

BLOCKCHAIN QUARTERLY

3Q 2019 | AS OF SEPTEMBER 30TH, 2019



8th Edition • Published by bqintel.com

FOREWORD

This document is the September 2019 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.

In order 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 or lack of precision are found, please contact us on research@bqintel.com.

TABLE OF CONTENT

1. GLOBAL MARKET UPDATE

01

2. UPDATE ON THE REGULATORY POLICIES

07

3. REVIEW OF BLOCKCHAIN INDUSTRY PLAYERS

15

4. INVESTMENTS & USE CASES BY INDUSTRY

25

5. TRENDS BY CRYPTO-ASSET CLASS

31

6. LATEST ADVANCEMENTS IN DLT TECHNOLOGIES

49

7. OVERVIEW BY COUNTRY

61

EXECUTIVE SUMMARY

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

- The crypto markets have benefited from the massive increase in prices seen in the first half of 2019, with a price spike at the end of June – large even by crypto standards. While the impressive evolution of the Bitcoin's price and volume invites consideration of whether the technical pattern is different from that seen in the previous cycle, not all crypto assets have behaved the same, as notably, the fundraising tokens of 2017 collapsed again after the spike, and many are now trading at their all-time lows.
- As a result, enthusiasm has returned to the communities. Some individuals are already back in the crazy zone, while others are still out of the market and cautious. The positive trend appears to be supported by several fundamental considerations, including accommodating central bank monetary policies, a growing appetite for alternatives to fiat in developing countries, and institutional money waiting to flow into the ecosystem. There is also no shortage of scams and frauds, which can be considered a clear indicator of a dynamic market...
- Regulators are maintaining pressure on controlling financial flows, thereby contributing to building an inevitable wall between the incumbent financial world (and its monetary system), and the new crypto world. Anonymous crypto-currencies are under significant threat and are going to be the next battle fought. Ultimately, the impossibility for governments to let go of the privilege of issuing money has been exemplified by the immediate official attacks on the Libra – which confirms that regulators see decentralized networks as being capable of providing a genuine alternative to the USD-dominated system.
- The development of distributed ledger platforms, and resolving related issues are progressing, but slowly. In practice, scalability is still not available, compromises between governance and decentralization have not appropriately been figured out, and it remains the Wild West in terms of the crypto-markets, as sound on-chain rules are not yet in place.
- On the applications and business side, the number of developments taking place is literally exploding. On the one hand, ICO platforms are struggling to deliver on their promises of products and services, let alone on their business models; they are facing extended development and financing problems, and at the moment, ICOs are struggling to raise money. Large companies and consortiums, on the other hand, are increasingly active; they were slow to get going, but are now organizing their sectors properly, in terms of standards.

1 GLOBAL MARKET UPDATE

EDITORIAL: GLOBAL STATE OF THE DLT ECOSYSTEM

In the cryptosphere, the atmosphere during recent months has been electric – even more so than usual. The renewed excitement around cryptocurrency prices has revived interest, waking up enthusiasts and opponents, not to mention those who continued to be involved after the 2018 downturn.

What is impressive with distributed ledger technologies is that it touches so many levels of the economic landscape, and to their essence. As such, it is challenging to guess how many of the current business models are going to be wiped out and how fast. Never before has a brand new (and readily available) macro-economic model been able to replace central banking principles, so it is clear it has almost no chance of overtaking the present system without significant opposition, in a situation whereas many will lose in the transformation, as those who will win.

So much uncertainty is both scary and exciting, and in principle, not much of it has been resolved over the past two years. We are all aware of what DLTs can do, but the social acceptance of it is not at all apparent. In this context, the inception of Libra, the all-out explosion in industrial projects that we are witnessing in 2019, the laborious effort to solve scalability issues, and the non-coordinated involvement of governments are all signs that much is going on in all directions. As such, it becomes impossible for a single individual to survey even the major current initiatives and use cases.

How some structure is going to emerge is unclear, but systems never diverge indefinitely without breaking apart. Some structure is needed, and with no surprise, we are starting to observe that standardization is a topic embraced by the actors in virtually all ecosystems. The least we can say is that there are still some exciting times ahead!

COMMENTS ON CRYPTO-ASSETS MARKETS

Prices

In early June, awakened by the price spikes, bears began to voice their doubts and concerns about Bitcoin, the likes of which we had not seen for a long time, since the beginning of 2018. This did not prevent cryptocurrencies from reaching surprisingly high levels during the same month.

In fact, with the price of Bitcoin, reaching almost US\$14,000, the technical price pattern was not the same as that seen in 2015-2017. Whatever reason you ascribe to it, the reversal of the trend towards a period of growth has been faster and more vigorous than most people would have expected. We are probably not taking any risk in saying that

it was the fundamental elements that investors/speculators believed in that caused the mid-year price increase – and they probably still have the same beliefs. Whatever it was, it prompted a new wave of entrants seeking to buy crypto assets and caused enthusiasts to be reluctant to sell, while opponents were simply out of the market (so, have no or little influence on it).

Since the observable events follow a different path, let's take a minute to reflect on what the differences are between 2019 and 2015?

- In 2015, there were no newspapers/websites/channels, or very few, that were talking about Bitcoin, let alone Ethereum or any altcoin. Today, the press knows that talking about crypto will sell papers, and the mainstream media often broadcast news of crypto price movements, probably creating a positive feedback loop that did not exist four years ago. In part, this may explain the surge in price volatility seen since the beginning of April.

- The viral effect of enthusiasts in their environments may not be in proportion to their number. Professionals, especially traders, have also entered the field in large numbers since then (and the possibility that some may attempt to manipulate the markets cannot be excluded). Actors have gained a better understanding of the technology and of the true nature of the crypto assets they are getting into, which may have had the effect of quenching some of the hype that was fueled by uncontrolled "fear of missing out", so perhaps making the whole environment a little less volatile.

- Due to the unprecedented exposure gained by Bitcoin, Ethereum, XRP, etc., the kind of people that are entering or considering entering the field is changing, and their modus operandi, as well as the depth of their pockets, cannot be the same, even if their psychology is similar – which it is not. We will touch on that later in the report, but that might be the most significant change, compared to four years ago.

- Today, access to cryptocurrency is democratized, let's even say more comfortable than it was in 2015. Exchange platforms have matured, and user interfaces and trading facilities on all of them have been improved. The inflow of money to the sector remains a crucial point, but it is a fact that more services are now available than ever to get in and out. Hacks continue to happen, but they represent a smaller portion of the capital handled. Also, platforms are more efficient at

WE ARE ALL AWARE OF WHAT DLTs CAN DO, BUT THE SOCIAL ACCEPTANCE OF IT IS NOT AT ALL APPARENT. IN THIS CONTEXT, THE INCEPTION OF LIBRA, THE ALL-OUT EXPLOSION IN INDUSTRIAL PROJECTS THAT WE ARE WITNESSING IN 2019

fixing weaknesses, and news of malicious activities are no longer regularly hitting the headlines.

- In terms of trading behavior, for similar price levels, we observe much higher traded volumes on the platforms, almost tenfold, according to CoinMarketCap. So, even if much of it is fake (probably at the time a good portion was fake already), we can safely say that there has been a significant increase in real activity. This is undoubtedly fueling today's volatility, and the dynamic is stronger than could be observed in the previous cycle.

- Use cases and concrete adoptions are still weak, but growing almost exponentially. The pace at which businesses and services are launching using the technology is mind-blowing compared to what it looked like a year ago. This is another feedback loop that was not as powerful in 2016.

- Governments and regulators have taken positions regarding cryptocurrencies, although not on everything. Nevertheless, and threatening declarations from officials are going to resume, and are likely to intensify as the price of cryptocurrencies goes up. However, the past two years have shown that Bitcoin ownership and its use for payment are not expected to be banned in democracies, so the legal environment is somewhat firmer than it was. At the same time, the threat that BTC & co poses to officials is going to grow with its adoption level, which is likely to impact its growth pattern, and has the potential to moderate the excessive behaviors we have been used to.

Correlations

For this time let's look at the correlations between crypto assets, rather than between the crypto classes. Interesting comments can be made, especially between Bitcoin and any other coin:

- We can observe an apparent general increase in the correlation figures in recent years. To us, this is very instructive because it is counterintuitive. One would have thought that the crypto assets

that are out there are very different objects based on their characteristics: infrastructure, ownership, anonymity, etc. So, we would have expected that the various asset classes would evolve independently, as investors or speculators projected a different mid-term future for each of them. Well, at least lately, this has not been the case at all.

- Before mid-2017, the correlations between altcoins and Bitcoin (and among altcoins themselves) were quite messy. Since then, the increases and decreases in correlation are much more of a crowd move. The particular case of Ethereum is extreme: at the beginning of its life, ETH was negatively correlated to BTC. Since mid-2018, its correlation has been 0.8.

- Almost all correlations increased from below 0.5 to above 0.75 during the first half of 2018, which was the start of the bear market. Since July 2018, the correlations have plateaued, and recently the trend is for a minor decrease in correlation, especially Litecoin; everyone is free to interpret this as they prefer, but to us, a year-on-year low in correlation may indicate that the crypto market has been moving in a bullish direction.

Still, on correlation considerations, it is noticeable that the BTC rally at the end of June occurred simultaneously with a surge in the gold price, and expectations of accommodating monetary policies by the Federal Reserve.

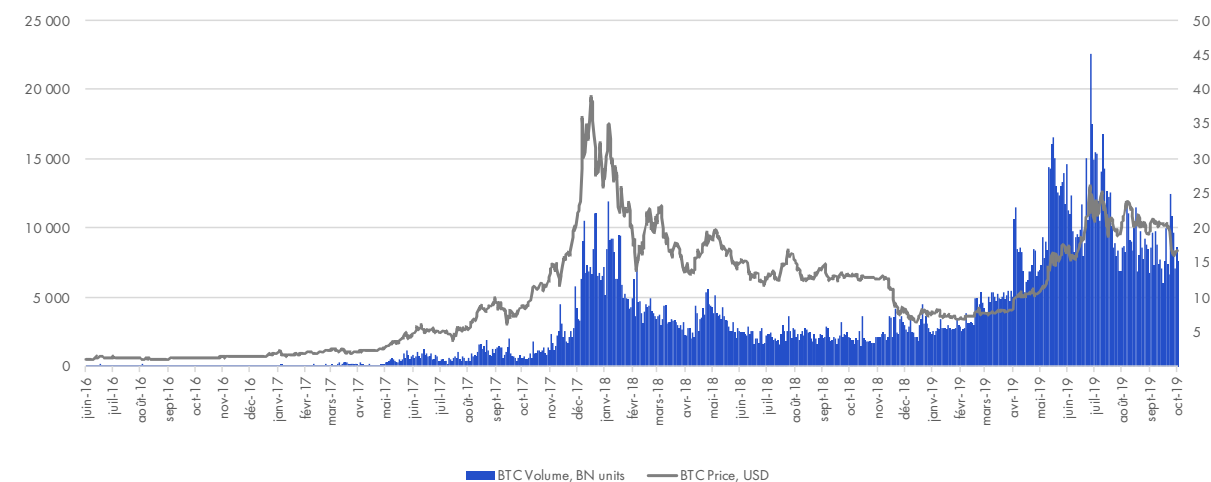
Exchange volumes

We can only confirm that off-chain exchange volumes have increased drastically in 2019, even when compared to 2017. They are also superior to the volume registered at the beginning of 2018 and considering that they are expressed in fiat terms, this is even more striking when transposed to cryptocurrencies.

After a peak at the end of June, volumes have stabilized. One can expect that the increase will resume during the next rally. (see Figure 1 and 2).

FIGURE 1:

BITCOIN PRICE DYNAMICS



Source: Coinmarketcap.com

INTERACTION WITH MACROECONOMICS

Articulation with the global economic situation

Whether due to an explosion of unrest in Hong Kong, the intensifying trade war between the US and China, or the Ormuz Detroit oil tankers at the center of Saudi-Iranian rivalry, it seems that the price of Bitcoin benefits each time. This is not to say that increasing world tensions are good news for cryptocurrencies, but one has to acknowledge that this might well be happening, and each time war scenarios are evoked, declining faith in fiat currencies, which are subject to depreciation, becomes a driver for a diversion towards BTC & co.

A significant piece of related news in the past three months was the decision by central bankers to maintain their accommodating policies. Central bankers usually tend to ease the money supply when the stock exchange collapses and lending by commercial banks declines, however, we are not yet in this situation, which is quite surprising.

The US Federal Reserve decreased interest rates by 0.25% to extinguish "threats ranging from uncertainties caused by Trump's trade wars, to chronically low inflation and a dim global outlook",

a move that has not been seen in over a decade.

