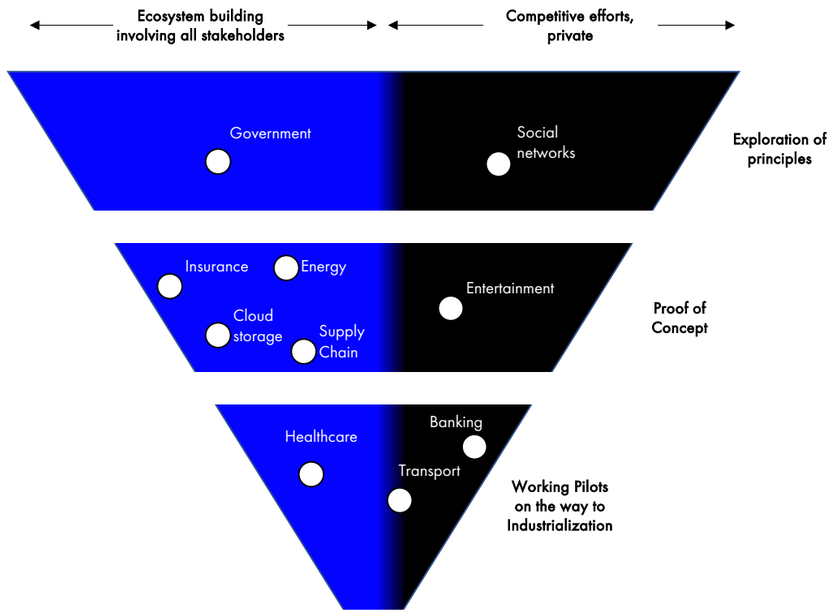
The U.S. Federal Emergency Management Agency (FEMA) now recommends using blockchain to expedite insurance payouts in the event of a disaster. It considers that "blockchain for parametric insurance is well suited because smart contracts can automatically trigger payouts if certain conditions are met." One of the reasons for the recommendation is the observation that hurricanes Maria in Puerto Rico, and Harvey in Texas, have caused citizens to lose essential documents such as insurance policies, land ownership records, and personal identification needed to file a claim – problems that DLTs can solve.

FEMA NOW RECOMMENDS USING BLOCKCHAIN TO EXPEDITE INSURANCE PAYOUTS IN THE EVENT OF A DISASTER.

B3i is now live, after having switched from Hyperledger Fabric to Corda. This year, a round of funding among the sixteen participants raised 22 million euros. The developed solution is called CAT XL; for now, it purely focuses on the placement of the reinsurance contract – but the purpose is to ultimately handle accounting, payments and claims. And as a first step, rather than requiring integration with participant systems, the data is entered via a web browser. But being able to share the contract, associated files, and the negotiation process is a big step.

FIGURE 15:

CLASSIFICATION OF BLOCKCHAIN USE CASES



Source: BQ Intel

SUPPLY CHAIN

Walmart Canada has announced it will begin using blockchain technology to track deliveries, verify transactions, and automate payments and reconciliations between the retailer and 70 third-party trucking companies. The system, set to go live at all third-party carriers in Canada by February 2020, will use a shared ledger to integrate and synchronize supply chain and logistics data in real-time. The platform will enable real-time invoicing, payments and settlements while integrating with each company's legacy systems. [scsoluionsinc.com]

Aeronautics supply chain is among the most demanding in the world; hence it comes as no surprise that a transition of component traceability and follow-up management to the blockchain is envisaged for this demanding sector: for an aviation component, several events occur, including approval, production, removal, testing, repair, reinstallation, etc. An initiative called FLYDocs has been launched with a multiparty approach allowing anyone to join, from all areas of the industry.

A borderline supply chain initiative called Travelport, using Hyperledger Fabric to track hotel bookings made through travel agents, to track and hopefully rationalizing fees paid to agents, based on the value of the accommodations reserved through their intermediary. This is an interesting move, originating with an idea to use traceability to claim compensation for a referral service; however, these intermediaries may well fear that the transition of the booking business to blockchain could reduce their share of the cake, as an efficient DLT-based platform to handle hotel bookings may reduce their business territory, re-centering them to the provision of assessment and advice, and be compensated, not with a commission, but a fixed fee.

KPMG has launched "KPMG Origins," a platform to compete with EY's OpsChain to serve as an infrastructure to provide transparency and traceability, initially for agriculture, manufacturing, and financial sectors. This shows that auditing companies are increasingly contemplating how they should position themselves in a world where accounting systems can shift to a blockchain, and maybe even envisage offering their services as a platform of trust, industry by industry.

Please also refer to the standardization chapter regarding efforts in the industry to capitalize on the various pilots conducted so far.

INFORMATION AND TELECOMMUNICATIONS

Tencent has announced that it will launch a blockchain-based virtual bank. The company's blockchain chief, Yige Cai, has revealed that the Hong Kong Securities and Futures Commission (SFC) has approved a new license and that the company is setting up a team to support the platform. [pymnts.com]

Huawei is approaching technology at large with an approach that involves "smart cities"; in this regard, blockchain is one aspect of their fintech adoption.

MEDIA, INCLUDING SOCIAL NETWORKS

In the cryptosphere, some players, like eToro, have called for Facebook to integrate existing stablecoins into the platform, instead of pushing Libra. And indeed, there is no doubt that if Facebook endorses any cryptocurrency on the platform, it will trigger an immediate and colossal adoption!

According to Gartner, an American information research and advisory firm, by 2023, up to 30% of world news and video content will be authenticated by blockchain ledgers. This comes as a prediction aimed at tackling the "fake news" phenomenon, which is increasingly used by some governments to manipulate public opinion and elections: indeed, traceability is essential to almost everything, and can be applied to information as well!

However, Korean social media appears to be moving in the direction that Facebook wanted to go. Yeo Min-soo, the CEO, has stated that his firm's Klaytn blockchain is way ahead of Libra in its development, with similar intentions.

An application, Pepo, claims to be the first DApp approved for use on Apple-Pay. It consists of a wallet, coupled with a platform that enables the tipping of content (video) creators.

ENERGY

The reader can refer to Alpiq's publications.

TRANSPORTS

Air

Air Canada is following the trend of other airlines (Etihad, AirFrance-KLM, S7 and Norwegian) as outlined in the previous Quarterly, in building a blockchain-based platform for its agents and customers to purchase and manage tickets.

In November, a German company, Hahn Air, also moved to issue tickets on the blockchain.

Automotive

Volvo has declared that it is examining DLT-based solutions to track its supply chain of Cobalt. Electric car production is increasing the demand for this mineral, and mines that employ children will be banned from the procurement circuit.

Shipping

The Port of Marseille has completed a blockchain pilot led by Marseille Gyptis International and start-up, Keeex. The Port Authority has declared that the project "demonstrated that harmonization of the

digital transport chain improved fluidity, reliability, and competitiveness of pre- and post-forwarding on the crucial hinterland axis."

HEALTHCARE

In healthcare, blockchain is moving slowly from proof of concept to real implementations. After pilots of a range of use cases, including supply chain, consent management, and patient data management, we are starting to see the first set of use cases moving into production. The Swiss pharmaceutical company, Novartis, has indicated that it intends to ramp up its focus on blockchain in 2020, and will go live with its first two use cases; third-party risk management, and digitizing manual processes to increase efficiency.

NOVARTIS LAUNCHES ITS FIRST TWO BLOCKCHAIN PILOTS: THIRD-PARTY RISK MANAGEMENT AND DIGITIZING MANUAL PROCESSES TO INCREASE EFFICIENCY

Consortiums are growing, such as Synoptic, Hashed Health (Professional Credential Exchange), Insureum, and MediBloc. Novartis is also leading a blockchain healthcare consortium as part of the Innovative Medicines Initiative. So far, 28 entities are onboard, including 11 pharma companies.

This European-funded program aims to establish a typical blockchain ecosystem for pharmaceutical development, manufacturing and distribution that provides an incentive and serves as the basis for all participants to engage, adapt and benefit from. The project will initially establish a practical approach and governance organization to enable continuous improvement and open competition among service providers while ensuring that critical factors such as data integrity, privacy, regulatory compliance and efficiency are built into a 'Healthcare Foundation' that serves as an integration layer between underlying blockchain technologies and the business application layer.

ADMINISTRATION AND POLITICS

Canada and the Netherlands have announced that they are working on a pilot project with the World Economic Forum and consulting firm, Accenture, to replace passports with smartphones. Blockchain will help to store the information securely.

Blockchain is being used for military purposes. The Indian Defense Minister has declared that "emerging technologies such as blockchain have the potential to define the war industry over the coming decades. Data and data sharing will be critical for warfare in the future, particularly with the development of artificial intelligence." Specifically, the focus is on protecting weapons from hackers. Using distributed ledgers to record the status of equipment, and logs of all interventions could, for instance, help to ensure that no attacker can modify missile launching software without being detected. Authentication on a blockchain will be required to do so.

The potential for verification of diplomas and certifications through records on a blockchain is increasingly being recognized by university administrators, with the hope of reducing the administrative costs of manual checking.

GAMING AND ENTERTAINMENT

Obviously, since Cryptokitties there has been no on-chain game success story. For a sector that tends to adopt technological changes, and with all the effort and investment in this sector, this says that, for a range of reasons, including maturity, technical and financial, at this point, there is no case for blockchain-deployed games.

CONCLUSION ON INDUSTRIAL APPLICATIONS THROUGHOUT SECTORS

Overall, there is no shortage of pilots and projects under development worldwide and across a range of industries. The most active sectors are still finance/banking and supply chains.

All in all, we observe a catch-up by corporations in the tech domain, compared with start-ups that made much noise initially, but which are currently struggling to achieve their dreams. Worth noting, in terms of research, is the number of patents applied for, which is an interesting indicator. The top three companies by the number of issued blockchain-related patents are Alibaba, IBM and Mastercard.

Otherwise, we can only confirm the trend that we highlighted in the previous issue of BQ: consortiums and joint work by all actors in any given ecosystem are more and more observable, as we reckon they are critical to the definition of DLT-based infrastructure, which can be then used by competitors to build their applications. Please refer to the standardization section regarding this aspect.

5 TRENDS BY CRYPTO-ASSET CLASS

CLASSIFICATION

As BQIntel is developing, we engage in providing tools to compare crypto-assets with each other, thanks to the creation of a database and of a suite of tools to exploit it. A primary added value is to use our classification as a criterion to isolate classes of tokens and study them as such.

As an evolution to fine-tune our classification framework, we are now refining by creating sub-categories for each of the functionalities. As part of this move, the E (Execution) functionality becomes a subcategory of the I (Infrastructure) function.

Just one remark worth mentioning as far as the classification is concerned, when designing and proposing DLT-based processes within corporations, the question arises within the Finance Departments of how to enter crypto-assets in the books. Accounting standards have not yet thoroughly thought and published principles for this, so that companies can follow in which accounting category they have to put Ether, Bitcoin, Tokenized gold, not to mention depending if they proceed from mining, from received proceeding of activities, from speculative acquisition, or whatever. Here again, the consideration through mapping of the 5 categories could prove very interesting for accounting researchers to work with.