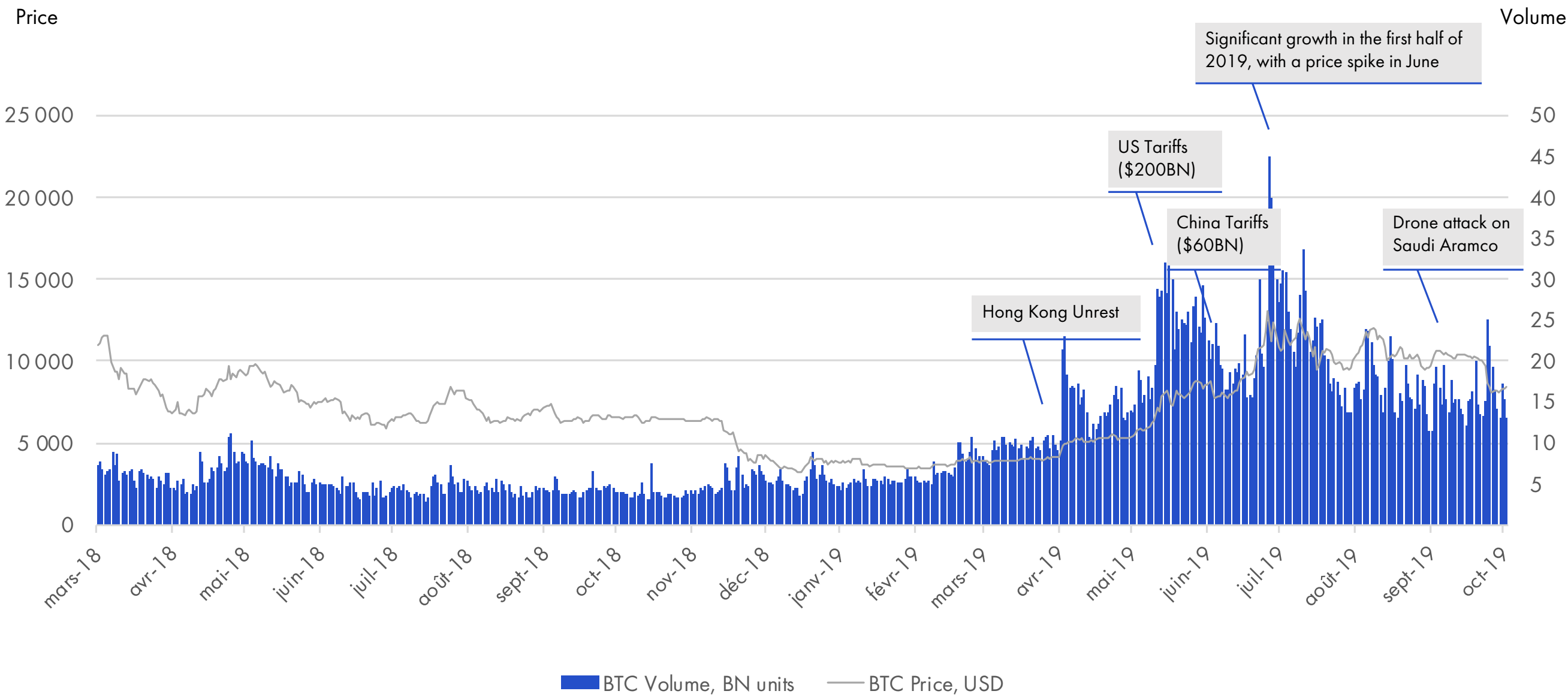
You may be wondering if this is a countercyclical attempt to pre-empt the impending stock exchange crisis, believing that governments cannot afford a rise in interest rates at the current level of debt. The reality is that the money supply is likely to remain plentiful shortly, or at least the expressed signal is that it is not going to be tightened.

And arguably, the relative sustained abundance of liquidity is good news for the short-term price outlook for cryptocurrencies and other high-risk assets.

Macroeconomic impacts of crypto-assets

AAAn interesting comment has come from Joseph Stiglitz – recipient of the Nobel Prize for Economics. He has stated that cryptocurrencies should be shut down. His view is that cryptocurrencies enable illicit activity by making financial transactions less transparent. He believes that the privacy of transactions should be fought because when more data is available in the real-time economy, it is more efficient and can be more effectively regulated.

FIGURE 2:
BITCOIN PRICE AND VOLUME DYNAMICS VS KEY EVENTS



Source: Coinmarketcap.com

2 UPDATE ON THE REGULATORY POLICIES

GENERAL APPROACHES BY GOVERNMENTS

Global evolution of official positions

The theoretic positions taken by regulators and officials are not drastically evolving in 2019. The embryos of formal laws and regulations come to a realization, with bills being passed that confirm the overall philosophy expressed in our previous reviews.

Finance ministers around the world have again voiced concerns and negative views of Bitcoin, as its price soared again in June. This was expected by many, and as yet, there have not been any negative consequences.

If anything, what we observe is a difficulty for regulators to classify the crypto assets they are dealing with properly.

Worldwide coordination

The intergovernmental Financial Action Task Force (FATF) is issuing dedicated guidelines to be followed by its member nations, in terms of requirements imposed on cryptocurrency exchanges regarding KYC. Crypto asset custodians will be obliged to obtain identification information before allowing any transactions to occur.

STATUS REGARDING OFFICIAL INITIATIVES TO PASS FIAT ON DLT

We can safely say that most, if not all, central bankers are currently studying the opportunity of issuing fiat money as blockchain-based units of account. The questions that remain unanswered include:

- Will issued central bank money be available only to commercial banks, or will central banks go a step further and make it open to the general public?
- Permissioned vs. public DLT: we can bet it will almost always be permissioned blockchains.
- Which technology to use?

In practice, these studies are likely to be conducted in relative secrecy, as we have not seen any recent press releases discussing this, or claiming that there are plans to move forward. China is the only exception in this respect; there are consistent rumors of a team that is speeding up the release of central bank digital money on a blockchain, which seems to confirm that work is being conducted in that direction (see Figure 3).

CRYPTO-ASSETS IMPACTS ON WORLD MONETARY SYSTEM

Cryptocurrencies will have a significant effect on macroeconomics but has the potential to go even beyond that in reshaping the world's monetary system.

We have already had the opportunity to touch on this, primarily through a dedicated article: the current fiat system was inherited from post-Bretton-Woods agreements, unilaterally imposed by the USA, and still in effect today, with the United States dollar playing an unchallenged role – until now. During press reviews, we continuously run into countries and populations relying on cryptocurrencies to circumvent the position of the USD and the consequences it has in terms of the USA dictating political sanctions or using its power to advance their interests. So, it is interesting to reiterate elements in an orderly fashion.

- Countries under US sanctions, such as Venezuela and Iran, have been trying to create some tokenized assets to create financial margin outside of the global USD-dominated system. Similarly, North Korea is hacking cryptos to gain some currency it can use to obtain foreign cash.

- In those countries and other failed states, populations are turning to cryptocurrencies as alternatives to their official fiat currencies, and the USD.

- Federal Reserve policies on the USD are decided unilaterally by the USA, but impact all countries on the planet, as most international trade, starting with energy, is priced in USD. Without a doubt, this is not an acceptable long-term situation.

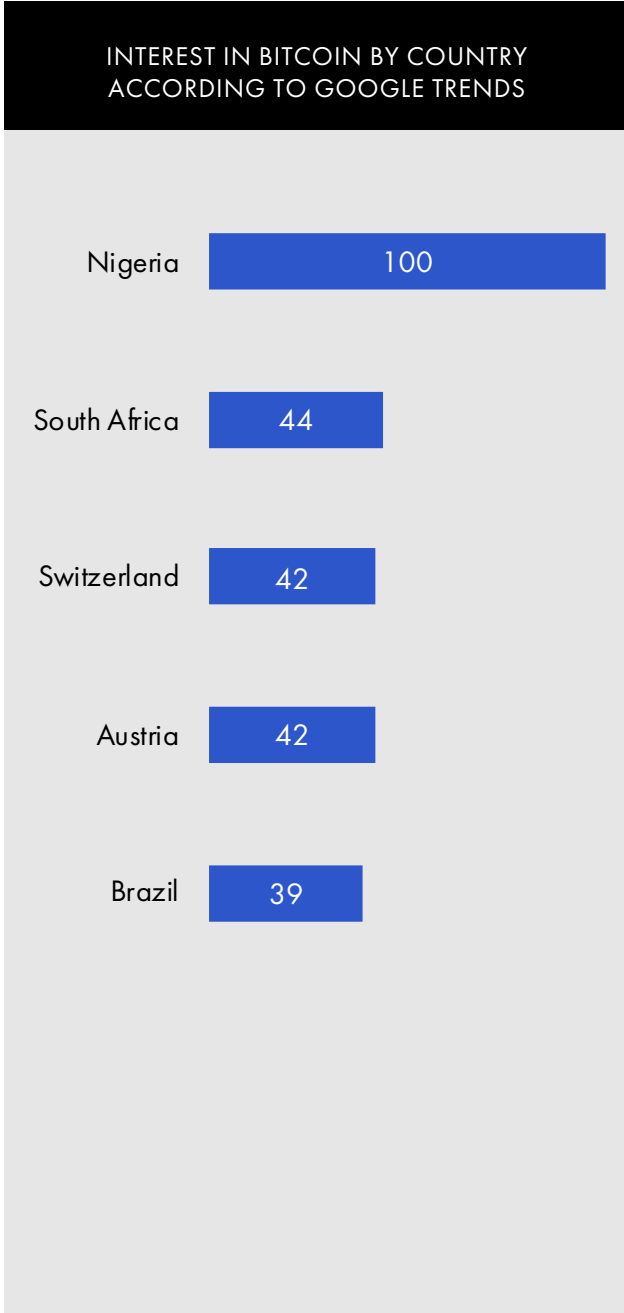
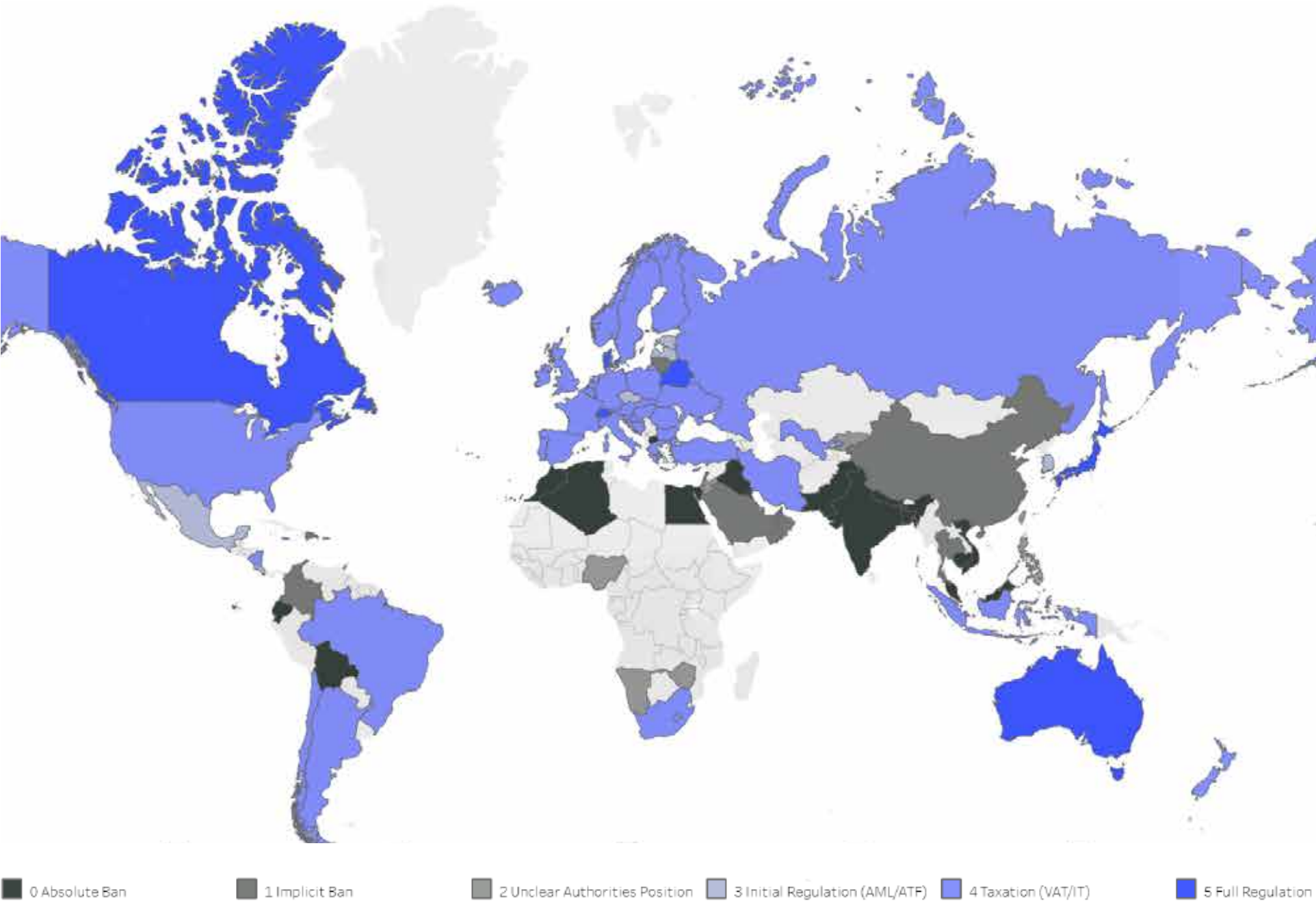
- The extraterritoriality of US laws related to USD transactions is driving non-US companies, especially European companies, to respond to abusive US legal actions. The loss of sovereignty here is such that the pressure to use an alternative to the USD is vast, and therefore the appetite for tokenized gold, for instance, is likely to grow.

REGULATION OF INITIAL CRYPTO-ASSETS OFFERINGS

Regulating public offerings of crypto assets has crystalized with the fight against the American SEC over whether or not to consider a given token as a security. The truth is that even before considering what requirements are to be imposed on issuers (and buyers) of crypto assets, the difficulty is inappropriately categorizing them to be capable of defining sound rules, and then consistently applying them.

WE CAN SAFELY SAY THAT MOST, IF NOT ALL, CENTRAL BANKERS ARE CURRENTLY STUDYING THE OPPORTUNITY OF ISSUING FIAT MONEY AS BLOCKCHAIN-BASED UNITS OF ACCOUNT

FIGURE 3:
LEGAL STATUS OF CRYPTOCURRENCY CIRCULATION BY COUNTRY



Source: BQ Intel, Google trends

The fact is that currently, most regulators are faced with a vast range of different crypto assets, without being sure of how to classify them. The variety of countries and philosophies in characterizing securities is likely to add to the mess when different jurisdictions will decide to classify tokenized gold as a commodity or as foreign exchange. Financial authorities are currently struggling to make up their minds on even simple cases such as Bitcoin,

so the blur of utility tokens, even when defined in whitepapers (which is not always the case...), is likely to take time to be resolved.

In that sense, our classification, which includes five dimensions of characteristics, could assist regulators by building clusters of crypto-assets according to their relevant features, or by enunciating requirements related to each of the aspects.

FIGURE 4:

NUMBER OF BITCOIN ATMS WORLDWIDE AS OF SEPTEMBER 2019



Source: Statista

To finish, the following news in the field of official classification of crypto assets can be reported: the SEC has filed a complaint about a Canadian company, Kik, which raised 85M euros in a 2017 ICO. The American watchdog is arguing that Kik presented the fundraising as a means to save itself from the draught of venture capital. The judicial fight is on, with Kik claiming that the token was intended to be used on its platform. So, here we have a perfect example of the blur experienced by many projects that obtained lucrative funding by issuing an asset intended to have future value on a platform (including Binance-like tokens). The Canadian regulator has not taken a position, but the judgment of the US court may have significant

repercussions, whichever way it turns out.

One curious point is to observe the growing number of ATM machines offering deposits in Bitcoins. US and Canada are leading the peer group (Figure 4).

KYC / AML / CFT Privacy / confidential cryptocurrencies regulations

An exciting event occurred in the UK recently that says a lot: ZCash owners on the Coinbase exchange platform had a choice imposed on them to “convert, send, or be liquidated”. That is, British citizens are being prevented from holding ZCash on exchange platforms. We can bet we will see much more of this

happening.

Legacy bank management

This section is an appropriate place to share an extraordinary experience of a relative of ours in France. This will illustrate perfectly how the banking system has been going too far with KYC and controls, but it tells us a lot more.

One of our relatives wanted to send some money to a major crypto exchange. It was only a small amount (a few thousand) that would routinely be transacted without much checking by the bank, that is, not ringing any “big movement bell” on the banker’s desk. But, in this case, the transfer took weeks, and then our relative received a letter in the post from his branch advisor, informing him that the money had been blocked until he completed and signed a form stating he had been warned and discouraged by the bank from acquiring cryptocurrencies. He was also required to declare that, under no circumstances explicitly, would he place responsibility on the bank. A press release from the AMF (French Financial Markets Authority) dated two years prior was attached, warning against price volatility and that there was no recourse attached to cryptocurrencies.

Our relative went berserk and turned to us to check if this was an isolated case. He could not accept (and who would?) that some company would judge or condemn what he does with his money, and in this case, even take steps to prevent him from disposing of his wealth as he pleased. We were able to quickly find other angry customers on social media complaining of similar situations. It appears that Crédit Agricole is systematically discouraging all its clients. Clients that transfer money to Kraken, Coinbase, or other exchanges are consistently threatened and inconvenienced with deliberate complications.

So, what does this tell us? Several things, some of which are quite profound. We have already discussed most of them, but they relate in an interesting way, which we will outline here.

First, let’s recap: banks routinely perform scans and

systematic checks on all money that they transact on behalf of their clients. This is a concern in terms of invasion of privacy. Very constraining legislation is being enacted on this matter, especially GDPR in Europe, to prevent companies from inappropriately handling the data of citizens. We can only observe that these general principles imposed by the state do not apply to the state itself. State officials believe that they have the right to monitor very private data related to what people buy and invest in, and how they deal with their wealth. It is difficult to accept this from the states - and the debate has only just begun.

So, it is a fact that today, as an individual or a company, the state requires that all your financial dealings are monitored and thoroughly checked (by robots, then humans) when a significant transaction occurs. The justification for this is to fight fraud – all sorts of fraud: corruption (the blurred limits of which are subject to broad interpretation), terrorist financing (the definition of which will often depend on which government you ask), and tax evasion (notwithstanding the iniquity or confiscatory characteristics of specific tax systems). So, when Crédit Agricole becomes intrusive and extremely conservative, as they do, they act as a delegate of the state, or, if you prefer, in a manner that reduces their own risk of being accused of negligence by the state, should a fraud incur. So, it appears that public acceptance of state control in such a detailed and intrusive manner is seen as a trade-off, as they expect that, as a whole, their life will be better off with the prevention of terrorism, corruption, tax evasion, etc.

This raises two questions: 1) Is this trade-off balanced by the status-quo, that is, does the control achieve its aims?; and 2) is there no alternative to this trade-off?

Answering the first question is touchy. Measuring the benefits of a policy without knowing how things will turn out if it were not implemented, is almost

THE BANKING
SYSTEM HAS BEEN
GOING TOO FAR
WITH KYC AND
CONTROLS

SECUREKEY
TECHNOLOGIES HAVE
CREATED A MOBILE
APP, VERIFIED.ME,
WHICH HAS A DLT
BACKBONE BASED ON
HYPERLEDGER FABRIC

impossible. Terrorism has not been defeated, and it is unclear whether tight financial controls are preventing their activities. What is sure, on the other hand, is the substantial cost to society that financial control incurs – paying hundreds of thousands, maybe even millions of employees to fulfill this incredibly dull, non-productive, harassing task. And at the cost of hundreds of billions of euros annually – look at the turnover of audit companies. This is an evident and inevitable cost that would have to be similar to the price of a higher fraud level. So, to us, the answer to this question is not so clear.

But answering the second question is even more impressive. If we believe that the privacy of the financial behavior of individuals is a goal in itself, there are ways to achieve it. Preventing tax evasion can be done by taking a cut of people's income when it is paid, as is done already in many countries. An appropriate method to achieve this can be devised and implemented, and then, if individuals own some money, it is theirs, and nobody should be watching what they do with it from a taxation perspective. That would be far easier and make more sense, philosophically. Preventing terrorism is a matter of avoiding the sale of dangerous material; the control of weapons and surveillance of hazardous activists

is far more efficient. Financial investigations could be authorized for such monitored individuals; for the rest, leaving people alone is a case to be defended. As for corruption, enforcement of some processes can do the job.

We should never forget that Bitcoin was invented specifically to enable people

to short-cut the controls of large corporations, and more or less, legit official bodies. This was the clear intention of the "peer-to-peer cash" system. What remains unclear is what Satoshi would say about the implementation of anonymity into DLT protocols, because a pseudonymous environment allows for enhanced and easy traceability of crypto asset movements – they are visible to everyone.

It is necessary to have superior knowledge to be able to associate an account with an individual, but the NSA, FBI, and CIA have proved that it is astonishingly easy to do, so one should assume that this is the norm. One could even decide to make it official and transparent; that would not defeat the purpose of peer-to-peer money because nobody would oppose the movement of funds if they can see it happening. But one is tempted to believe that Satoshi, himself anonymous among the anonymous, would take the position, as we do, that payment data should be kept private and untraceable. So, it would seem that Bitcoin falls short of the goal that Satoshi set and that MimbleWimble, ZKP implementations, and Monero are the crypto assets that are delivering on the promise. They are the ones that are going to be fiercely fought by states and regulators all over the world.

Back to Crédit Agricole, on social networks, their customers and random commentators cannot find words strong enough to condemn the bank's behavior. What shocks most people, in this case, is the actual roadblock put in place by the financial institution to prevent people from disposing of their own funds as they please, whether to go to a restaurant, purchase a plane ticket to a dodgy country, buy cryptocurrency, or to make a donation to a controversial political party. This censorship by powerful institutions is not acceptable – this must be said, and dissidents should proclaim it loudly. When one looks at Crédit Agricole's warnings and precautions, it is easy to think: "Guys, you have no understanding of what is going on here." Bitcoin came along precisely to make sure that this sort of situation could be overcome by anybody.

This relates to the usage of money, but there are also concerns regarding investigations by financial institutions into the origin of funds. Today you are systematically asked to explain, at length, where your money comes from when you want to transfer funds from one place to another – before the people that are keeping your money comply with your request; this is insane.

To make things clear, we pay these bankers to

hold our savings. They run a profitable business by providing this service. Usually, when the money is deposited, there are few, if any, questions asked. The least you can expect is that when you need your money, you will have access to it. So, when the system does not operate this way, clients can't understand why banks don't merely instruct their IT systems to subtract some numbers from an account and add it to another. The bank gets paid for doing this, sometimes a lot, so they should execute, as instructed.

HSBC is also reported to be blocking all transactions related to cryptocurrencies, so this story is indeed not isolated. So, it appears that, when it comes to crypto assets, banks do not know what to do or how to behave. There is probably an element of being afraid of the unknown – the pressure of potentially being disrupted or becoming obsolete. Preventing people from reaching out to the new financial system highlights that banks are in fear of losing their business position. Commercial banks are becoming paranoid – just an observation.

In conclusion, when looking at this situation, this is no wonder that Bitcoin has so many enthusiasts. One could say that cryptocurrencies appeared just in time to enable people to be their banks, and manage their wealth as they please. And to reiterate, if regulators have the will, some other means of control can be found to fight money laundering, terrorism, and corruption, which will have nothing to do with monitoring all financial flux on the planet.

Blockchain-based solutions

As we predicted, DLT-based solutions are beginning to appear in an attempt to ease the systemic KYC challenges. SecureKey Technologies have created a mobile app, Verified.Me, which has a DLT backbone based on Hyperledger Fabric. It appears to be working, with users storing their data on the blockchain, and granting access as they please.

3 REVIEW OF BLOCKCHAIN INDUSTRY PLAYERS

MINERS

Market growth and profitability

Bitcoin hash rates are hitting new all-time-highs. On Ethereum, the cost of operating the network is now estimated to be close to half a billion euros yearly (Figure 6).

Mining is attractive again, overall, but it still depends on cryptocurrency prices. Small PoW coins have not enjoyed a revival as strong as the major ones. As a corollary, these coins are becoming less and less secure and more prone to attack.

Material

With the price of Bitcoin going up, mining profitability has again taken off, and miners are seeking to equip themselves with cutting-edge equipment. The Bitcoin mining difficulty is at all-time highs, with the block halving projected for May-June 2020.

ASIC manufacturers are swiftly re-entering the market, with machines that have unprecedented power (70 terahash/s), and that is more economical (0.01Wh/terahash).

So, all in all, the cryptocurrency mining industry is recovering strongly from the bear market. A significant new player is entering this lucrative market: Samsung.

Business finds markets in all directions: some mining applications have been developed to run on small devices like smartphones to enable individuals to engage in cryptocurrency mining using a small device (e.g., Honeyminer).

The concentration of hash power

Siberia is touted as the new mining Eldorado, a cold climate and cheap energy. But, probably still not sufficient, in itself, to drive the Chinese miners from their dominance!

The ASIC-resistance battle, led by Monero, has had unexpected implications that are worth mentioning. While hardware designers and producers have proven to be very efficient in bringing specialized equipment to the market, the struggle to have the protocol evolves (implying hard forking) to preserve the decentralized character of cryptocurrency mining has had the unexpected consequence of centralizing the power in the hands of the developers that are trusted with this evolution, and with hard forking. This is interesting philosophically: it proves that maintaining decentralization is always a considerable effort in itself, as human nature still causes individuals to work for a bigger slice of the cake for themselves...