A – ANONYMITY CHARACTERISTIC

Prices of anonymous cryptocurrencies have been struck at the end of 2019. Compared with mainstream Bitcoin, or even native mainstream infrastructure tokens, Monero, Dash, ZCash, MimbleWimble and the like are losing momentum.

Of course, governments are likely to resolutely fight these crypto assets, because they support the anonymous movement of the value, and hence would be the preferred medium of exchange for offenders in parallel economies. However, it is precisely this that makes the sluggish situation surprising, if not worrisome: there is a clear use case for anonymous cryptocurrencies, yet they are not following their usual tendency to resist downturns.

I INFRASTRUCTURE NATIVE CRYPTO-ASSETS

I(Ē) – Pure accounting infrastructure functionality

Bitcoin

Bitcoin's Proof of Work reward will be halved around May 2020. This is written in the protocol, and is, therefore, no surprise, just the previous occurrence in mid-2016, which reduced the price paid by the network to winning miners from 25 to 12.5 BTC per block. This time, the reward will be reduced to 6.25 BTC per block. This means that all of a sudden, the number of "fresh" bitcoins being created and brought to the market by miners is going to be halved, causing a significant supply shock.

When examining the BTC price history and attempting to identify the potential impact of the halving, it is quite apparent to any observer that the price usually increases after the halving, and continues for some time after. The price history indicates that increases have occurred after previous halvings. This is why, today, many commentators believe that this may very well again be the case, and in the coming months, a bull run could develop in the same way it did in 2016-2017.

WHEN EXAMINING THE POTENTIAL IMPACT OF THE HALVING, IT IS QUITE APPARENT THAT THE PRICE USUALLY INCREASES AFTER THE HALVING, AND CONTINUES FOR SOME TIME AFTER

This is one of the strong arguments we see again and again these days, supporting the idea that the price of BTC may soon skyrocket. However, others claim that the price adjustment related to the halving has already been taken into account; the rally in the spring of 2019 was just that. So, speculation is on!

Even though it may have been forgotten since 2018, the primary problem for Bitcoin is still, of course, the war that the most powerful governments on the planet will wage against it. J.P. Morgan's Chief Executive, Jamie Dimon, once told a group at a Fortune Global Forum that "Bitcoin would likely be stopped by the U.S. government before it became a true currency of use."

In other words, there is nothing more specific than the fact that the US government will defend the USD as the world's currency, which is a fantastic tool of foreign policy power. Whether the US government can stop Bitcoin remains to be seen, despite Dimon's apparent faith in the almighty Washington administration. However, at least the fight over pure cryptocurrencies, should they gain acceptance worldwide, is going to be paralleled by the Chinese and probably the Indians, which together are a nice chunk of the world's population and business.

So, even if we are confident that nodes will continue to run indefinitely, and that there will always be a jurisdiction that will brave the rest of the world by allowing this for the sake of attracting crypto businesses (and money), major governmental crack-downs on non-official currencies that could undermine their power, is a sure thing. The question we should be asking ourselves is this: where is the equilibrium point of mutual acceptance, beyond which governments will attack cryptocurrencies, and below which the appeal to populations shall cause their increased usage? We do not have the answer.

High-resolutoin image of the table is available for download at:

bqintel.com/dlt-infrastructure-compare

PLATFORM NAME	COMMENTS	CONSENSUS MODE	CONTROL ON PARTICIPATING NODES	MARKET SIZE, $M (updated Jan-2020)	DATA CONFIDENTIA-LITY	TRANSACTIONS/ SECOND PER SHARD	APPROACH TO "SCALING TO INFINITE"	VALIDATION TIME	SUPPORT OF SMARTCON-TRACTING	COST OF EXECUTION	MATURITY OF THE PLATFORM	CURRENCIES AVAILABLE ON-CHAIN	DEVELOPMENT TEAM ROBUSTNESS	DEVELOP-MENT ECOSYSTEM
ETHEREUM (pre-PoS upgrade)		PoW	Public distributed ledger	18,400	Not easy - to be engineered specifically	1x	Sharding from a "Beacon-chain"	10s	Built-in, Turing-complete	Gas, market price; can get expensive	Available	All sorts	State-of-the-art and well funded	Largest existing
EOS	Criticized for not being decentralized	dPoS	Pseudo-centralized; inconvenients from both world	4,000	Not easy - to be engineered specifically	100x	Sharding	Around 2 blocks per second	Built-in, Turing-complete	Free; paid through dilution over time	Available	To be introduced by ad hoc bank; no technical problem	Important and well funded	Large. And EOS's smartcontract code is non specific
TRON	Focus on "dWeb"; based on Ethereum logic, with 27 elected nodes every 6h	dPos	Pseudo-centralized; inconvenients from both world	1,200	Not easy - to be engineered specifically	1000	Probably some sort of sharding (a priori)	Around 2 blocks per second	Built-in, Turing-complete	Minimal	Available	To be introduced by ad hoc bank; no technical problem	Heavily criticized for not being able to deliver	Smartcontracts in java (=not specific)
TEZOS	Focus on on-chain governance	LPoS	Public distributed ledger	1,200	Some expressed plans to implement reccursive SNARK	1,000	Reccursive SNARKs... To be demonstrated	60s	Built-in, Turing-complete	n/a	Still developing, especially the smart-contracting environment	To be introduced by ad hoc bank; no technical problem	Contradictory comments; lots of mess with the Tezos Foundation	Own language: Michelson
CARDANO		PoS	Permissionning is possible	1,100	Not easy - to be engineered specifically	100x	Sharded	Adjustable in Ouroboros, never lower than 0.5s	Built-in, Turing-complete	n/a	Yet to be deployed	To be introduced by ad hoc bank; no technical problem	Research-oriented, technically excellent	Decent
STELLAR		Federated Byzantine Agreement	Public distributed ledger	1,100	Not easy - to be engineered specifically	1000x	Not debated yet; sharding not a priority due to already decent throughput rate	3s	Not Turing-complete	Minimal, just to prevent network flooding	Available	To be introduced by ad hoc bank; no technical problem	Decent	Decent
NEO	Same family as Ethereum	Delegated Byzantine Fault Tolerant	Public distributed ledger	800	Not easy - to be engineered specifically	100x	Probably some sort of sharding (a priori)	10s	Built-in, Turing-complete	Gas principle	Available	Finance oriented, assets a priori on-chain	Chinese	Non-specific programming languages
IOTA	Direct Acyclic Graph	Gossip of gossip, + currently authority by IOTA foundation; ultimately PoW	Public distributed ledger	600	Not easy - to be engineered specifically	1000x	In DAG structure, more participants, higher security and throughput	<1s	Not supported natively	n/a	Available	Just IOTA as long as no smartcontracting can be agreed upon	Controversial opinions expressed about the team and the technology	Modest
COSMOS		Byzantine Fault Tolerant	Permissionning is possible	900	Not easy - to be engineered specifically	100x	Specific architecture of sharding	<1s	Not supported natively	n/a	Maturing	To be introduced by ad hoc bank; no technical problem	Decent	A number of real projects use it

BEST AMONG PEERS WORST AMONG PEERS

PLATFORM NAME	COMMENTS	CONSENSUS MODE	CONTROL ON PARTICIPATING NODES	MARKET SIZE, $M (updated Jan-2020)	DATA CONFIDENTIA-LITY	TRANSACTIONS/ SECOND PER SHARD	APPROACH TO "SCALING TO INFINITE"	VALIDATION TIME	SUPPORT OF SMARTCON-TRACTING	COST OF EXECUTION	MATURITY OF THE PLATFORM	CURRENCIES AVAILABLE ON-CHAIN	DEVELOPMENT TEAM ROBUSTNESS	DEVELOP-MENT ECOSYSTEM
ONTOLOGY	Based on NEO	Delegated Byzantine Fault Tolerant	Public distributed ledger	440	Not easy - to be engineered specifically	4000	Sharding, probably like Ethereum	15s	Built-in, Turing-complete	Gas principle	Available	To be introduced by ad hoc bank; no technical problem	Decent	Non-specific programming languages
VECHAIN	Thought from the beginning for traceability and supply chain	In between Proof of Authority and Proof of Stake	Public distributed ledger	300	Not easy - to be engineered specifically	100x	Probably some sharding (not specified) - but already good scalability in basis	10s	Built-in, Turing-complete; specific logics available serving supply-chain use cases	Probably minimal	Available	To be introduced by ad hoc bank; no technical problem	Modest	Modest
QTUM	Implementation of a VM based on BTC's like UTXO logic	PoS	Public distributed ledger	200	Not easy - to be engineered specifically	10,000	Unknown	15s	Built-in, Turing-complete	Gas, market price; can get expensive	Available	To be introduced by ad hoc bank; no technical problem	Modest	Specific Qtum smart contract language
NANO (ex-RAILBLOCKS)	Direct Acyclic Graph	Vote of "representative" nodes on gossips of gossips	Public distributed ledger	100	Not easy - to be engineered specifically	1000x	In DAG structure, more participants, higher security and throughput	4s	Not supported natively	n/a	Available	Just NANO as long as no smartcontracting can be agreed upon	Decent	Modest
ZILLIQA		PoS	Public distributed ledger	50	Not easy - to be engineered specifically	100x	Specific architecture of sharding	60s	Not Turing-complete	Likely to be gas principle	Available	To be introduced by ad hoc bank; no technical problem	Decent	Unknown
LIBRA		PoS	Permissionned, governed by corporations	N/A	Transparent	1000	Not envisionned	1s	Built-in, Turing complete	Zero; consortium rewarded by interest on collateral	Yet to be deployed	Libra native	Nascent	Nascent
CONCORDIUM		Proof of Stake (with some refining on incentivation)	Permissionned	N/A	Yes, promise	100x	Sharding	Combination of PoS and BFT allowing for fast confirmation	Built-in, Turing-complete, and promise to make them upgradable	Gas principle (pre-calculated)	Yet to be deployed	To be introduced by ad hoc bank; no technical problem	A priori good	Just starting; own language Oak
CORDA		Relies on ad hoc Notaries identified beforehand	Access to the network is public, but records are privates	N/A	Yes	1000x	Naturally sharded as groups of nodes can talk directly	~2s	Built-in, Turing-complete	Free in principle; cost of running nodes and remunerating notaries	Available	Finance oriented, assets a priori on-chain	A priori good	A number of real projects use it
DFINITY	"Public decentralized cloud hosting next gen of software and services"	Proof of Stake	Public distributed ledger	N/A	Not easy - to be engineered specifically	1000	Unknown, probably sharding	120s	Built-in, Turing-complete	Gas principle	Available	To be introduced by ad hoc bank; no technical problem	A priori brilliant minds contributing	Just starting
ETHEREUM (post-PoS upgrade)		Proof of Stake	Public distributed ledger	N/A	Not easy - to be engineered specifically	1000	Sharded	16s	Built-in, Turing-complete	Gas; price is manageable; if too expensive then new shard created	Yet to be deployed	All sorts	State-of-the-art and well funded	Largest existing

BEST AMONG PEERS WORST AMONG PEERS

Deflationary cryptocurrencies
The experiments with deflationary cryptocurrencies are failing miserably. Even if one can argue that it is due to the turmoil in crypto prices, it is difficult to find a fundamental difference between these and asymptotic money creation, such as bitcoin. It looks to us that the size and security of the network is the prime parameter for broader adoption; the actual mechanism of money creation might ultimately matter little.