Environmental issue – electricity consumption

It is often said that Bitcoin mining has a disastrous environmental impact due to the waste of energy resulting from Proof of Work. When looking at this a little closer, while the amount of raw power consumed for absolutely nothing (other than claiming the network is secure) can be

FIGURE 5:

BITCOIN ENERGY CONSUMPTION

Minimum TWh per Year



Source: Digiconomist.net

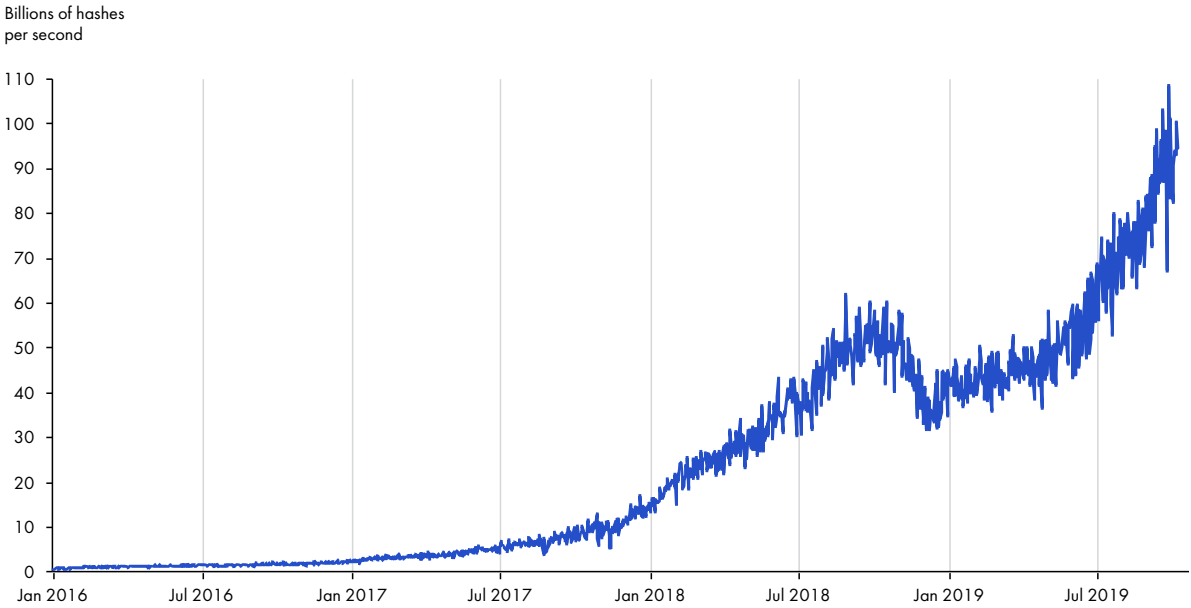
compelling, the situation has to be nuanced (Figure 5).

Electrons do not (yet) have a color when they emerge from the power socket. Nevertheless, it is a fact that many, if not the vast majority of mining farms, are situated close to "renewable" energy facilities, primarily hydro. This is the case in Québec, Sichuan, Switzerland, etc., and in Iceland, geothermal energy also qualifies as "clean" (Figure 7 and 8).

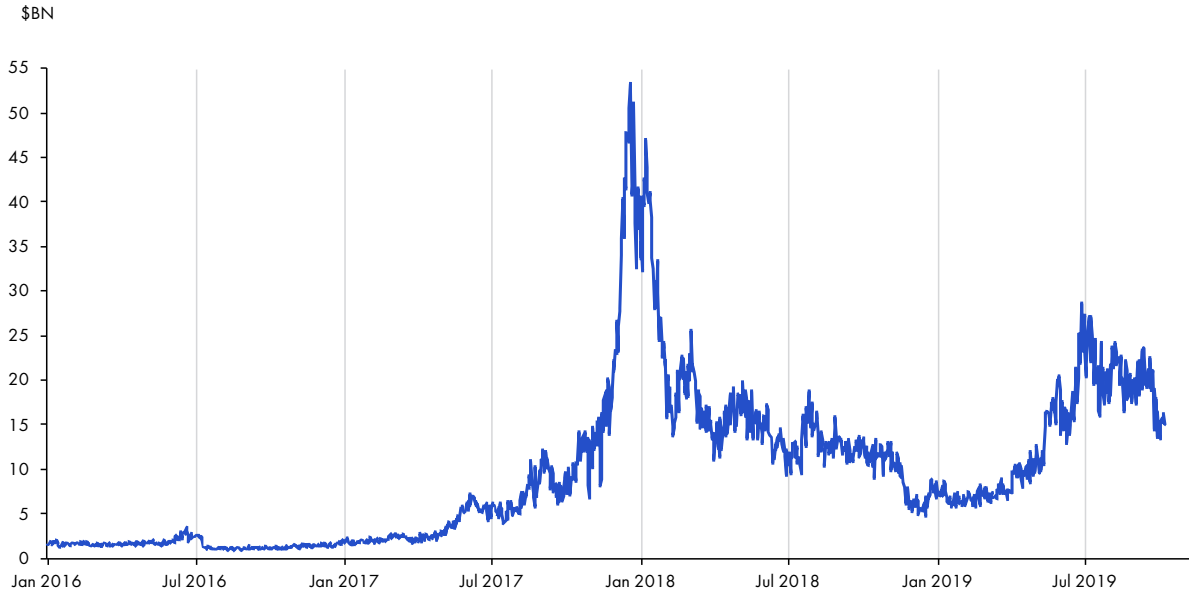
To extend this line of thinking, arguably, at several sites, a significant portion of the power consumed by mining would have been lost. Hence, the real impact of mining on the climate is significantly less, and overall,

FIGURE 6:

BITCOIN HASHRATE



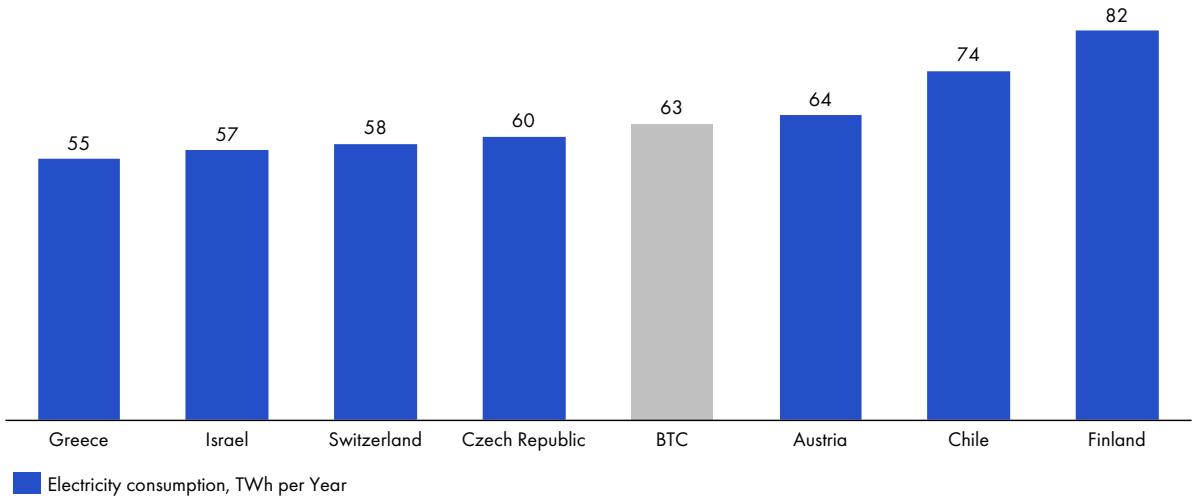
BITCOIN MINERS REVENUE PER DAY



Source: Statista

FIGURE 7:

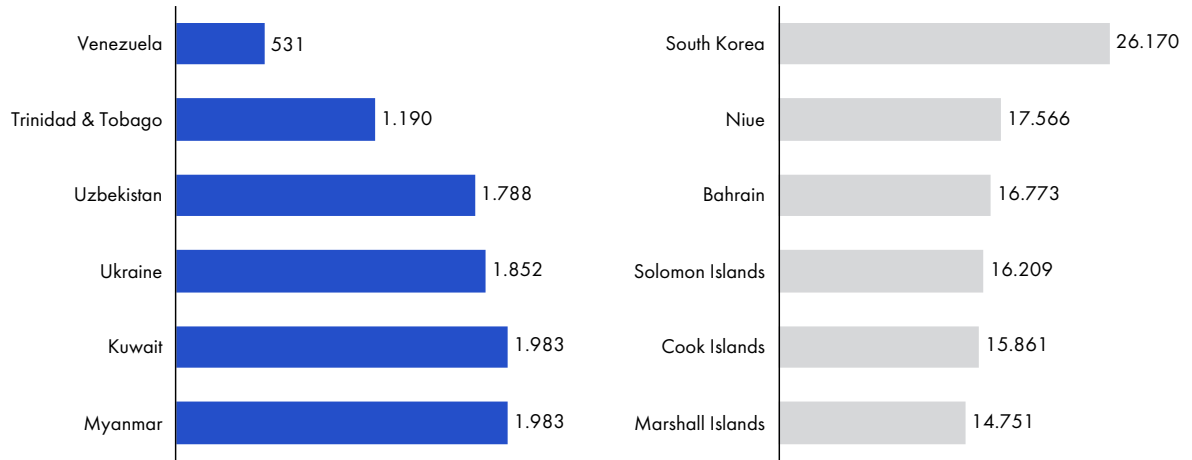
BITCOIN ENERGY CONSUMPTION COMPARED TO OTHER COUNTRIES



Source: stats.oecd.org

FIGURE 8:

CHEAPEST AND MOST EXPENSIVE COUNTRIES TO PRODUCE BTC, USD



Source: Investopedia

the effect of PoW is not quite as terrible as it seems. The mining lobby has begun to express these points in an attempt to clean up the image of the industry.

EXCHANGE PLATFORMS
Decentralized exchanges (DEX)

A phenomenon has appeared – or rather, has been exposed – on decentralized exchanges. This has to do with arbitrage bots that exploit inefficiencies in the exchanges to make profits. Basically, by paying high fees for transactions, it is possible to prioritize some executions in a manner that cannot be achieved manually by traders.

A Cornell research paper states that “Like high-frequency traders on Wall Street, these bots exploit inefficiencies in DEXs, paying high transaction fees and optimizing network latency to front-run, i.e., anticipate and exploit ordinary users’ DEX trades.” It further estimates that this is not a minor phenomenon; potentially hundreds of millions, if not billions of euros worth of crypto assets, could be extracted from the market due to this phenomenon.

To an extent, this highlights the power of miners: when they favor transactions with a higher-

paying fee, less profitable orders are penalized with delays. Moral: in this new and decentralized financial environment, unexpected dangers need to be taken care of!

Otherwise, one aspect worth mentioning is that the pressure for the control of centralized exchanges, pushed by international financial taskforces, is likely to accelerate efforts by the community to make decentralized exchanges work.

Off-chain crypto exchange platforms

Objectively, exchanges have become very powerful. With great power comes great responsibility. To illustrate this, a compelling case to analyze is Binance’s move to delist BitcoinSV. Even though this cryptocurrency’s fork was dubious, the decision to delist it came abruptly, and directly from the CEO, Changpeng Zhao, apparently to punish the primary individual behind BitcoinSV who claims to be Satoshi Nakamoto. This is a question of principle: clearly, Binance is a central player in this space, so its actions cannot be ignored. As the most significant player, some could argue it bears some public service duty. The public will oppose arbitrary decisions in this context, and we can expect more of this to happen.

Talking of dominant positions; worldwide, CoinMarketCap.com is a central aggregator of price and volume data that many refer to when they want access to crypto information. It is well established and exhaustive and has consequently acquired a central position. Following the fake volume scandal raised by BitWise a few months ago, CoinMarketCap has made an effort to clean up some of the mess. It launched a “Data Accountability and Transparency Alliance” that was immediately joined by the leading exchanges. And to go further, they decided to require exchanges to provide some mandatory data or face being delisted. This should have a clear and direct impact: we shall see if it triggers concrete change!

All of this is a consequence of the massive market that the cryptocurrencies exchanges have become.

Looking at such an attractive business (Figure 9), many actors are eager to capture a share of the market, and in such an unregulated environment, all methods are employed to attract traders. The present proliferation of exchange platforms is good news, as competition is critical to push for better services, but only time will tell how the industry will ultimately evolve, as many small, crappy exchanges are currently profitable despite offering very low liquidity.

Legacy exchanges

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

CUSTODIANS

Custodians of crypto assets are still relatively small players. They are by no means unique in the landscape; actors like Bitcoin Suisse, Xapo, and others have been around for a long time. But lately, they have been promoting their service more actively, either in forums or by advertising. The offer of cryptocurrency vaults, in the sense of safeguarding private keys for customers, is, of course, a segment of the value chain that appears to be becoming profitable.