(I)E – Execution environments platforms
Please refer to the section on the technical development of infrastructure platforms.

F – FINANCING FUNCTIONALITY FAMILY

"Utility tokens" 2017-style ICOs
ICO tokens, issued in 2017, which skyrocketed in 2018, continue to collapse on the markets. Quite clearly, this shows, in financial markets, very low liquidity (even for utility titles, if you prefer to name them that way) is a source of pressure on the actual price of the asset. Regardless of how the teams are performing (some are still active and struggling to deliver a product), the fact is that some tokens are vulnerable to investors who are willing to exit, putting downward pressure on the price. Even if this is perhaps just an artifact of having a continuous quotation, as opposed to no transaction in classical venture capitalism, the reality is that it endangers the company, which is then under scrutiny and unable to raise further capital if it needs to.

Trying to raise money in the 2017 fashion is not convincing many investors, to say the least – teams that are still trying to do so, do not appear to be very serious. The financing scheme of 2017-style ICOs has not converged and will need to be appropriately reworked (if this is feasible) to succeed.

Ripple's CEO has stated that he believes that the vast majority of cryptocurrencies have no future, and foresees that 99% will fail and that only a few key projects will be able to solve an actual problem and be able to scale. This analysis, no doubt, apply to tokens that were issued to finance dubious platforms, and, with reason, are being wiped out by the market.

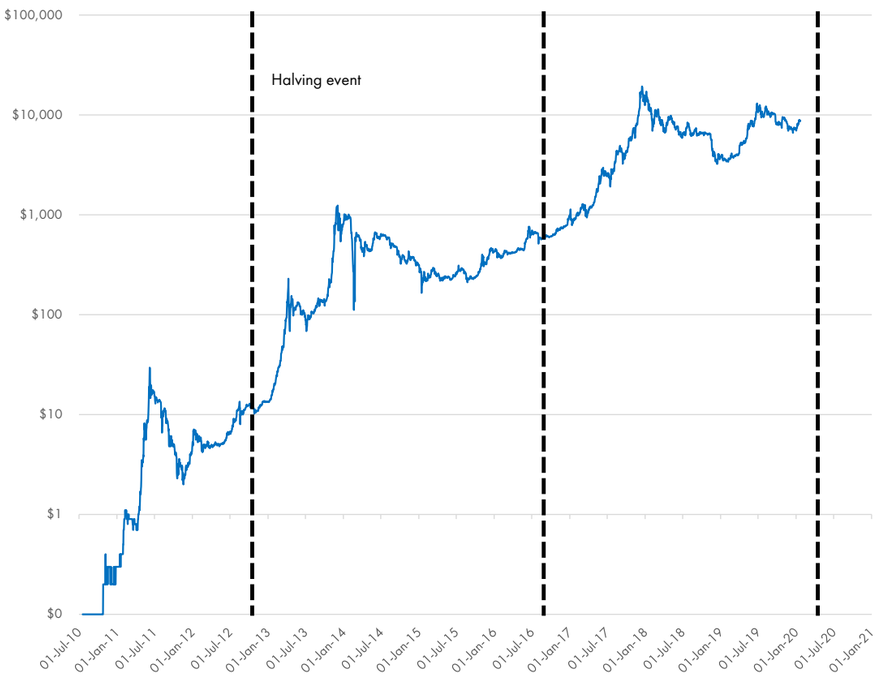
Securities tokens offerings
Very few 'use-cases' appear more evident than the management of financial titles as tokens on distributed ledgers. Importantly, there is no real technical issue here, at least not in terms of algorithms. The feasibility is purely a matter of regulatory acceptance and the legal infrastructure to ensure the enforcement, in the real world, of an on-chain title.

The start-up, BnkToTheFuture, estimates that as early as 2020, 50% of the security offerings will be digital and on a blockchain. It might not be that fast, but we observe that things are moving:

- A theme park in Thailand has issued its security tokens with the help of Via East West Capital.
- Fundament, a German company, has received approval from the BaFin (German regulator), authorizing the tokenizing of real estate. The company intends to use the Tezos technology.
- Securitize has received Japan's SBI Investment funding.

FIGURE 17:

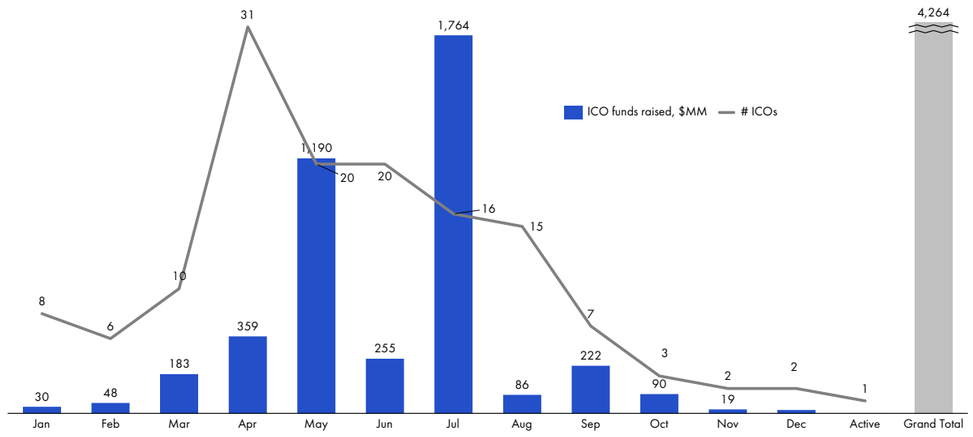
EVOLUTION OF BITCOIN PRICE AFTER HALVING



Source: bitcoin.com

FIGURE 18:

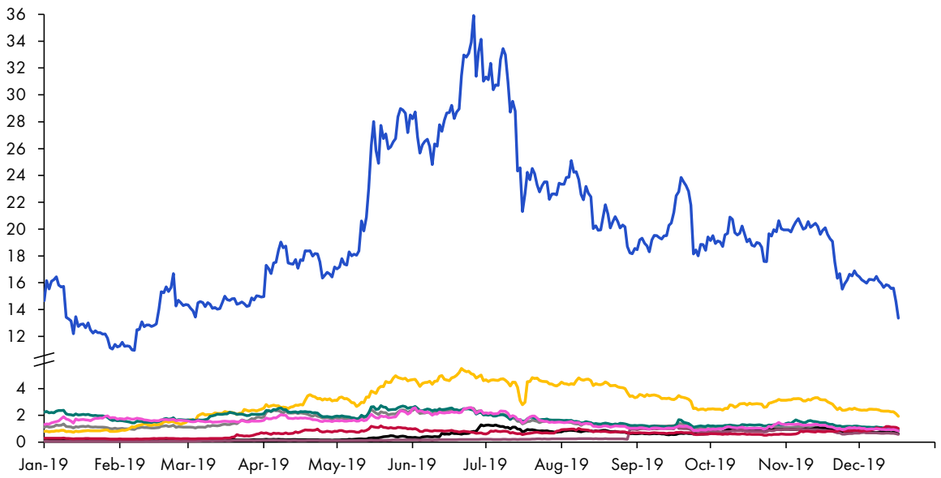
ICO FUNDING & #ICOS IN 2019



Source: icodata.io

FIGURE 19:

MARKET CAPITALIZATION OF TOP UTILITY TOKENS OVER TIME, $BN



Source: CoinMarketCap

• Harbor, a security token platform, has received a "transfer agent license" from the SEC. Before that, the startup Blockstack was the first to receive the go-ahead from the SEC for a $23 million capital raising under Regulation A+.

Initial Exchange Offering (IEO)

During the summer of this year, there was a race between exchange platforms to position themselves as partners for the introduction of start-up fundraising – that is, after all, what it is.

IEOs have been successful so far: reportedly, 1.5 billion euros were raised this way in the first half of 2019. An important observation is that this money has gone to quite a limited number of companies because serious exchanges are not accepting all projects – their reputation will be at stake if the money vanishes in a scam, or if the team behind the project is so weak that nothing eventuates.

But of course, changing the logistics and adding an intermediary does not immediately improve the quality of projects available; as of now, IEOs are not occurring to the extent one could have expected. Rather than regarding this as proof that Binance, Bittrex, and the like are unsuited for the initial offering of tokens and other securities, we believe that it is, instead, an indication of the moderate dynamism of the cryptosphere as of the second half of 2019. Fundamentally, and provided some due diligence can be delivered efficiently to investors, IEOs can succeed. And, by the way, the essential characteristic of a successful listing is likely to be liquidity, which in turn will be higher for large, well known and expected projects. So, just like today, for established companies, financing on the markets is much easier than when you are a small, unproven business. Things are not changing that much!

The evolution of IEOs will result in a pure listing of the issued tokens. An initial listing, true, but in practice, that is relevant to how it works. Behind the scenes, the fundraisers will ensure supply, as this will be in their best interests, and according to established best practices, that will enable efficient price discovery. But market mechanisms will prevail as soon as the tokens are released to the public. For liberal observers, this will be good news; for less liberal-minded people, there is obviously an urgent need to prevent market manipulation. Again, regulations will have to adapt, but only marginally in order to accommodate and support the management of crypto assets.

O – OWNERSHIP REPRESENTATION

Financial securities

Importantly, tokenized financial securities can only gain momentum, and ultimately replace the way they are currently managed if the infrastructure to handle them is in place. In this respect, development is ongoing.

• Deutsche Bank, jointly with various companies, has recently announced the successful implementation of distributed ledger technology for the settlement of tokenized securities. Swisscom and Zürcher Kantonalbank were part of the trial. It convincingly demonstrated that DLTs could provide an instant and secure means of settling trades involving securities.

• Another initiative by Paxos in New York (USA) is geared in the same direction. Wall Street has not yet shown much enthusiasm in embracing the technology, but the SEC has just authorized Paxos to "conduct a two-year pilot project for settlement and clearing of securities on a distributed ledger." So, this opens the door for blockchain experimentation in the infrastructure of money markets in the US.

• J.P. Morgan has also reported it has developed a distributed ledger-based solution to manage margins for derivatives trading.

• All of these privately-proposed systems add to other projects, such as those undertaken by the Australian Stock Exchange and the Swiss Stock Exchange (SIX), of Gibraltar, etc. to manage ownership of securities on the blockchain.

Of course, there is nothing very technical here. Nevertheless, it is essential to observe corporation transitioning to the new IT infrastructure. The benefits are numerous: faster and more efficient business processes that currently can take days, reduced operating costs, elimination of errors, reduction in labor costs – and all of this accessible worldwide.

Real estate

While not a financial security, real estate is another obvious application of blockchain that has excellent potential. In countries that include Germany, China, and Hong Kong, there is an ever-increasing number of projects holding discussions with regulators to confirm the suitability of managing property titles on distributed ledgers.

Commodities, including precious metals

However, there is not much momentum by pure players towards the tokenization of commodities.

What we observe, though, is that commodity exchanges are showing a willingness to build new infrastructures, hopefully, based on blockchain, thereby creating alternative exchanges with a clear objective to exclude brokers. So, to an extent, this is arriving at the same destination, but the other way around: instead of having new companies provide the service of tokenizing the physical assets and ensuring redemption, we are talking about established traders and financial institutions being qualified immediately to take positions, even virtually, and coming together to define the protocol according to which these tokens are going to be exchanged and managed in the ecosystem.

Loyalty program points

Here the frontier between privately emitted

money and coupons is becoming really blur. As Walmart is studying the opportunity to introduce its cryptocurrency, we see how the continuum in the qualification of crypto-assets managed on the blockchain is getting impossible to separate.

Collectibles (art, luxury or historic objects, etc.)

There has not been much progress in the tokenization of collectibles since we last discussed this topic. Technically, there is no complication; it all depends on the related logistics and the management of tokenized assets, which, at this stage, is not mature, hence preventing the transition to blockchain platforms.

THE USAGE OF CRYPTOCURRENCIES FOR EVERYDAY PURCHASES IS STILL ALMOST NON-EXISTENT, AND NOT GROWING. WHY IS THAT?

P – PAYMENT FUNCTIONALITY

Acceptance in retail

As of today, marginal acceptances keep popping up now and then, but not much more. The usage of cryptocurrencies for everyday purchases is still almost non-existent, and not growing. Why is that? Let us see if we can find reasons for this lack of growth, and identify what it would take.

First, of course, as always, is the issue of scalability. As long as scalability is not resolved and no pressure emerges on the use of traditional cash (such as a crisis triggering generalized quantitative easing), there is no fundamental reason for the mass adoption of pure cryptocurrency usage.

This is true, all the more, while cryptocurrencies remain volatile. Egg or chicken; the big question is, will volatility decline first, or is it the consequence of broader adoption of cryptos? The only thing we can be sure of is that mass adoption and stable volatility will coincide.

Regulatory uncertainty is a brake for conservative merchants, large and small. States enforce the acceptance of their official fiat, which is not the case with cryptocurrencies. This is seen by businesses as a risk that is not acceptable, and with few advantages to balance the risk. Existing payment systems work sufficiently well; so, there is zero pressure for retailers to change!

A layer of service providers to facilitate the use of cryptocurrencies is desperately missing. TenX, Crypto.com and the like have failed to deliver or gain momentum, which is a real pity. Indeed, it is evident that a facility for the live conversion of crypto assets to fiat money, acceptable by merchants, is vital for adoption. Strictly speaking, then, if using such services, the customer would be paying with cryptos, even if at a (limited?) cost. Note that one alternative would be to install a conversion facility on the merchant's side in a seamless way (this is the PundiX approach, and Cardano has recently attempted to launch its system to allow merchants to accept its currency, ADA).

Stablecoins

Crypto-collateralized and decentrally managed stablecoins continue to gain momentum.

In this respect, MakerDAO is a notable flagship: it has now issued $100M worth of DAI, collateralized by $300M worth of Ether. This amount was a limit established by the organization, but there is now a proposal to lift it to $120M, and it will then be subject to an on-chain vote. So, all in all, we are seeing that the Maker/Dai system works as expected and that it is continuously extending its reach. This is quite good news, showing that Ether can be valid collateral, when appropriately handled, to base value management on-chain for use in, notably, automated settlements of smart contracts. Already, the intent is to offer some loans on the platform, with an interest rate that will be voted on by holders of the Maker token.

Objectively, the MakerDAO system, its competition, is quite simple and cannot be considered an ultimate usable system. The over-collateralization mechanism is quite huge, and the entries and exits are not very dynamic – although, the wider the adoption, the more efficient it will become. Hence, the platform functionality is likely to evolve or be replaced by a more elegant and practical alternative. However, the principles are there and are valid.

As a side note, tokenized-fiat stablecoins can be expected to fade away when central bank-issued digital currencies are available.

Libra

The Libra project has encountered problems. PayPal is the first to withdraw from the association. Other partners in the project, Visa, Mastercard and others, have received a letter from the US Senate, stating, "Facebook appears to want the benefits of engaging in financial activities without the responsibility of being regulated as a financial services company. If you take this on, you can expect a high level of scrutiny from regulators not only on Libra-related activities but on all payment activities."

Some senators have prepared a bill, tailor-made so that Libra would qualify as a 'security.' It is unclear to us, though, how knowledgeable and honest regulators can believe that Libra is comparable to a financial instrument that is invested in, with the hope of an outstanding return. USD would then be considered a security under such an approach (note that governance tokens of the foundation may well be securities, but that is another debate). This proves just how lost these politicians are in understanding the profound nature of what is happening.

6 LATEST ADVANCEMENTS IN DLT TECHNOLOGIES

As usual, but specifically in this Section, it is assumed that the reader is up to speed with studies covered in previous reports. Past Blockchain Quarterly issues can be accessed through our website.

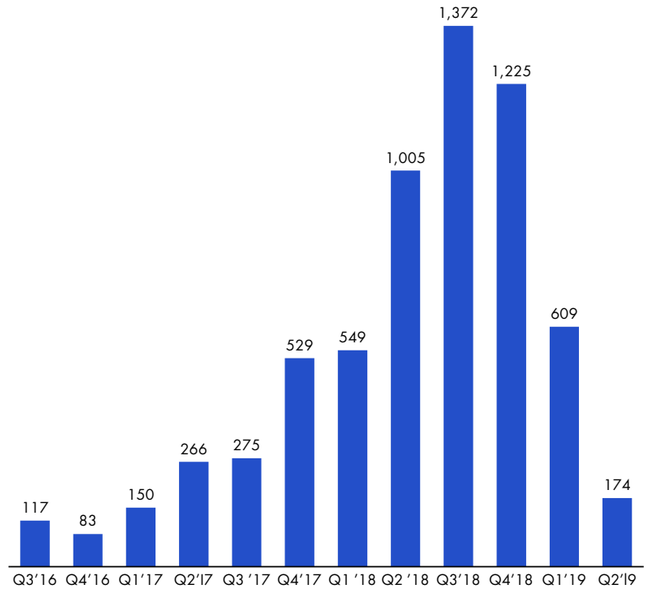
INVESTMENT IN DLT TECHNOLOGIES

Investment in the cryptosphere shifted throughout 2018-2019, from wild funding of small ventures through ICOs, to large companies creating their innovation teams and paying for the development of enterprise information management solutions. So, the financial investment is by no means down, although the current state of the cryptocurrency market is more worrisome.

Unknown Fund has been created by the Anonymous 'hacktivist' organization specifically to invest $75 million (of Bitcoin) to boost privacy-preserving technologies. In an announcement, the group said that it considers the management of data as a powerful tool to manipulate people, declaring "The Unknown Fund sees incredible opportunities to protect the rights and freedoms of people that technology such as blockchain and cryptocurrencies give us. This is a chance for humanity to create a new environment, a new and honest monetary system, and to make the world a better place".

FIGURE 20:

EQUITY FINANCING ON BLOCKCHAIN SOLUTIONS (EXCLUDING ICOS), $MM



Source: Statista

CONSENSUS MODE – AND GOVERNANCE

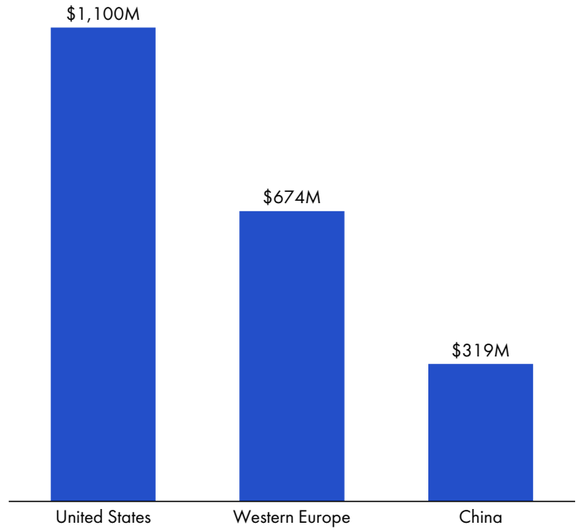
[Consensus method on DLTs is largely determining then the scalability of the infrastructure, and in general scalability, features need to be governed carefully. Therefore, we discuss these topics mostly within the scalability paragraph.]

Technical developments on consensus modes

The consensus mechanism intended to be used on the Concordium

FIGURE 21:

PROJECTED SPENDING ON BLOCKCHAIN IN 2025, BY REGION



Source: Statista

blockchain is worth examining, as it is quite elegant. The principle is to combine a Proof of Stake mechanism that ensures fast block production, and hence, a decent throughput rate, with a Byzantine Fault Tolerant mechanism on some blocks that allow for safe finalization. The combination of "the best of both worlds," as they put it, results in a chain that is both lively and safe, which means that the PoS fast consensus, which is prone to forking, is surely converged by the BFT college, whose requirement of a percentage of consistent votes can be adjusted.

2019 WAS ANNOUNCED AS THE TAKE-OFF YEAR FOR THE LIGHTNING NETWORK AS SOLUTION TO THE SCALABILITY ISSUE - THIS HAS NOT BEEN THE CASE.

Governance

There is a type of paradox, as far as governance, in general, is concerned. Industries and administrations, after gaining an understanding of blockchain's promises, are enthusiastic in identifying that it is going to help them with governance. Indeed, the more "liquid" the democracy, the more direct the contributions and votes, and, of course, tamper-proof authenticated records will build trust in governments, as well as leaders.

This, indeed, presents a very positive future, if you assume that the DLT infrastructure itself will be built appropriately. The only problem is that the governance of the blockchain itself is far from being resolved!

Governance is a problem that has several aspects. For example, who is going to have the authority/prerogative in managing the deployed logic? However, the most sensitive issue is the consensus model. The more control identified parties have on the agreement mechanism of what is written to the chain, the less decentralized it is, and the higher the risk of attack on the given individuals, even potentially from official bodies. Even in the case of full decentralization, governance is a concern: a 51% attack, whether it be stake or work-based, can never be totally ruled out, and having businesses running on platforms with the sword of Damoclès hanging over them, would likely result in loss of sleep for those responsible for continued operations.

We believe there are two ways things are likely to develop. These are likely to progress in parallel, as there is room for both approaches to succeed in their specific contexts.

The first one is the emergence of private "houses of trust," providing their clients, against a remuneration, an execution environment that they are (easily) accountable for. This first approach involves consortiums, whose governance today is through companies collaborating within a given industry; ultimately, a body will be in charge of running the execution environment, which eventually may or may not become independent. This will be at the discretion of its stakeholders.

The second is going to emerge, with no compromise in terms of decentralization. This is the aim of Ethereum, for instance. For this approach, concerns around the safety of the network may be resolved by intelligent consensus mechanisms being actively researched and developed. But most would agree that the best protection is always going to be the sheer size of the network, the required number of participants, which needs to be consistent in the long term.

Hard forks

Ethereum's hard fork, named Istanbul, has been successfully implemented. This was nothing special, really, just an expected step on the road to Ethereum 2.0.

SCALABILITY

Scalability in terms of transactions per unit of time

The news on the scalability front is not good. Analysts are starting to express the view that they do not expect to see full scalability within the next ten years.