Crypto exchanges are integrating vertically to become crypto asset custodians, which they have always been, in many ways. The decision by the asset manager, Grayscale, to move their billions of euros worth of BTC, XRP, and LTC to Coinbase is an example of this.

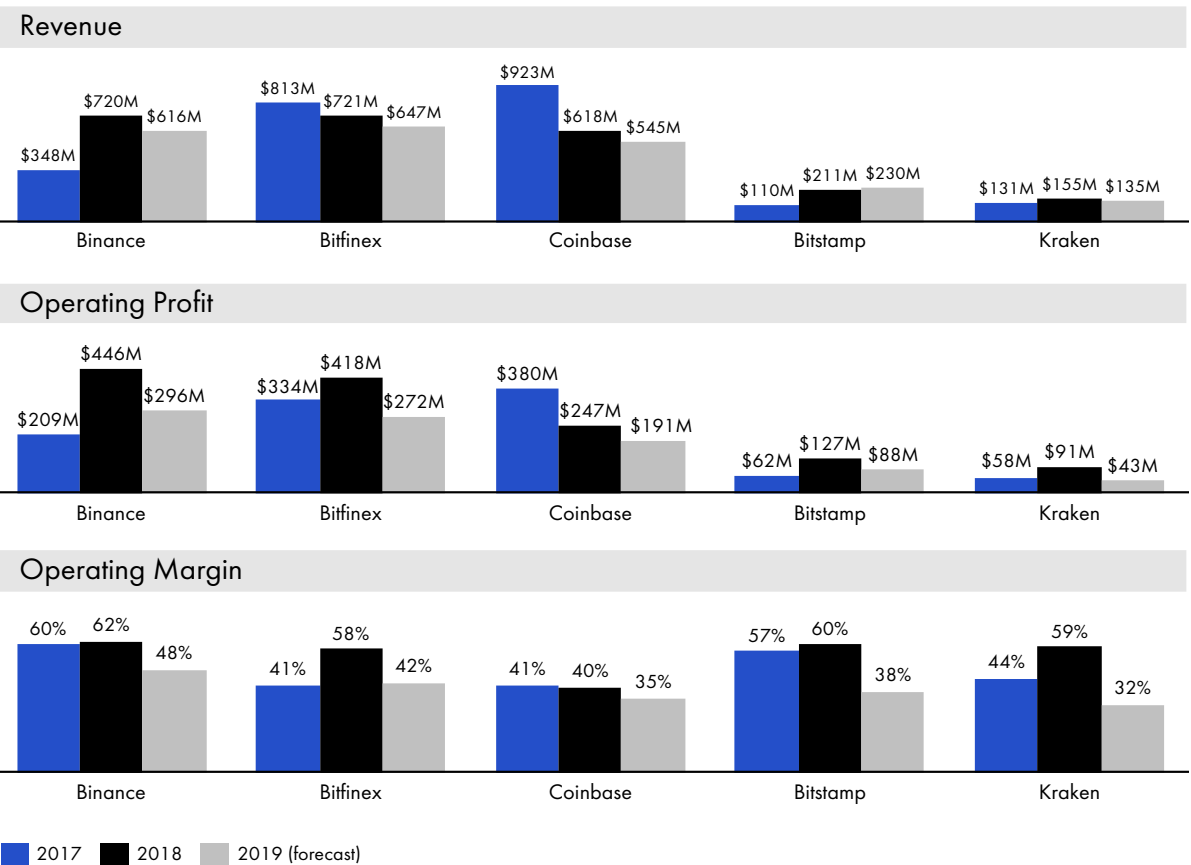
MONETARY EROSION

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

BLOCKCHAIN CREATORS, ENTREPRENEURS

The surge in the price of Bitcoin in the first half of 2019 had a positive impact on the value of ICO tokens. Altcoins prices, overall, tripled in market cap, from their low point in early 2019 to the peak in June. But, while infrastructure tokens have kept some of these gains, most, if not all of the tokens issued in 2017 and 2018 for fundraising purposes

FIGURE 9:
REVENUE, OPERATING PROFIT AND MARGIN FOR TOP 5 CRYPTO EXCHANGES



Source: BQ Intel

■ 2017 ■ 2018 ■ 2019 (forecast)

are, with a few exceptions, back to their lowest levels (as of September 2019), and a number of them are even plumbing new depths. Analyzing the reasons for this is difficult, but we believe that the need for finance to sustain the founders and pay employee wages is likely to result in selling pressure on utility tokens while their models have not yet demonstrated viability.

Examples of such tokens include TenX, Melon, Gnosis, PundiX, LAToken, Power Ledger, SirinLabs, Polymath, Mithril and many others that, despite having a sound team (in principle) and some deployed products and services, are obviously struggling to gain traction and investors' confidence, all the more so with the "utility token" financing model.

For the people behind these projects who are genuine and still committed to the success of their value propositions, this is, of course, a catastrophe. As cash is needed to continue the development and build the business, for many, survival depends on whether the capital raised by the ICO has been well managed or if it has shrunk dramatically to the point that another round of fundraising is necessary. On the other hand, if the project had foreseen difficult times and kept some tokens aside, another fundraising may be possible, but at the current market for tokens is hardly favorable for that.

As such, the only alternative, for the majority of projects, seems to be the classic VC financing method. It's a reasonably safe bet that, in this situation, many more projects are likely to die soon, paradoxically, despite any revival in the Bitcoin price.

INDIVIDUALS ACTING FOR THEMSELVES Whales

It is challenging to validate the information from private brokers. For example, the story that hit the headlines that Dadiani Syndicate was approached by a wealthy client willing to buy up to 25% of all existing Bitcoin is probably fake news to create interest. Nevertheless, this tends to indicate that wealthy individuals were buying massive amounts

of cryptocurrencies in June, mainly Bitcoin.

Concerning whales, a significant number, if not the majority of them, can be qualified as "new rich" young people, an emerging socio-cultural category that marketers have already been curious about studying, and unsurprisingly, their consumption patterns indicate the acquisition of "bling-bling" goods, expensive cars, and luxury mansions. Vendors of these goods have identified the segment, and are offering cars for sale with payment exclusively in Bitcoin, and apartments in Dubai reserved for buyers who prefer to pay with cryptocurrency.

Casual holders

Individuals holding cryptocurrencies resumed their interest, mainly due to the BTC price surge. However, from our observation, even among the most enthusiast circles, there are still mixed feelings, and while some have once again taken positions, they are not the majority. To that extent, there is still some upside potential.

Overall, individual holders still account for most of the trading volumes. However, their share of it is being reduced by the increase in institutional activity.

It is also worth noting that there is a high probability that casual holders who entered during the first half of 2019 will hold their positions.

INVESTMENT FUNDS

PE/VCS

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

Private bankers and classical investment/ hedge funds

Justin Sun, the controversial CEO of TRON, has bid \$4 million to be the guest of a Warren Buffet charity lunch. This was quite a media coup, but Sun canceled the lunch due to health reasons. However, there are suggestions that Chinese investigators are preventing him from leaving the country...

Anyway, Warren Buffet does not appear to be ready for conversion: in August, he repeated how much he believed that Bitcoin does not produce anything, which means it's just a bubble, like tulips in their day. For this reason, he would never hold BTC rather than invest in productive businesses. This summer, critics of cryptos have been pretty active, with media coverage.

Otherwise, the SEC has again delayed the examination of three Bitcoin ETF proposals; decisions are expected in October 2019 – stay tuned.

Dedicated (and new) crypto investment funds

As of mid-2019, an audit of crypto hedge funds shows several holes in their management and reporting, let alone the varying independence of their directors. From this, we can acknowledge that this industry is so young that it needs to consolidate at every level of its business.

A report by PWC giving the results of a study of 150 crypto funds holding a combined billion euros (uncertain of the date) confirms that, despite the bear market in 2017, they were able to increase their assets under management from significant subscriptions by clients. The interesting data from this report also mentions that average assets under management are €20 million, and only 10% manage more than €50 million (among them, Pantera and Polychain). The funds are overwhelmingly based in the Cayman Islands, with the teams typically working from the US. This looks like a traditional finance scheme: nothing has changed in this respect!

The most significant crypto investment funds are Grayscale (€2 billion in assets under management), Polychain Capital (close to €1 billion), and Pantera Capital (€650 million). Grayscale has revealed that 84% of its client base were institutional investors. Other, more 'classic' PE/VC funds are investing tens, and sometimes hundreds of millions in the crypto-world through these large "pure" players.

On the contrary, PWC reports that more than 60%

of 150 active crypto hedge funds have less than €10 million in assets under management.

UNIVERSITIES AND RESEARCH CENTERS

Recent issues of Blockchain Quarterly have identified a trend of significant activity, both in proposing dedicated DLT courses and in research programs being financed. Fundamentally, we observe that the movement continued and strengthened during this quarter. Here are the most prominent related headlines:

- The Wharton School of Pennsylvania has issued some online programs about financial technologies, including a significant focus on digital currencies.

- The National University of Colombia has joined the global blockchain consortium for science, dubbed Bloxberg, to establish an infrastructure that broadens the scientific landscape of regionally and nationally governed blockchain networks to become the first genuinely globally-maintained decentralized network by scientists for science.

- One of Ireland's prestigious higher-learning education institutions, Dublin City University, is fortifying its crypto stance in the financial world with a new online master's program in blockchain technology, with the help of funding from the Irish government.

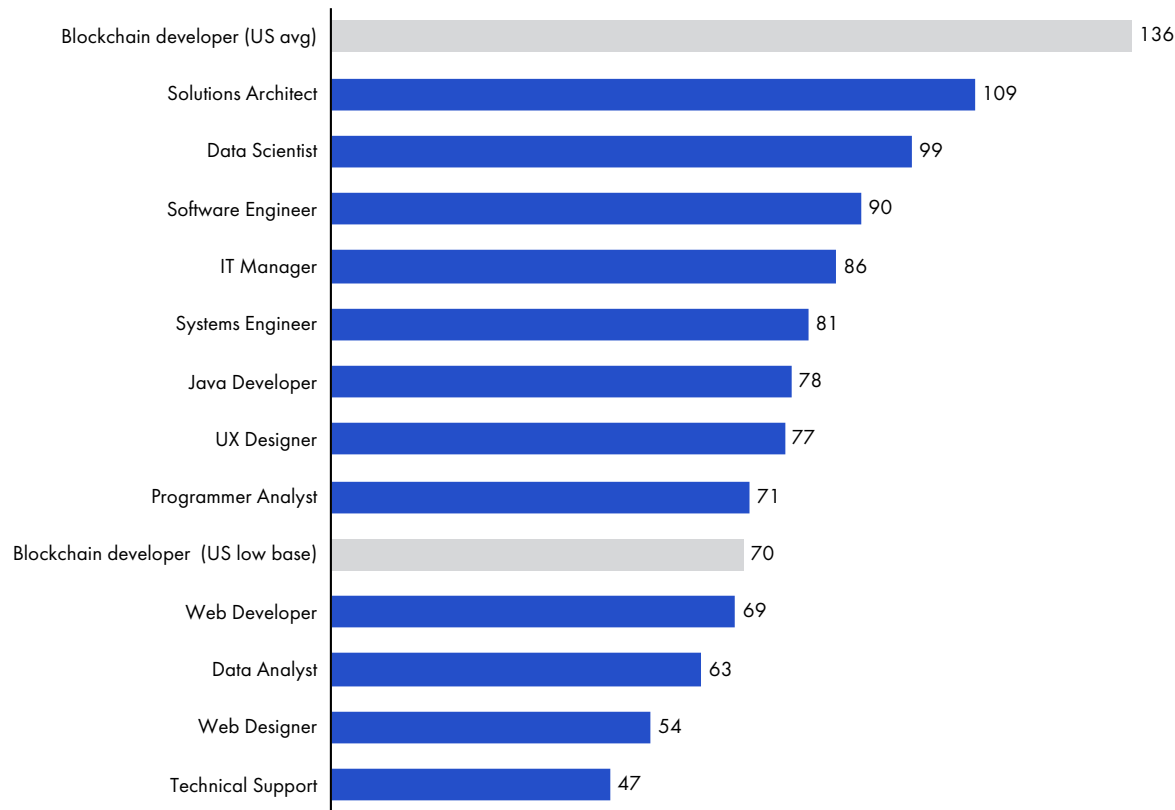
- The University of Nicosia in Cyprus was the first in the world to offer students the option of paying fees with Bitcoin.