Trusted Execution Environments

Research on providing Trusted Execution Environments (TEE) is taking off. This is somewhat paradoxical but makes perfect sense: if we can perform computation in local enclaves that trust each other to compute in parallel, can coordinate the sharing of information, and endorse transactions, then this part of the process can be removed from the main chain, thereby increasing scalability.

Companies as diverse as Visa, SuperComputingSystems, etc., are working on their own solutions in this direction. Cartesi is another project that is also proposing to rely on off-chain computation, available to any blockchain.

Importantly, the use of TEEs will also favor the introduction of privacy, as it is easier to keep information private if it is shared by only a limited number of participants.

Lightning network for Bitcoin

2019 was announced as the take-off year for the Lightning Network, driving BTC adoption, as it was seen as the solution to the scalability issue. This has not been the case.

The community has answered impatient critics in various ways. With a call for patience, claiming that the current poor user experience is the main factor behind the slow progress.

Claiming that Bitcoin is hodled, instead of being used as an everyday exchange medium because this is its inherent nature. In our view, this argument is not at all convincing!

Explaining that practical Lightning Network usage is hard to estimate, because, as a second layer protocol, its traffic is sort of "in private," and therefore cannot be aggregated correctly.

But all in all, the lack of adoption of LN has come as a disappointment to many – a concrete sign of overall difficulties within the DLT sector.

A different usage is being explored for the Lightning Network: the transmission of private messages. An application has been released, called Whatsat. It has always been possible to add some text to a BTC transaction, and, by extension, to a Lightning transaction.

Ethereum

During the Ethereum DevCon held in October in Osaka, Ethereum's main stakeholders conceded that Ethereum 2.0 was still some way down the track. Among the over 3000 participants at the event, developers acknowledged that the post-scalability version of the platform might not be available before late 2021, two years from now.

Funding for development still comes mostly from the Ethereum Foundation, domiciliated in Zug.

One of the most debated topics at DevCon was how to migrate tokens from Eth.1 to Eth.2. Many ways exist, but one has to be chosen, with no definitive answer provided thus far by Vitalik Buterin, who stated that it would favor "close to no disruption at all" – so, everyone can feel reassured.

The figure of Buterin is still as central to Ethereum as it ever was. As the Grand Priest of DevCon, his speech is listened to carefully by believers. His view is that the current version of Ethereum has been an interesting experiment, mostly paving the way for Ethereum 2.0 and that more iterations are necessary, especially with projects like Raiden, Plasma and others, which leaves an impression on the community.

IOTA

IOTA has announced a bridge connector to communicate between IOTA and Hyperledger Fabric

Cardano

Cardano has the specificity to be a project aimed primarily at sound academic research. In this sense, monitoring its progress indicates confidence in obtaining functioning PoS, sharded mainstream solutions.

The indication is that research is ongoing; the contracted team under Hoskinson's IOHK (Input

Output Hong Kong) has grown to 200 people worldwide, with a very detailed roadmap that will still take years before it bears actual fruit.

Tezos
Kathleen Breitman, co-creator of public PoS blockchain, Tezos, recently stated: "I can tell you for a fact, it's extremely unromantic and extremely unpleasant to watch a proof-of-stake network evolve. ... It's an extraordinarily hard task to switch to a PoS network or to launch a PoS network. The reason why is because there's so much more coordination cost, more than anything else. It's not a trivial task."

EOS
An airdrop of the EIDOS token has clogged the whole EOS platform. The token itself looks pretty useless, but those behind it appear to have triggered its distribution to make a point: by design, they encourage a maximum number of transactions. Users are invited to mine for new EIDOS tokens by moving EOS back and forth on the network.

THERE IS STILL NOT MUCH RESEARCH ON HANDLING LARGE AMOUNTS OF DECENTRALIZED DATA SECURELY, AND THE SIZE OF THE LEDGER WILL BECOME AN ISSUE ONLY WHEN SCALABILITY ALLOWS HIGH VOLUMES TO BE PROCESSED

To get EIDOS, users send tiny amounts of EOS to the smart contract. The contract then sends back the same amount plus a small portion of the daily release of EIDOS. Importantly, it doesn't appear to matter how much EOS is sent. What matters is how many transactions a person can submit. EIDOS is designed to generate maximum transactions. By providing a profit motive to encourage people to take action, rather than spend more money, EIDOS seems to have been designed to test the capacity of EOS itself.

Others
A number of more or less credible projects are developing their approach to solving scalability, while also developing specific consensus algorithms.

Solana is proposing a mechanism that can run independently on each participant's computer in order for them to agree on the time, and include this "proof of history" in the validated blocks agreed upon by PBFT. Claimed scalability is in the range of 50000 TPS.

A Korean platform, Fleta, also claims to have achieved 14000 TPS after the launch of its main net.

Metahash uses a Multiple Proof of Stake (MultiPoS) consensus mechanism. This involves ranking nodes in the network in a hierarchy: above light clients for users are peer nodes that decide to participate in the consensus. Among them are selected verification nodes, based on a range of criteria, including performance, but also geography and randomness. The role is to provide a college that is adapted to the network configuration and representative.

Verification nodes have a more significant capacity requirement, in terms of processing than peer nodes, but less than core nodes, which are the top category. With this configuration, MultiPoS relies on multi-layered validation to protect against the corruption of some nodes in the network. This model allows validation and block distribution processes to run in a parallel, thus decreasing consensus time. Core nodes generate blocks, but a voting mechanism exists for lower-level nodes to ask for a re-build of the network whenever they observe corruption. Over 50,000 TPS is claimed by Metahash, with nodes on five continents.

Relictum, which will have a reduced block size, and a throughput rate of one million TPS.

Algorand, created by a proven and famous cryptographer, Silvio Micali, was designed to solve the trilemma of decentralization/security/scalability. Blocks are produced in two phases: first, a block proposal phase, with one proposer being chosen randomly, then a voting phase by a randomly chosen college among the willing participants that are staking at least 1000 tokens. The advantage of the resulting blockchain is that it confirms immediately, does not burn energy to do so, is effectively decentralized and highly resistant to attack, as a hacker would not know whom to target.

CONFIRMATION TIME: FINALIZATION MECHANISMS

Let us highlight here the fundamental difference, in terms of finalization, between what is commonly called the "Nakamoto consensus mechanism" (either PoW or PoS), and the Byzantine Fault Tolerant voting mechanisms. When the chain is agreed upon after the proposal of a block by one or more participants, chosen according to a specific principle, the possible existence of competing chains can cause a given user to rollback a transaction that appeared to have been validated, with the probability of such an event decreasing rapidly, along with the number of blocks waiting. On the contrary, when every next block is the object of a vote among a pool of chosen voters, identified upstream, the block, once accepted in BFT voting mode, is, by definition, finalized.

LEDGER DATA STORAGE SOLUTIONS

There is still not much discussion or research on the question of handling potentially large amounts of decentralized data securely, and, as problems begin to arise, the size of the ledger will become an issue only when scalability allows high volumes to be processed.

Solana proposes to incentivize "Archivers" to store the ledger history. This incentivization is probably an interesting option to explore.

INTEROPERABILITY

This quarter, there is nothing fundamentally new to report in the field of interoperability, but we can still take the opportunity, in this calm period, to mention the main initiatives and approaches, thanks to a summary by Stephen O'Neal. Indeed, different methods are being researched, including cross-chains, sidechains, proxy tokens, swaps, etc.

- Polkadot is a multichain, or cross-chain, technology. It allows different blockchains to plug into a broader, standardized ecosystem. It was founded by Gavin Wood, a co-founder of Ethereum. Technically, Polkadot is comprised of parachains (i.e., parallel blockchains that process transactions and transfer them to the original blockchain), a relay chain (i.e., a central component that connects parachains and ensures their security), and bridges that connect Polkadot to external blockchains.

BY PROVIDING AN INCENTIVE TO ENCOURAGE PEOPLE TO MAXIMIZE TRANSACTIONS, RATHER THAN SPEND MORE MONEY, EIDOS SEEMS TO HAVE BEEN DESIGNED TO TEST THE CAPACITY OF EOS

- Cosmos also follows the cross-chain principle. Specifically, it employs an inter-blockchain communication (IBC) protocol to establish blockchain interoperability. It serves as a TCP/IP-like messaging protocol for blockchains. Since various established blockchains (like Bitcoin) do not support IBC by design, Cosmos uses the so-called "peg zones" to connect them to the "Cosmos Hub" – as the project is called – a "flagship" blockchain that binds all the zones together and coordinates communications between them via standardized languages. However, the Cosmos Hub is a part of the broader interchain ecosystem developed by Cosmos that can contain other entities. For instance, there is also Iris Hub, which focuses on enterprise customers and Chinese clients.

- Chainlink is a decentralized Oracle service. It allows for data to be retrieved from off-chain APIs and be put on a blockchain. In other words, Chainlink serves as a bridge between blockchains and all the infrastructure that exists off-chain: Oracle nodes receive real-world data, process it through the network and take it to the blockchain. Notably, the company cooperates with SWIFT, the global interbank data transfer and payment system used by most banks across the world.

• Wanchain uses a different protocol to facilitate data transfers between otherwise unconnected blockchains. Thus, instead of deploying peg zones or its multichain analogs, Wanchain creates so-called "wrapped" tokens that can be traded on other blockchains. For instance, to move 10 ETH to the BTC chain, the platform would first lock that amount of ETH on the Ethereum blockchain using smart contracts, which would then mint 10 Wanchain-wrapped ETH (WETH) on Wanchain. These WETH could then be traded for Wanchain-wrapped BTC (WBTC) on a trading platform. Those wrapped BTC tokens can then be turned into the original tokens located on the Bitcoin blockchain.

• Quant: unlike the examples mentioned above, Quant is not a blockchain. It uses the Overledger protocol, a layer that runs over existing blockchains. Overledger ostensibly allows developers to create "MApps" (decentralized applications that utilize multiple blockchains at the same time) in "three lines of code" and without any additional infrastructure. This allows for more options in blockchain engineering. For instance, a MApp could rely on the Ethereum blockchain for data storage while using Bitcoin Cash (BCH) for value transfer.

• Other projects researching interoperability include Cardano, Aion, Icon, Ark, Bytum, Dragonchain, and Ferrum network, among others.

PRIVACY – CONFIDENTIALITY

Mixing

From the possibility to group transactions with multiple inputs and multiple outputs like typically on bitcoin, to obfuscate where is going which money, have appeared some "mixing" services.

The "fun" part is that regulators have immediately started to clamp down on such services! For instance, Bestmixer.io has been shut down by the Dutch regulator. This all too much illustrates where the next crypto battle is being waged, as expected! States are not going at all to let go the control over financial flows.

These moves from official bodies are considered very seriously by crypto communities. The controversial McAfee has stated: "Bitcoin mixers are now being targeted. Anonymity itself is slowly being considered a crime. The word 'Privacy' will soon mean 'Criminal Intent'." Vitalik even pressed for the creation of on-chain mixers in response to off-chain actions by regulators.

MimbleWimble

The MimbleWimble technique came under threat in November, as Ivan Bogatyy reportedly de-anonymized 96% of Grin's transactions in real-time. The researcher claims that the method can no longer be considered a viable, secure alternative for private transactions, saying that MimbleWimble is "fundamentally flawed."

In practice, MW relies on merging transactions to obfuscate them. But because transactions are continually being created and originating from separate locations, if a node picks up all transactions before the cut-through aggregation is finished, it is able to unwind the CoinJoin. Any sniffer node can observe the network and take note of the original transactions before they are aggregated. While this does not show the number of transactions, it exposes the addresses. The better connected the attacker is, the more effectively it can uncover transactions. This will become more difficult as the network grows in size but remains a potential breach of security.

Grin developer, Daniel Lehnberg, said that Bogatyy's assertion is unfair and attention-grabbing – a story to be followed-up.

Zero-Knowledge Proof

Research continues on the magical technique that is ZKP. Findora recently revealed a breakthrough - 'supersonic' proof that is practical, trustless, succinct and verifiable as zero-knowledge. These are smaller than 10Kb and take only milliseconds to verify, even for the most complex statements. Fedora claims these are at least 25 times smaller than any other trustless zero-knowledge proof system with comparable verification times.

Ben Fisch, CTO at Findora, stated that until now, sk-SNARKs have not been practical as a trusted set-up. "Supersonic's combined proof size and verification time improve on the state-of-the-art by more than an order of magnitude for complex statements. They are at least 50 times smaller than STARKs and 1000 times faster to verify than Bulletproofs for these kinds of applications."

IDENTITY AND PERSONAL DATA MANAGEMENT

Please refer to the GDPR paragraph in the Legal Section of this report.

CRYPTOGRAPHIC ROBUSTNESS – QUANTUM COMPUTING EVOLUTIONS

Not coming back on the functioning and potential impact of quantum computing, let us simply inform here that there is no shortage of a frenzy of press releases and technical development claims from firms involved in making this a reality. So, the inception of quantum computing is a matter of time, that may be shorter than expected.

STANDARDIZATION

Using distributed ledgers to propose an infrastructure for information management and automation of business processes (including settlement), requires at its core, the need to formulate a protocol and the platform requirements. Some argue it might be too early to work on standardizing blockchain. However, DLT-based systems are fundamental, a method of handling business processes and communicating between independent actors. To successfully achieve this, the business processes and technical requirements have to be stated in detail and agreed upon beforehand.

This may occur informally between large actors, or officially by standardization bodies, however, if any of the promised benefits of using blockchain are to be achieved, an exhaustive collaboration of stakeholders must be coordinated to formulate the information management processes and protocols, and the infrastructure requirements to deploy it.

Several initiatives are being developed in diverse industries such as power generation and insurance, and lately, the film industry, under the patronage of the American Film Market. The case of logistics/supply chain looks emblematic to us; after a considerable number of pilot projects by Walmart, Carrefour, Maersk, IBM, SAP and Nestlé, with each focusing on their supplier ecosystem, the lack of generally admitted principles to build the traceability mechanism has become evident.

At the most official level, ISO standards, ten papers have been initiated, starting with identification of use cases and standard terminology. Most of the work is being done by AFNOR, the French standards, and certification body, with oversight by Julien Bringer, focusing on issues such as digital assets management on DLTs, privacy issues, security, etc. The work is ongoing but illustrates how serious some stakeholders are in defining universal principles to assist the whole blockchain sector is progressing in an orderly manner.

MALICIOUS ACTIVITIES

Double spending – 51% attack

It has been observed that an unidentified miner managed to control 50%+ of the hash rate on BitcoinCash during 24 hours, mining 73 blocks, or roughly half of the blocks mined during that period. Interestingly, the miner chose not to write the whole chain, even though this was theoretically feasible. No double spending was reported, so no fraud was reported.

We are referring to the fourth most prominent cryptocurrency, so the 51% attack is more than ever an ongoing concern, even for the strongest, Bitcoin. It is something that no one can rule out. Further, the halving of the Bitcoin reward in the coming months is likely to reduce the safety of the network, making this attack all the more concerning, even though possible.

Market manipulations

We continue to observe indications of questionable market behavior, but with little hard evidence.

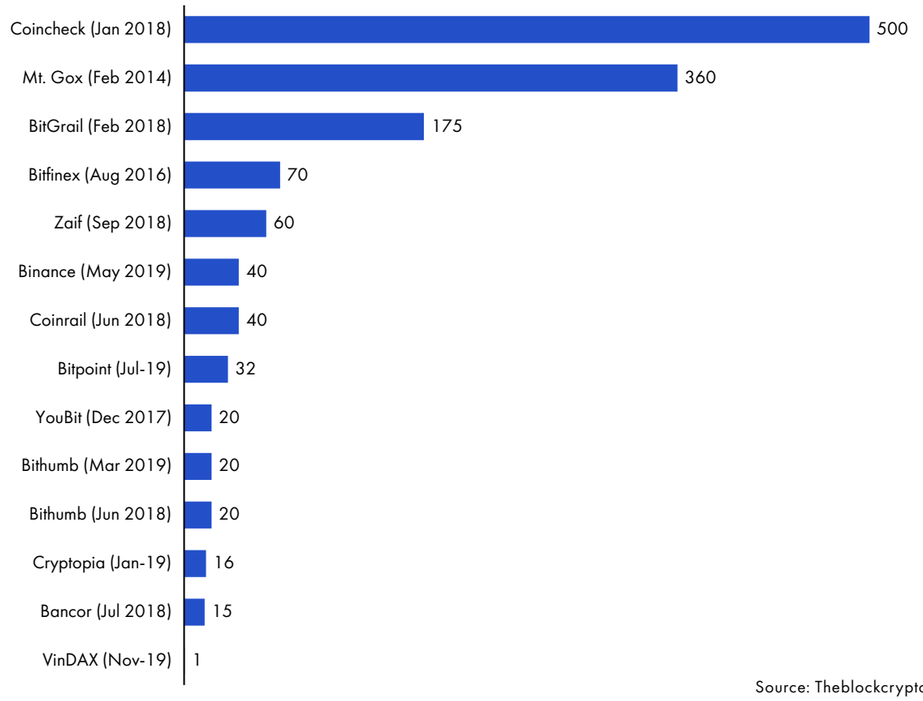
A case was filed to prosecute Alameda Research LLC, with accusations of attempts to manipulate Bitcoin's price on Binance (even though unsuccessful).

Some research on the trading of Bitcoin and Tether between March 2017 and March 2018 has been conducted by US academics. Patterns have been identified that led the researchers to claim that most of the impact on the Bitcoin price during that period (i.e., the exceptional run to $20k) was caused by the actions of a single large trader that they code-named 1LSg. This casts further doubt on the already shady Tether and Bitfinex connection. If this is true, then it shows that dramatic fluctuations in the price of Bitcoin was, and continues to be, caused by only a limited volume of transactions, and puts in question the fundamental analysis we have recently put forward...

Other researchers, however, point out that the purchasing power of Tether (Tether's market cap per BTC market cap) increased throughout 2017, and decreased afterward, highlighting that whenever BTC falls, this metric increases. To us, this reasoning does not seem very convincing. The only sure thing is that the crypto market is still the Wild West, and nobody can effectively control the actions of large or small players that attempt to influence the market!

FIGURE 22:

LARGEST CRYPTO EXCHANGES HACKS



Source: Theblockcrypto

Thefts, hacks, frauds, and scams

The latest victims of exchange hacks were Vietnam-based VinDAX, which lost half a million USD on November 5th, spread across 23 different cryptocurrencies, and UpBit, a Korean platform, which lost $49 million worth of crypto, which evaporated on 26th November 2019.

The attacks are not stopping!

Mining malware

Always more sophisticated mining software continues to spread on the internet.

On its side, Firefox now provides an add-on option to block crypto-mining scripts automatically.

SYNERGIES WITH OTHER TECHNOLOGIES

IoT synergy

Blockchain is regarded as a technology of interest within the robotics sector for managing information transfer between machines in a secure manner, and immune from attack. In particular, swarm robotics poses a challenge in terms of robots working together to perform tasks and operations. The collective behavior of the swarm is what is of interest. By using cryptographic digital signatures and secure public-key cryptography, blockchain promises to provide optimum security for data across shared channels between swarm robots. So, while AI-powered robotics is emerging as a forefront technology, blockchain empowers robotics with an optimum security solution.

Artificial intelligence

Beyond implementing advanced algorithms as distributed applications, artificial intelligence can enhance blockchain in a variety of ways:

- Saving energy: AI can be highly effective in keeping a check on energy consumption, thanks to optimization.

- Data screening: the significant amount of on-chain data, not necessarily organized, calls for new approaches to exploit (mine) it, which are compatible with machine learning.

Conversely, blockchain can help AI development, especially in providing a data repository to train algorithms, with or without homomorphic encryption to hide the data itself. This is a typical blockchain use-case, including a fee to the data owner.

MOMENTUM GAINED BY DLT ALTERNATIVES TO BLOCKCHAIN

Direct Acyclic Graph (=Tangle)

The progress published by IOTA is earning the project some momentum in the fight towards reaching mainstream adoption.

Corda, Hyperledger & other permissioned non-blockchain DLTs

The CordaCon conference was held in November, and was attended by 2000 delegates, twice as many as the previous conference. The organizers congratulated themselves on the number of significant enterprise blockchain consortia preparing to go live. R3's Chairman, Frédéric Dalibard, noted that the conversation has changed from experimentation to "how do I put my CorDapp into production, and how to iron out the legal details, which means this is real."

Importantly, Corda is being adopted beyond finance, with big consortia currently readying to launch in sectors such as insurance, trade finance, and capital markets. Objectively, the scale and outreach of projects deployed on Corda are impressive: insurance consortium B3i, the Swiss Exchange SIX platform, the Marco Polo trade finance solution. These are all significant, top-tier systems that are going to have a considerable impact when, or if, they are put into full production.

Other permissioned non-blockchain DLTs

Hyperledger is committed to organizing a significant event in Phoenix in March 2020, capitalizing on the continuous inflow of new members, and use cases that are being developed on the platform.

CONCLUSION OF THE TECHNICAL DEVELOPMENTS

There is no denying that the slow and challenging progress in the technological development of DLT infrastructures is disappointing. There are very few new concrete technological solutions to report. Ethereum's DevCon, in particular, embodies the difficulty of coordinating a community, and how far we still are from the satisfactory scaling of blockchains. Even Bitcoin's Lightning Network is plateauing.

So, there is not much positive development to report, either incrementally or disruptively, which is quite worrisome. This gloominess, however, explains, at least partly, the current depression of crypto asset prices.

7 OVERVIEW BY COUNTRY

ASIA

JAPAN

The Japanese banking giant, Softbank, has released a new payment card that has a built-in WiFi that can be used for both fiat and digital currency transactions. The original product, named SBC Wallet Card, features a prepaid debit card, a blockchain-based wallet that can be used either "hot" or "cold" for blockchain-based transactions, and a small on-card display. The underlying technology for the card was developed by the US firm, Dynamics Inc., which raised $110 million from investors, which included MasterCard.

Nomura Securities and SBI Securities have helped to found the Japan Security Token Offering Association, along with Daiwa Securities, Rakuten Securities, and others. It aims to develop self-regulation around security token offerings.