EMPLOYEES – TALENT

One has to wonder if a shortage of technology-educated workers will be a significant roadblock to unlocking the potential of distributed ledger technologies in the coming years. Not only are there some mechanical delays for populations to gain exposure, get interested, get involved, and adopt the technology, time is also required to build a sufficient pool of competent professionals to make it happen. All of this takes time; it is not just a matter

FIGURE 10:

AVERAGE SALARIES FOR TECH SPECIALISTS IN USA, \$1K



Source: Glassdoor; Hackermoon

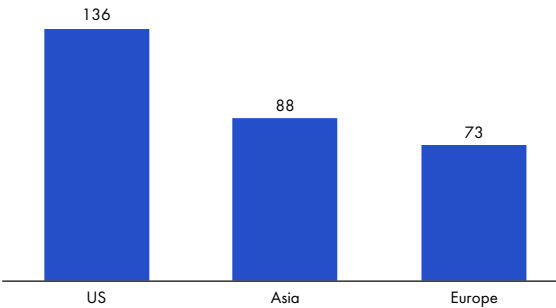
of the technology maturing. To us, these are, in fact, independent concerns. The problem is, these concerns are not easily quantifiable.

A shortage of DLT-qualified talent is evident everywhere; we can accurately quote shortages reported in Australia, and a 300% + increase in demand for blockchain skills in the US, year-on-year, etc (Figure 12).

To get an order of magnitude, a comprehensive study of blockchain consulting prices shows that a distributed application developer costs €200 per hour in the US, €120 in Western Europe, €70 in Eastern Europe and €35 in India (Figure 10 and 11).

FIGURE 11:

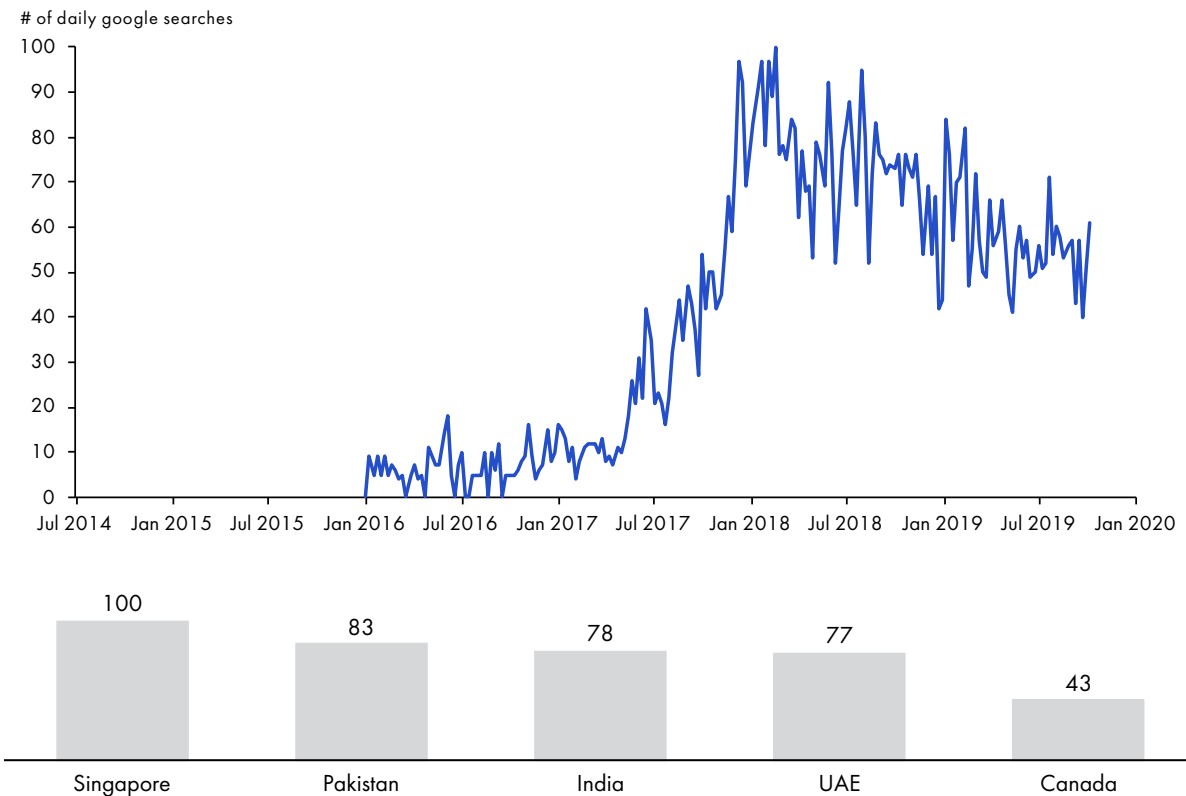
AVERAGE SALARIES BY REGION, \$1K



Source: Hackermoon

FIGURE 12:

INTEREST IN BLOCKCHAIN DEVELOPER POSITION WORLDWIDE



Source: Google Trends

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

This quarter, it is quite difficult to project which money is flowing in and out of cryptocurrencies.

- There is still a net outflow of money from the ICOed start-ups that are now struggling with the collapse in the prices of their tokens, and their need for further financing. Exchanges and miners also routinely add to this selling pressure, particularly for ICOs in the infrastructure token category.
- Individuals still appear to be quite cautious, even though they explain, at least partly, the spike seen in March-June 2019. In the short term, it is unclear

whether they will become more involved, despite the apparent appetite for cryptos that is emerging in developing countries. Ultimately, the buying pressure has to come from people willing to use cryptos as an everyday vehicle of value, and this still appears to be far off, even though there has been progressing.

- Institutional investors still lack the legal framework and the risk management models to enable them to pour substantial funds into the crypto environment. Despite this, we have observed some movements in this regard. However, fund managers are still not comfortable with cryptos and are averse to taking the responsibility of being criticized if there is a collapse.

4 INVESTMENTS & USE CASES BY INDUSTRY

Here are highlights of the latest DLT applications by sector. Insight: some elements relevant to this sectorial round can be found in the section that reviews tokenized assets.

BANKING

End-customer payments

Let's highlight here that Visa and Mastercard are participating in the Libra initiative.

Tokenized financial titles

- Société Générale, the French bank, has issued bonds to the value of €100M on the public Ethereum blockchain. A fun fact was that a sole entity acquired the bonds, and guess what? It was Société Générale itself! As the proverb goes: "On n'est jamais si bien servi que par soi-même." [You are never so well served than by yourself.] With this amount of bonds involved though, it is hardly just a PoC, and the bank has explained that it gains overall because of increased transparency and reduced likelihood of errors arising from the complexity and the number of intermediaries involved in issuing covered bonds using traditional means.

Interbank settlements

A group of 14 banks (European, Japanese, etc.) led by UBS, launched a trade settlement platform based on blockchain.

Another consortium of banks, in conjunction with the London-based Finality International, is organizing the creation of a dedicated cryptocurrency for cross-border transfers and settlement among themselves.

This all indicates that banks are trying to build, by cluster, their solutions to compete with Ripple and with the JPM dollar, in a bet to avoid being overtaken, especially by JP Morgan. This domain continues to be at the forefront of use cases at banks and is increasingly competitive: the trend continues. Interestingly, for the moment, neither JP Morgan nor others are considering issuing their currency to the public – which sets them apart from Ripple.

Custody and management of crypto-assets

The Korean institution, Kookmin Bank (KB), is moving towards proposing custody of tokenized assets/cryptocurrencies.

Banking crypto-related businesses

Overall, the divide between crypto banking and traditional banking is only increasing, with the two worlds often willing to avoid interfacing with each other, and crypto businesses being pushed to find alternative

solutions on their side. Consequently, the crypto world is incentivized to develop fast.

In Israel, the crypto start-up battle for general banking services is embodied by "Bits of Gold", an exchange that is being taken to the judicial courts. Banks are not legally obliged to serve a client, and there are only a handful of banking institutions in the country.

Trading

Grain trading, supported by a blockchain infrastructure, is being tested in Colorado. Promoters of the initiative quickly realized that they needed to extend the outreach of participants to have a chance of enabling their solution to gain momentum.

INSURANCE

Two American insurance companies, USAA, and State Farm, are engaging in a process leveraging blockchain to pay each other when two of their customers are involved in an accident. It is foreseen that regular settlements will be made between the companies, resulting in savings in processing, reconciliations, and error reduction.

Allianz SE from München is developing a blockchain-based ecosystem to facilitate cross-border insurance payments for its corporate customers.

SUPPLY CHAIN

Salesforce, a software editor, is detailing the benefits of blockchain when full supply-chain traceability is implemented: thanks to great customer satisfaction capture, faster and better selection of providers can be achieved, which in turn can help to better target markets. Who said that we lived in a world fueled by data? One could object that it will take a long time to achieve effective data collection throughout the value chain systematically and reliably. Not to mention that Salesforce would be acting as the retributed data management, the third party!

Carrefour's blockchain tracking system enables customers to track the origin of 20 goods, including meat, milk, and fruit, from farms to stores. Customers will appreciate the ability to avoid products with genetically modified content, antibiotics, and pesticides, and the likelihood of commercial success looks positive, based on reports of increased sales. The brand expresses the intention to add 100 more products in the system this year.

A GROUP OF 14 BANKS (EUROPEAN, JAPANESE, ETC.) LED BY UBS, LAUNCHED A TRADE SETTLEMENT PLATFORM BASED ON BLOCKCHAIN

Nestlé, which had been participating in the Food Trust blockchain initiative (with IBM), has launched another project to serve its supply chain monitoring. Of course, Nestlé is a big enough player to work on its tool, which would then be imposed on its suppliers. However, it remains to be seen if other supply chain initiatives ultimately emerge, which will probably need to interface with Nestlé, or if the Nestlé's one will be robust enough to be expanded to other competitors, depending on whether they are willing to accept the Swiss company's head start. All industries are likely to face this sort of configuration, with big companies trying to front-run while it only makes sense to implement a system if all the market participants can participate...

Swiss luxury watch companies are researching ways to register their products on distributed ledgers. The eternal question here is, if a watch has just a serial number on it, while all relevant data on provenance, manufacturing processes, sales channels and owners is trustworthy and quickly recorded, what prevents a counterfeiter from putting an existing serial number on a watch and pretending that it's real? Here, the reasoning gets interesting. To customers that buy luxury, expecting the product to be genuine, it may be easy to implement some information about the current owner and make sure to check the identity of the seller to ensure a match. And thus, a unique serial number that only the manufacturer can create proves the point. But to the customer that is happy to buy a cheap counterfeit that looks precisely the same, checking the source of the object is not a priority – a market for such goods will still exist. The point is that, for enforcement, it could become more natural to ask customers for their blockchain registered proof of property. So, in principle, this can work. We'd point out that luxury clients are usually not interested in the burden of managing a private key and finding it when needed, nor are luxury retailers likely to displease their high-worth customers by asking them to prove they own genuine products. Furthermore, counterfeit is sometimes part of the marketing strategy of some brands (a component of their popularity). To connoisseurs, the difference is noticeable, and the real luxury world is all about that.

Still, on the subject of tracking valuable goods, another approach is to attach a connected device to the item, that is, a miniature IoT cryptographically identified on a DLT. The issue is then, how to make sure that the IoT device cannot be detached from an old or broken object to be put on a counterfeit; otherwise, of course, this approach provides more than the serial number, by feeding even product lifecycle data to the manufacturer, if so designed.

INFORMATION AND TELECOMMUNICATIONS

Apple and Samsung seem to be competing to embed crypto asset management in their respective devices. The Korean chaebol has a lead, as it already integrates a hard wallet able to manage private keys in its upper-end products, and it is reported to be working on a Samsung coin based on Ethereum, while Apple is maintaining its stance against cryptocurrencies. This again exemplifies the relative advance of Asia over America in the field of DLTs.

Google's blockchain activities have been surprisingly discreet, although it is hard to believe that many of the IT giant's teams are not enthusiastic and pushing the technology. The dearth of information that is filtering through shows that blockchain positions exist in the company and are increasing. However, the focus of the company is instead on studying how to provide services to companies, due to either direct public proposals or to improve its processes.

Microsoft has launched a decentralized identity tool on the Bitcoin blockchain. Baptized Ion, this open-source project is supposed to handle the decentralized identifiers of a given user when they choose to use it to access a website. Scant information is available on how it works, but one can infer that the choice of Bitcoin is essential to anchor the system on the most secure blockchain (most hash power for validation); and then probably a root of the Merkle tree is anchored in empty transactions, while the client gets a sequence of combined hashes. So that combined with the password and identity data, one can prove their identity.

IBM has applied for a patent for a blockchain-based web browser. Other initiatives have already proposed seamless integration of a wallet in internet browsers that allow for easy integration with decentralized applications; but in IBM's case, the attempt is to use blockchain to track and ascertain session data, mainly so that the user data is placed back in its control (see the paragraph on personal data management, the same principles apply).

MEDIA, INCLUDING SOCIAL NETWORKS

"FaceCoin" (nicknamed "ZuckBuck") is now out of the woods, and official. With its official name Libra, this is arguably the most critical piece of crypto news regarding social media, as FaceCoin is backed 95% by Facebook. Embedding a type of payment system has probably been on Zuckerberg's to-do list for a long time, even if it's not to lag too far behind WeChat. For a more detailed analysis of Libra, please refer to the "Payment Functionality" section.

The Korean messaging app company, Kakao, has launched its blockchain. Applications on it may follow; the real question is, if this is about a single-company infrastructure, what is the actual difference compared to a centralized database?

Otherwise, Voice, a social media platform, is being launched on EOS by Block.One. Everything posted and shared on the platform will be public (and stay there forever). Let's see how the public reacts to this...

TRANSPORT

Air

Etihad has partnered with a Swiss start-up, Winding Tree, to create an Ethereum-based system to support its flight times, travel itineraries, baggage tracking, etc. This will allow to cut overpriced third-party data management services. Back in October 2018, Air France-KLM also approached Winding Tree to work on the definition of a DLT-based system. The question remains whether an industry-standard can emerge from private initiatives of this kind.

Russian airline S7 has revealed it is using a distributed ledger to issue air tickets. The interest in using blockchain is to securely connect the ticket booking system to the banking system, speeding up payment processing and slashing the amount of manual paperwork traditionally required.

Another airline, Norwegian, has got its hands on a crypto exchange, to accept a range of cryptocurrencies for payment of airplane tickets.

Automotive

Bosch is partnering with the Germany-based electric utility company EnBW (Baden Württemberg) to test a prototype of blockchain-based car charging stations.

Shipping

As one of the most straightforward use cases for blockchain logistics, the shipping industry is still in the lead. The sector is now collaborating to produce the definition of a standard. The fact that ports enter into the landscape makes it essential to have a genuinely global approach that would not be the property or led by any particular market participant – a general trend with all ecosystems, as we will sum-up later.

HEALTHCARE

Consultants and observers have different economic projections for the "blockchain healthcare industry": €800M in 2023; a 70% annual compound growth; €1.5Bn in 2026; leading to savings in the healthcare sector as a whole of €100Bn. Now, all of this looks difficult to achieve, especially with all the world's economic uncertainties, but one thing is sure – everybody agrees there is money to be made!

CHARITY

The Plastic Bank, a non-profit organization, claims it will be turning plastic waste in the oceans into a currency. The plan is to reward people for collecting plastic (in some countries, a cynic could say that it is almost a conflict of interest! – why throw it away in the first place...). The hope is that environment-

friendly activists around the planet will purchase these tokens, thereby conveying value to them.

ADMINISTRATION AND POLITICS

To sum-up how DLTs are bound to change the way populations rely on their governments, the following can be identified:

- If the property and contractual engagements of civil parties are notarized (and potentially settled) on a blockchain, then it should bring some reliability to official recordings, that today, in many jurisdictions, are not satisfactory, too slow or even missing. Increased clarity and reliability will, in turn, reduce disputes or ease their resolution.

- Cryptographically secure identification of citizens can open the way for more direct democracy, as opposed to almost always representative democracy, as we know it.

BLOCKCHAIN
WILL SHORTLY BE
EVERYWHERE, BUT
INVISIBLE, AS A
FOUNDATIONAL LAYER

- Transparency and even traceability of financial allocation by public officials would be a new thing. We can imagine a world where officials are made much more accountable – not to mention assisting the fight against corruption.

- Some commentators have expressed the view that blockchain has the potential to simplify taxation significantly. If automation of taxable cash flows eventuates, and we can directly submit the tax component to authorities, then the cost of handling tax payments could be reduced, which is of particular interest to businesses. So yes, but maybe the tax laws should be simplified first!

In HR functions as well, blockchain is being seen as a means of transformation, especially when it comes to transparency of pay equality, more effective and feeless wages payment (especially abroad), and smooth and instantaneous checks on the educational background of new hires.

GAMING AND ENTERTAINMENT

A developer company is working on a game based on Star Trek, where spaceships embodied in ERC721 non-fungible tokens would be for sale. The game, CSC, will be an open-universe game where players command the starships.

Gambling and casino applications are still among the most popular because verifying the code running on the distributed virtual machines allows participants to ensure that the service provider is not cheating.

CONCLUSION ON INDUSTRIAL APPLICATIONS THROUGHOUT SECTORS

For some time now, the general feeling gained from producing this Quarterly is the remarkable and even striking observation that news on blockchain, in general, is tilting more and more towards highlights and press releases from companies and start-ups that communicate on DLT applications in their businesses.

The number of projects being reported is increasing almost exponentially. There are so many, across a range of industry sectors, that it becomes impossible to track even the most prominent. Back in 2017, or even mid-2018, in this Blockchain Quarterly report, we could be confident of presenting all of the initiatives that were worth mentioning. Today, this is no longer achievable: hence, we highlight the most significant and can only give a general description of the development atmosphere. As of the second half of 2019, it is intense, particularly in the field of traceability, and interbank settlements. Nowadays, the quantity of updates and new initiatives is enormous, which makes it essential to choose a few to present at the expense of others, let alone those that aren't advertised. Hence, we are tempted to gear towards a general sum-up of the situations, sector by sector.

Technological applications in the various sectors (and banking is not specified in this respect) are continuously promoted, their authors thinking their achievements are worth being proud of, and this

has taken the media space from cryptocurrencies and above all from Bitcoin.

However, concerns have been raised about the fast obsolescence of early-developed solutions. Gartner, a research and advisory firm, is particularly concerned about this: it claims that a vast majority of enterprise projects will be abandoned for just this reason.

Another claim that is voiced by individuals involved in building infrastructures is that blockchain will shortly be everywhere, but invisible, as a foundational layer, as a protocol that runs and is relied upon by applications that will interface with it.

As a final comment, several "common" DLT projects are being reported, that is, there are fewer and fewer genuinely new ideas being presented, and more and more competitive use cases.

5 TRENDS BY CRYPTO-ASSET CLASS

CLASSIFICATION

As BQ Intel develops, we engage in providing tools to compare crypto assets, thanks to the creation of a database and a suite of tools to exploit it. A significant added value is 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 finance departments of how to enter crypto assets in the books. Accounting standards have not yet thoroughly considered and published principles for this so that companies can be guided as to which accounting category to put Ether, Bitcoin, Tokenized gold, etc., not to mention proceeds from mining, receipts proceeding from activities such as speculative acquisition, or whatever. Here again, the mapping of the five categories could prove very interesting for accounting researchers to work with.

A – ANONYMITY CHARACTERISTIC

Anonymity coins are increasingly being scrutinized by regulators, as we were expecting, so, not much to report here.

I INFRASTRUCTURE NATIVE CRYPTO-ASSETS

I(Ē) – Pure accounting infrastructure functionality

Bitcoin

Bitcoin is regaining its dominance in the cryptosphere, against every other cryptocurrency. Its dominance had increased by up to 70%, which has not been seen since the spring of 2017, when the ICO explosion started. This is a sign of investors reckoning that BTC is still, as of today, the flagship blockchain, most renowned, most secure, and hence the safest short-term store of value.

In this sense, BTC benefits both from the recognition of blockchain technology throughout the industry, as well as investor doubts and disappointments regarding ICOed tokens and the lengthy development in the execution environments, including Ethereum.

Otherwise, one quote that we liked in an attempt to defend BTC as a protected instrument: "Bitcoin is code, code is speech, and speech is protected"!

Deflationary cryptocurrencies

A "trendy" kind of pure cryptocurrencies has been flourishing in recent weeks, with a lot of similar projects being born: deflationary-by-design coins. Examples: Mero-currency; Boom; Bomb; Ethplode; Hype-token; Golden-token. Just by the names, you can see these are a bit dodgy.

The principle is always more or less the same: upon transfer of a coin, a fraction of it is burnt, destroyed. This can be typically 0,001%, 0,1%, etc., and is quite a simple smart-contracted feature on the Ethereum platform.

Some projects are openly describing themselves as an experiment – and yes, to an extent, it is interesting to study the evolution of the price of a value transfer and storage medium when the supply decreases as a function of its use. But then, it seems that several developers have decided to ride the wave and describe this mechanism as a revolutionary one with the magic property to make the value of the coin rise just by doing nothing, while other users erode the value of the coin when using it.

Not sure if we want to comment on the scammy nature of such an economic expectation, all the more that monetary erosion is already very present in, say, Bitcoin: but as far as we are concerned, we expect these coins to collapse ultimately. The only good thing is that people obviously will start thinking of how the monetary mass should be managed, and at the end of the day, that means challenging the central banks on that.

(I)E – Execution environments platforms

What comes to mind when invited to comment on these platforms is that improvements appear to be a long way in coming. It has now been two years that Cardano's researches have been carried extensively, and the network is still not there. This is an endless expectation for PoS and sharding on Ethereum, and everyone is anxiously awaiting the end of this year to see if anything concrete will be delivered. Please refer to the technical section for the relative updates.











F – FINANCING FUNCTIONALITY FAMILY

"Utility tokens" 2017-style ICOs












The increase in the value of cryptocurrencies, and the first rank, Bitcoin, the interest in riskier investment vehicles (ICOs) is resuming as well. The number of ICO projects registered on ICOBench has risen significantly in the first half of 2019 (Figure 14).

But this should not obfuscate the fact that the net amount of funding raised by ICO projects is down an astonishing 97% year-on-year (Q1 2019 vs. Q1 2018, source BitMex). The money raised thanks to ICOs in the first half of 2019 has been in the range of €300M (Figure 13), which

HIGH-RESOLUTION IMAGE OF THE TABLE: bqintel.com/dlt-infrastructure-compare

PLATFORM NAME	COMMENTS	CONSENSUS MODE	CONTROL ON PARTICIPATING NODES	MARKET SIZE, \$B	FUNDS RAIZED, \$M	DATA CONFIDENTIALITY	TRANSACTIONS/ SECOND PER SHARD	APPROACH TO "SCALING TO INFINITE"	VALIDATION TIME	SUPPORT OF SMARTCONTRACTING	COST OF EXECUTION	MATURITY OF THE PLATFORM	CURRENCIES AVAILABLE ON-CHAIN	DEVELOPMENT TEAM ROBUSTNESS	DEVELOPMENT ECOSYSTEM
 ETHEREUM (pre-PoS upgrade)		PoW	Public distributed ledger	30.8	18	Not easy - to be engineered specifically	1 x	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	5.3	100	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
 LIBRA		PoS	Permissioned, governed by corporations	N/A	N/A	Transparent	1000	Not envisioned	1 s	Built-in, Turing complete	Zero; consortium rewarded by interest on collateral	Yet to be deployed	Libra native	Nascent	Nascent
 TRON	Focus on "dWeb"; based on Ethereum logic, with 27 elected nodes every 6h	dPos	Pseudo-centralized; inconvenients from both world	2.2	70	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)
 CARDANO		PoS	Permissioning is possible	2.0	62	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	2.0	3	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	1.2	100	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	1.1	N/A	Not easy - to be engineered specifically	1000x	In DAG structure, more participants, higher security and throughput	<1 s	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	Permissioning is possible	1.0	17	Not easy - to be engineered specifically	100x	Specific architecture of sharding	<1 s	Not supported natively	n/a	Maturing	To be introduced by ad hoc bank; no technical problem	Decent	A number of real projects use it
 TEZOS	Focus on on-chain governance	LPoS	Public distributed ledger	0.8	232	Some expressed plans to implement recursive SNARK	1,000	Recursive 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

 BEST AMONG PEERS
  WORST AMONG PEERS

PLATFORM NAME	COMMENTS	CONSENSUS MODE	CONTROL ON PARTICIPATING NODES	MARKET SIZE, \$B	FUNDS RAIZED, \$M	DATA CONFIDENTIALITY	TRANSACTIONS/ SECOND PER SHARD	APPROACH TO "SCALING TO INFINITE"	VALIDATION TIME	SUPPORT OF SMART CONTRACTING	COST OF EXECUTION	MATURITY OF THE PLATFORM	CURRENCIES AVAILABLE ON-CHAIN	DEVELOPMENT TEAM ROBUSTNESS	DEVELOPMENT ECOSYSTEM
 QTUM	Implementation of a VM based on BTC's like UTxO logic	PoS	Public distributed ledger	0.5	17	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
 VECHAIN	Thought from the beginning for traceability and supply chain	In between Proof of Authority and Proof of Stake	Public distributed ledger	0.4	N/A	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
 NANO (ex-RaiBlocks)	Direct Acyclic Graph	Vote of "representative" nodes on gossips of gossips	Public distributed ledger	0.2	N/A	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	0.1	1	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
 CONCORDIUM		Proof of Stake (with some refining on incentivization)	Permissioned	N/A	N/A	Yes, promise	100x	Unknown, probably sharding	Promise to be fast	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 private	N/A	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	167	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)		PoS	Public distributed ledger	N/A	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
 HASHGRAPH	Direct Acyclic Graph	Gossip of gossip + "Virtual voting", -> Asynchronous Byzantine Fault Tolerance	Only tested in permissioned environments so far	N/A	118	Not easy - to be engineered specifically	500000	In DAG structure, more participants, higher security and throughput	n/a	Probably under development; probably a challenge to make it supported	n/a	Still not launched	To be introduced by ad-hoc bank; no tech. problem once smartcontracting	Decent	Modest
 HYPERLEDGER FABRIC		Permissioned voting-based consensus	Permissioned	N/A	N/A	In principle yes; may hinder the functionalities	1000x	Unknown	<10s	A priori yes, but no actual obvious example implemented	Free in principle; cost of running nodes	Available	Not architected to propose it; all projects separated	IBM & Linux foundation	IBM (with pros and cons)
 QUORUM	Banking-oriented; JP-Morgan complexification of Ethereum	Ethereum's PoW on validating hashes of messages passed in private	Public network to pass and record informations; private data via another channel	N/A	N/A	Yes	1x	Sharding, probably like Ethereum	10s	Built-in, Turing-complete	Gas principle	Available	Finance oriented, assets a priori on-chain	Able to implement Ethereum's developments	Ethereum's

 BEST AMONG PEERS
  WORST AMONG PEERS

is less than one-tenth of the amount raised in the first half of 2018. Furthermore, one characteristic of the 2019 ICO market is that it is dominated by a few projects raising tens of millions, with all the rest being practically failures. All in all, the classical, hype-averse VC approach is taking over again (Figure 15).