The Japan-based Muroran Institute of Technology is piloting a program to verify its students' academic records using blockchain technology. It will also be used to fight resume fraud.

Also related to this topic, Japan's recent move to raise the sales tax from 8% to 10% was accompanied by the decision to allow merchants to reward cashless payments by providing consumers with a 5% rebate on purchases. This is similar to Sweden, where the government is preparing citizens for the disappearance of cash.

Japan's Tech Bureau is set to launch a blockchain-powered medical records platform and has teamed up with Yokohama-based HealthCareGate for the project.

SOUTH KOREA

South Korea's national policy committee has passed an amendment establishing a legal framework for cryptocurrencies. It requires crypto exchanges and service providers to register with the country's financial regulator, and comply with the recommendations set by the Financial Action Task Force.

The CEO of crypto exchange, CoinUp, was sentenced to 16 years in prison for having duped thousands of investors, promising them a return of up to 200% within weeks. The scheme lured people into investing in an unlisted cryptocurrency and convinced them that the price would skyrocket after listing. However, the coins were never listed and investors lost money.

South Korea's Ministry of Science and Technology plans to invest 450 billion won (~ $382 million) in blockchain research and development over a period of six years, from 2021 to 2026.

NORTH KOREA

An American cryptocurrency researcher and member of the Ethereum Foundation has been arrested after traveling to North Korea for a secret conference on blockchain technology. He was charged by US authorities under the International Emergency Powers Act for allegedly providing technical advice on how to evade international sanctions using cryptocurrency and blockchain technology.

It appears that North Korea has been using a Hong Kong-based blockchain company to launder money, according to the quarterly report of the UN Security Council's Sanctions Committee on North Korea. The report claims a man named Julian Kim, using an alias of Tony Walker, was the sole owner and investor in the firm and had attempted to withdraw money from banks in Singapore on several occasions. The laundering scheme circulated the stolen crypto using 5,000 transactions in multiple countries to obfuscate its source. So, everything is, in effect, public and analyzed on the BTC ledger!

CHINA (MAINLAND)

Binance announced that it was now accepting fiat payment from WeChat and AliPay. This will, once again, provide Chinese citizens with access to cryptocurrencies.

The most senior official of the People's Republic, Secretary Xi Jinping, has publicly declared support for blockchain, saying the country needs to take advantage of the opportunities the technology offers, qualifying it as "a key breakthrough that can facilitate China's progress in core technologies." Bitcoin soared from $7,500 to $10,500 in just a few hours following the statement. This impact is quite surprising because this statement does not indicate a significant change in the Communist Party's position on Bitcoin, or it is banning the exchange of crypto for yuan (even though China has moved ahead of other nations in other vital technological fields, such as 5G and AI). Nevertheless, the market considers that any official statement that embraces a state-issued cryptocurrency is highly beneficial to BTC.

Later, when the Chinese central bank warned businesses involved in cryptocurrencies against improper actions and cautioned investors to be wary of virtual currencies, this was seen as justifying a price correction. And indeed, valuing the technology has nothing to do with endorsing new decentralized currencies.

At the end of November, central authorities cracked down on exchanges that were re-emerging to serve Chinese clients, leading five exchanges to either halt operations or announce that they would no longer serve domestic clients.

The Chinese State Administration of Foreign Exchange (SAFE) has expanded its pilot program for a cross-border blockchain financing platform from 9 to 19 provinces (out of 23 in total). Results so far appear to be very positive: by the end of October, the platform had processed 6,370 transactions and issued $6.8 billion in loans to a clientele of over 1,262 companies, most of which are small and medium-sized. Officials report that the pilot has reduced processing times from as much as two days to just 15 minutes. It also saves a mountain of paperwork and cuts out fraud.

CHINA (HONG KONG)

Since the Arab Spring, civil protests have changed, enabled by the internet and social networks. Usage of blockchain-based messaging systems is likely to push this to the next level (not to mention the use of cryptocurrencies by seceding territories).

Hong Kong's unrest seems to be the perfect test case for an open-access financial system resistant to government interference. However, governmental forces have levers; for example, the internet is systematically shut down in HK protest areas, irrespective of the operator, reminding us that peer-to-peer networks are built on existing connectivity.

SINGAPORE

The Monetary Authority of Singapore (MAS), the city-state's central bank, has completed development (in partnership with J.P. Morgan and Temasek) of a blockchain-based cross-border payment system, named Ubin, aimed at supporting a variety of currencies. It has been successfully tested with counterparts in the Philippines.

The MAS has also published a consultation paper, seeking to green-light what it calls "payment token derivatives" for listing and trading on "approved exchanges" in the country under its Securities and Futures Act (SFA).

The country is providing grants worth millions of SGD to sustain the local blockchain start-up scene.

VIETNAM

Ho Chi Minh City aims to establish a regulatory framework and policies to tackle blockchain, to develop smart cities. People's Committee Vice Chairman, Tran Vinh Tuyen, declared that science and technology projects that can help solve difficulties in the town and develop smart urban areas would receive priority, particularly projects using artificial intelligence. The city is increasingly becoming a regional high-tech hub.

INDONESIA

Indonesia recently changed its tune regarding cryptos. Amid concerns of rampant fraud and suspicions, the Jokowi-led government initially turned its back on the blockchain when it issued an outright ban on cryptocurrencies, which took effect on January 1, 2018, in the wake of the crypto mania of 2017.

While the use of Bitcoin in transactions for goods and services is still prohibited, the country has signaled that it will encourage blockchain innovation. Back in February, the Indonesian government announced that it would create a legal framework to regulate cryptos and digital asset futures. This came just a few days after the Commodity Futures Trading Regulatory Agency announced that Bitcoin and other cryptocurrencies would be classified as tradable commodities.

The formal tone is resolute in trying to create a blockchain start-up landscape in Indonesia.

THAILAND

Thailand is conducting three pilot projects, one of which is a blockchain-based system that processes tax refunds for oil exporters. Another is a platform for trading "renewable" energy certificates, in association with the Energy Web Foundation.

The regulator is considering proactively reviewing the existing Thai crypto regulations that went into effect in May 2018. The Securities and Exchange Commission (SEC) Secretary-General is currently studying whether the current rules have any areas impeding the growth of the digital asset industry, and stated that the regulator would adopt a flexible attitude in applying the regulations, in line with the market environment.

INDIA

India's Ministry of Electronics and Information Technology is preparing a national blockchain strategy, or "framework". Indeed, considering the potential of blockchain and different uses cases in banking, finance, and cybersecurity, the Government has decided to incentivize research and development of blockchain applications.

Indian investors continue to devise ways to bypass the ban on cryptos, including supplying fake KYC information when registering on foreign exchange platforms.

Crypto exchanges, Megatron and Binance, have added support for the Indian rupee. Traders can now buy and sell crypto with Indian rupees.

AUSTRALIA

A project is underway to use blockchain to manage Australian digital health records. This follows many reported security breaches related to the current data repository.

SOUTH AMERICA

VENEZUELA

The Central University of Venezuela in Caracas will offer crypto and blockchain 101 workshop-type courses to entrepreneurs from a range of business backgrounds.

Paxful says it plans to install 100 cryptocurrency ATMs in Columbia, Venezuela and elsewhere in Latin America, in conjunction with its partner, CoinLogiq.

ARGENTINA

News from Argentina revolves around the local super-inflation situation. As a result, citizens are attracted to alternative means to store value, and methods of currency exchange; USD is one, but BTC is another.

On September 1st, the Central Bank of Argentina imposed restrictions on U.S. dollar purchases to revive the plunging peso. Consumer purchases made in dollars will be limited to $10,000 a month, with special permission required beyond that limit. The bank also said that, until December, it would restrict dollar purchases to $200 per month via bank accounts and just $100 per month in cash.

On November 1st, Argentina's central bank formally banned consumers from purchasing Bitcoin (BTC) and other cryptocurrencies using credit cards. What followed was the very opposite of what the Argentinean government had anticipated: trading by Argentinians on the peer-to-peer platform, LocalBitcoins, subsequently increased.

EUROPE

RUSSIA

The Russian parliamentarian in charge of drafting the country's crypto laws has stated that a method should be devised to prevent criminals from using cryptocurrencies. The stance taken is that legislation should allow blockchain and crypto businesses to develop, but at the same time block channels that exploit the illegal usage of these tools.

Ministry of Internal Affairs intends to develop legislation to seize cryptocurrencies involved in criminal activity. In this regard, tokens that have no legal status is proving to be an obstacle for police when fighting crime funded by cryptocurrencies. But the ministry is said to be teaming up with law enforcement agencies in a bid to have an appropriate legal framework in place by 2021.

On November 29th, the Central Bank of Russia came out against Bitcoin, claiming that the local ruble should be the nation's only legal tender. Lately, the support of a complete ban is a trendy position for officials to take – obviously worrisome for pure cryptocurrencies.

Sberbank is the first Russian bank to obtain patents for a repo deals solution and an execution system that utilize distributed ledger technology. The answer was developed in-house and enabled the parties (to a deal) to register the terms of a repurchase agreement inside a self-executable decentralized environment, i.e., sign a smart contract. The parties then sign the smart contract with e-signatures via a distributed ledger. The contract will then meet the terms of the first part of the repo deal by transferring funds and securities to the respective parties.

UKRAINE

Ukraine recently appointed a new pro-crypto minister and wants Binance to help it work out how best to serve its citizens. According to Binance's press release, the exchange will help the Ukrainian government develop "transparent and effective mechanisms" for crypto sales, and "beneficial conditions for investments and business in Ukraine." The working group hopes to present something to the Ukrainian Parliament before the year is out.

SWITZERLAND

The Swiss Federal Council has submitted the finalized draft law on distributed ledger technology to the Swiss Parliament. A cornerstone of the bill is improved legal certainty in connection with the issuance and transfer of tokenized rights and financial instruments, such as bonds and shares.

To that effect, it introduces "Uncertificated Register Securities", a new concept with specific rules in the Swiss Code of Obligations for corporations looking to issue shares in tokenized form. The tokenization of rights will, in effect, enable the electronic registration of reasons that have the same functionality and equal protection as traditional negotiable security. Consistent with existing regulations, the Swiss regulator has excluded payment tokens (i.e., "pure" cryptocurrencies, for example, Bitcoin), from this new concept, since these do not give rise to claims against an issuer or a third party.

Bitcoin Suisse continued to consolidate as an important actor in the country, highlighted by renewed advertising campaigns on the streets of Zürich. As a custodian, it intends to offer its clients a staking service in the future Ethereum 2.0 (and taking a 15% cut).

UNITED KINGDOM

The United Kingdom Jurisdiction Taskforce, one of the Lawtech Delivery Panel's taskforces, has published a statement concerning the status of cryptocurrencies, distributed ledger technology, and smart contracts under English and Welsh law. The document attempts to address the legal uncertainties of cryptocurrency and recognizes crypto assets as tradeable property, and smart contracts as enforceable agreements under the local law.

SWEDEN

Sweden's Central Bank governor has outlined a six-step plan on how the state bank can implement its digital currency. A checklist of required steps was outlined that must be completed before the idea is fully implemented. Sweden's digital currency will have to meet the following criteria. (1) It must be available 24/7 and allow for payments anywhere, no matter how big or small. (2) Cross-border transactions are a must. The Swedish digital currency must also be easily convertible to other acceptable currencies. (3) Legal tender laws must be updated to include digital currencies. (4) The digital currency will be issued directly by banks, with Swedish Central Bank oversight. (5) Digital IDs will accompany digital currency to prevent money laundering and improper use. (6) Physical cash must still be kept as a safeguard in case the digital currency systems fail.

GERMANY

The German Federal Financial Supervisory Authority issued a warning against 5 Capital, a Bulgarian cryptocurrency broker after the firm illegally offered CFDs (contracts for difference) designed to expose clients to the price movements of cryptocurrencies.

The Parliament passed a bill allowing banks to sell and store cryptocurrencies. From January 2020, German custody providers and crypto exchanges will be required to apply for a license before the end of 2020. The expressed intent is to attract foreign capital that seeks security and regulatory certainty. As one observer put it, "Germany is well on its way to becoming crypto heaven." German crypto companies have three specific options: apply for a license, work with a licensed cryptocurrency custodian, or work with a licensed provider.

FRANCE

The central bank of France, Banque de France, is seeking a blockchain analyst to help the bank define a program for implementing a digital currency. The bank is also hiring a development engineer to study the application of blockchain for crucial banking functions.

EUROPEAN UNION

The European Investment Fund (EIF) and the European Commission have together put 110M euros on the table, and hopes to raise other 300M euros from private investors to fund blockchain projects through VCs. The stated goal is to take action to ensure that it does not lag behind the US and China in the development of distributed ledger technologies and related applications.

SPAIN

The Comisión Nacional del Mercado de Valores has warned the public against an ICO, AlyCoin, which purports to provide its customers with financial services that Spain considers to violate the second paragraph of the securities markets law.

ITALY

Italy is following the crowd by working on a legal framework to regulate cryptos and blockchain. The government is favoring distributed ledger technology innovations, especially in fintech (which is nothing extraordinary, of course).

MALTA

The Malta Financial Services Authority has issued a warning related to a Bitcoin scam. The agency cautioned the public that an entity, dubbed "Bitcoin Future", appeared to display "the same deceitful characteristics" as a separate scam, dubbed

"Bitcoin Revolution," against which it had already issued two public warnings.

The Maltese Prime Minister, Joseph Muscat, said that he would resign in January after it was revealed that his former chief of staff, Keith Schembri, was linked to the killing of a journalist in 2017. As Muscat was highly involved in making Malta a crypto island, this may have an impact on the country's policy regarding the big players that he was keen to support, with Binance at the top of the list.

NORTH AMERICA

CANADA

The Royal Bank of Canada has shown interest in blockchain patents, which indicates at least curiosity towards the technology.

Canada's blockchain ecosystem has delivered a petition to the Canadian administration advocating more legal clarity.

A survey published by the Bank of Canada indicates that between 2016 and 2018, the percentage of Canadians who were aware of Bitcoin increased from 62% to 89%, and those who owned Bitcoin increased from 3% to 5%. However, the number of past owners also increased, suggesting an influx of Bitcoin owners, many of whom subsequently divested after the steep price rises in 2017. The main reason for owning Bitcoin remains speculation, although this share is decreasing steadily. On the other hand, the percentage of Canadians who reported using Bitcoin for transactions a few times a month or more increased. These are interesting statistics to bear in mind as far as adoption is concerned.

UNITED STATES OF AMERICA

In recent years, centralized cryptocurrency exchanges have consistently exited the US market. The most significant was the exodus of Poloniex, obviously the result of stringent local regulation, basically rendering the service of US passport-holders too risky, and a business that no one wants to support. This shows that the exchange platforms are the weak point of the crypto environment. US citizens are mostly reduced to using VPNs or decentralized exchanges to participate in the game, while Coinbase is, in effect, merely a brokerage platform. So clearly, there is a space available for competitors, for example, Abra which is currently expanding.

AFRICA AND MIDDLE EAST

In this edition, we will look at Africa in more detail than usual. The "leapfrogging" concept, as seen in the example of mobile phones that reached the African continent before landlines, is often seen as applicable to banking/finance thanks to the promise of cryptocurrencies. In that sense, Africa is regarded by many as the place that is likely to play a central role in cryptos. Analysis of Google searches related to blockchain and Bitcoin shows that countries like Nigeria, Ghana and South Africa lead the global ranking in terms of the sheer number of searches. In these countries, the proportion of internet users who own crypto is exceptionally high, reaching as high as 10% (compared to the worldwide average of 5%).

One of the reasons is that poor African families, who depend on money transfers from abroad to make ends meet, regard the high cost of using PayPal or Western Union as unacceptable. These populations cannot afford to lose 10%+ of their financial resources, which is sure to push people towards crypto alternatives.

Also, for those living in Zimbabwe, for example, with no bank account, a crypto wallet, and say, XRP or Monero makes much sense, provided the cryptocurrency is not more prone to devaluation than the official fiat. Regardless of the underlying technology, if that provides an effective alternative to storage and transfer value, then why not?

SENEGAL

The artist, Akon, is using his regional popularity to promote his philanthropic visions, which include the electrification of the continent, and enhancing African unity utilizing cryptocurrencies. He is building a city in Senegal that will be 100% crypto compatible.

GHANA

The governor of the West African nation's central bank, Ernest Addison, stated that Ghana might issue a digital form of the nation's currency, the cedi, shortly, and is in talks to develop a pilot project in a sandbox environment.

KENYA

Kenya, the financial hub of Africa, has been testing the first blockchain application to provide banking services to its otherwise unbanked population. Notably, Kenyan banks aren't pleased about this, as the new competition will undermine their business.

Apart from serving individuals, AZA, a company based in Kenya, is helping African companies to do business with foreign countries, especially China. For instance, a Nigerian customer can directly benefit from the naira/yuan pair, which all standard banks would route through USD (or sometimes EUR). Passing through cryptocurrencies is an option with a low barrier to entry, which AZA deploys, and which is now worth ~100M euros per month in transactions handled throughout Africa.

LESOTHO

The Apollo Foundation has announced a Memorandum of Understanding (MoU) with the nation of Lesotho to develop and implement blockchain technology in various government departments and initiatives.

SOUTH AFRICA

The central bank of South Africa is formulating new rules to govern the use of cryptocurrency and digital currency in the country and will deploy the new rules in early 2020. The main goal is to prevent cryptocurrency from being used to evade currency controls. The new regulations will limit the amount of local currency that can be transferred out of the country. This concern is a clear parallel with Chinese interests and was the stated reason for the regulation that forbids yuan/crypto exchanges.

The First National Bank (FNB), one of South Africa's biggest banks, has shut down the accounts of all companies dealing in cryptocurrencies. The banking sector in the country is increasingly concerned about the risk associated with serving crypto-related businesses.

The trial of a land registry on the blockchain is being conducted, involving about 1000 government-subsidized properties in Cape Town.

TUNISIA

The Central Bank of Tunisia issued a statement denying that it has issued an e-dinar, saying that an unrelated "proof of concept" project was taken "out of context". But it confirmed interest in exploring all existing opportunities.

ALGERIA

The Algerian Government appears to be moving towards a total ban of Bitcoin and other digital

currencies, including the prohibition of possession, not just banning it as a form of payment.

MOROCCO

Morocco intends to simplify access to various financial services by implementing blockchain technology. The country's central bank governor, Abdellatif Jouahri, while talking at the Africa Blockchain Summit in Rabat, stated that the country would employ financial technology to improve access to financial services.

Fintech applications, including the deployment of blockchain technology, are intended to assist Morocco to offer "all individuals and businesses fair access to formal financial products and services to promote economic and social inclusion."

TURKEY

Turkey is emerging as a country with a lot of activity and interest in cryptocurrencies. Binance has revealed that the country is increasingly important in terms of trading activity. The recent Turkish currency crisis may explain this trend, at least partly.

Turkey's 11th Development Plan covering 2019-2023 was recently released and includes a commitment to creating 'digital money' via blockchain technology. In other words, Turkey is joining the pool of countries whose central banks are working on putting their fiat on a blockchain.

ISRAEL

The launch of the Hogeg Institute for Blockchain Applications by Tel Aviv University in 2018 has strengthened the development of talent to drive innovation in blockchain technology.

The proactive participation of the government with developments such as the highly detailed "Interim Report on the Regulation of Decentralized Cryptocurrencies" released by the Israel Securities Authority is also providing regulatory clarity that gives startups the freedom to experiment.

SAUDI ARABIA

On the occasion of a visit by the Crown Prince Mohamed Ben Salmane to the Emir of Abu Dhabi, Mohamed bin Zayed al Nahyan, a surprising joint declaration was made: the Saudis and the UAE intend to launch a universal digital currency to facilitate exchanges between the two countries. However, the intention is to use it exclusively for interbank settlements.

CONCLUSION: MID-TERM CONSIDERATIONS

The general feeling obtained throughout this report is mixed, to say the least. Notably, there is not much positive news! The price of Bitcoin has clearly stalled; public adoption seems still far away; the laws passed are overall not so favorable to cryptocurrencies, beyond just the strict KYC excuse; industrial applications are still slow to move to commercial exploitation; and above that, there are still no major breakthroughs on the technical development front.

But despite this rather gloomy outlook, it is still possible to find a positive note. The question is, what would it take break this negative trend?

- On the regulatory side, the new financial paradigm will always be supported by at least a few jurisdictions. So, paradoxically, there is only limited concern in that regard, regardless of the short-term turmoil caused by current bans. And, with China, India, USA and Russia practically engaged in opposing cryptos, the situation is quite possibly at its worst, in which case it will only improve in the mid-term.

- On the adoption side, this too can only pick up, as we are still pretty much at zero. Thanks to the tokenization of Bitcoin on side chains or even off-chain, perhaps an enhanced user experience will make a difference. Also, if Libra aborts, there is little doubt that another will take its place. The timeframe is, of course, unknown.

- In reality, only the demonstration in production of the new infrastructure can conclusively establish the suitability of various blockchain applications to handle businesses requirements. Again, this is going to take a great deal of time, because, as by nature, this requires the coordination of many actors. And, there is no need to mention, it requires scalability...

- Research and development on the governance of decentralized platforms and their scalability is ongoing, as these are linked - they show some progress.

Long story short: it will still require time. Time for ecosystems to be built, time for regulators to calm down, and time for crypto enthusiasts to find their way. And, ultimately, time for adoption to gain momentum, once scalability and governance issues have had time to converge.

Clearly, cryptocurrency prices are unlikely to recover as fast as they did in spring 2019. The parallel price pattern that analysts were expecting, that is, the 2014-2017 period potentially repeating in 2018-2021, appeared to be have been invalidated in June, however, it is still plausible. The crypto winter may have ended in 2019, however, even in meteorology, late freezing can always happen – so we are far from being out of the woods yet!

CONTACTS & REFERENCES

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

Halim Nader | Head of Operations and Partner | halim.nader@bqintel.com

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

This publication has been prepared for general information purposes only and is not to be relied upon as accounting, business, financial, investment, legal, tax, or other professional advice. It should not be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

© 2020 bqintel. All rights reserved.