So, it is interesting to share some insights gained by our daily monitoring of new crypto assets being listed on CoinMarketCap.com. Typically, there are three or four new entries added every day on the site (except on weekends), and one or two are delisted – which does not prevent some bigger batches from being added or removed from time to time.

Out of, say, an average of 20 new coins that appear over the course of a week:

- Almost all are ICOs, that is, they have been issued with a clear financing purpose. There would be no more than one or two native DLT platforms released per week.

- Only 20% can be considered as serious projects. That is one every second day; still not too bad, the sign of vibrant activity worldwide – as no geography can be said to be over or under-represented, pretty much following the intensity of activities reported in the geographical round paragraph (see further).

- But the problem is that consequently, 80% of new crypto assets listed on CoinMarketCap.com qualify as weak projects, or worse. They display poor material on their websites (we are referring to grammar errors in the headlines), the business case or use case is poorly articulated if at all

FIGURE 13:
CUMULATIVE ICO FUNDING, \$MM

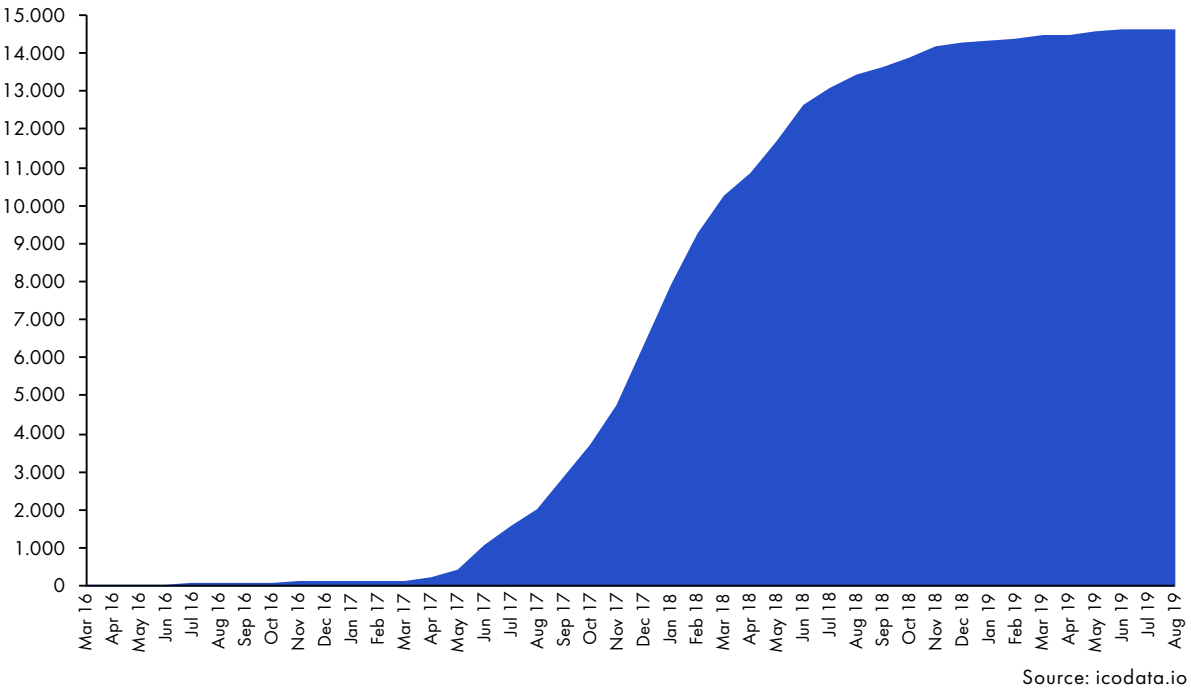
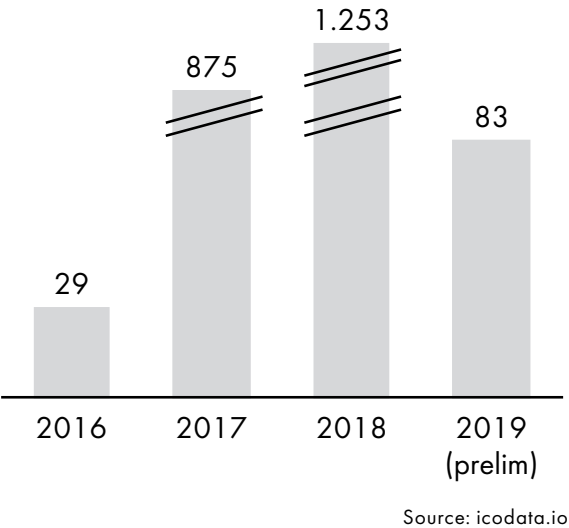


FIGURE 14:
NUMBER OF ICO BY YEAR



understandable, casting doubt on whether the teams behind these projects understand in what they are driving.

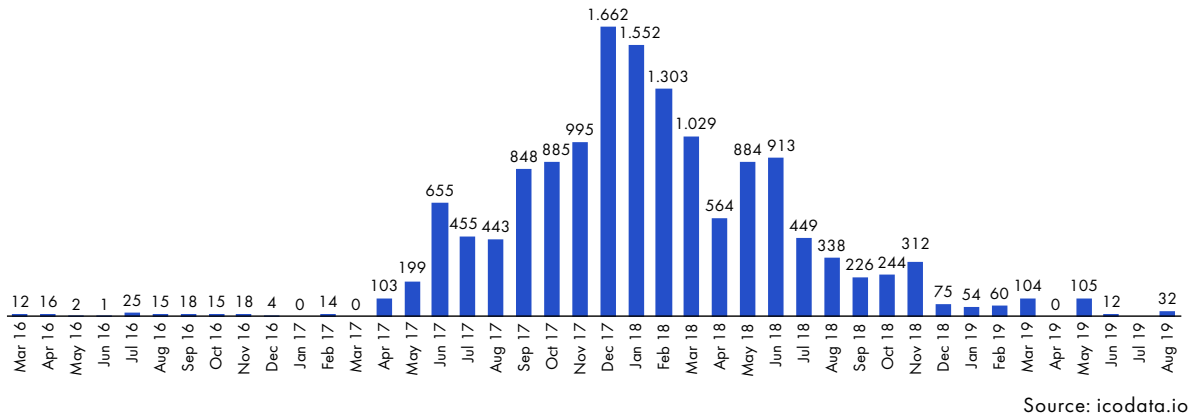
- More worrisome, apart from naïve teams and light-weight websites, some crypto assets among the discarded 80% look like scams. It is difficult to

accurately identify which projects were conceived purely to raise capital with no intention to do anything compared to genuinely weak companies. While in both cases token holders will lose all their money, the fact that the 2017-type scams have not been cleaned from the landscape is quite a concern and makes it difficult to defend the ICO model, which otherwise would be very innovative. Either the ecosystem manages to clean some mess on its own, or no doubt official regulators will “propose” to step in, under the guise of protecting investors!

Securities tokens offerings
An excellent question to ask is, will we end up managing tokenized securities or instead security tokens? The difference is interesting.

The former presupposes that the security titles pre-exist somewhere, typically in the legacy system, and a company takes on the task of being the custodian and issues it in the blockchain world, a token that it declares to be the title of ownership of the security (share, bond, etc.). However, for the latter, this means that the token is the security itself and that a whole new process is needed to support its compliance with the legal requirements of issuing such financial instruments, which is then proposed to investors.

FIGURE 15:
ICO FUNDRAISING BY MONTH, \$MM



It looks “easier” to some extent to immediately go the tokenized security way, harvesting some of the benefits of asset management automation. But let’s make no mistake, it is the security tokens that constitute the real change for the financial world. Automation of agreed cash flows (coupons, dividends) can be fully leveraged only with tokens standing alone as the financial title, and cutting the link to the legacy systems will significantly ease the operational burden associated with trading and custody of securities.

Initial Exchange Offering (IEO)

Using an exchange-facilitated initial token offering is currently among the most significant phenomena, not to mention among the hottest topics. With the ICO hype still down from its golden days, changing the “C” to an “E” is part of the move. In our view, this phenomenon is legitimate because it revolves around nothing less than transforming securities exchanges and asset management.

What is happening is that crypto exchanges are moving into the field of proposing the tokens of some projects/companies. As one would expect, serious exchanges (e.g., Binance’s Launchpad) carefully assess and then select the projects that they intend to support because their reputation is at stake – but of course, not all platforms are equally conscientious. This “initial listing” is a business of its own; exchanges are making money from it.

For start-ups, an IEO is an efficient substitute for an ICO or STO because much of the hassle is taken care of: in particular, all of the KYC requirements, the smart-contract deployment, and of course, the power of the exchange’s marketing. Taking charge of customer checks is by no means the least of the advantages for issuers, and is likely to remain a running one...

Following the Binance example, which launched as early as the second half of 2017, other platforms are now quickly making up for their delay: KuCoin, OKEx, Huobi, and Bittrex are putting in much effort, proposing to conduct their IEOs.

The power of these exchanges explains why IEOs are raising more than 10 times the amount raised by ICOs in early 2019.

The only question is the legitimacy of the exchanges to choose the projects that they are going to support. Today, stock exchanges operate, in a way, as companies that have benefited from privatization by offering securities exchange services. Tomorrow, we picture a situation where private companies, potentially even decentralized, will judge, using their private criteria, which start-up companies are good enough to propose for fundraising, and which are not. That raises other questions, we shall see.

O – OWNERSHIP REPRESENTATION

Financial securities

The €100M bond issue by the Société Générale on Ethereum is quite remarkable, not so much because of the outreach, but because it has been done on a public blockchain. This is an exciting decision from a financial institution, as they have always claimed, one louder than the other, that non-permissioned blockchains were unsuitable for their usage! Here, it seems that the bank wants to explore what happens when managing tokenized assets that have precisely the same legal rights embedded in them, on a public blockchain. It looks very much like an attempt to see what additional advantages are to be gained by making these otherwise very regulated assets available “in the wild”, as opposed to controlling them in a permissioned environment. It is, in effect, the recognition that the real power of blockchain is to allow for far more comprehensive outreach. The question of how they are resolving the beloved KYC requirement, in this context, remains to be seen, though.

Please also refer to the “STO” section.

Real estate

There is no shortage of articles and development related to the tokenization of real estate, including the financing of mortgage rehabilitation, rent smart-contracting, etc. So, not much is new regarding the tokenization principle we highlighted previously

(and it is conceptually pretty simple); quite a lot of ‘proptech’ is being launched in this field.

Otherwise, there is an interesting view regarding the impact of the tokenization of real estate on poverty. That is, if assets owned in currently failed or fragile economies can be tracked more effectively, then these could be used as collateral to obtain loans. Thereby, it can unlock the so-called “dead capital” in these areas. Interestingly enough, that would mean that the tokenization of assets has far more potential for societal change in unfavored areas than it will have in affluent places.

Commodities, including precious metals

Not much is going on here, which is surprising to us. Price of gold, and other precious metals, is going up, so this should be favorable, but we have not seen any traction, no take-off of companies that are proposing to tokenize, then redeem precious metals (Figure 16, 17 and 18). The Digix Gold Token exchange volume, for instance, is very low, and

there has not even been an increase in the amount of tokenized gold. Disappointing.

Otherwise, an impressive influence of blockchain on the commodities markets is that things that were considered previously as fungible material are starting to be traced, depending on their origin; not necessarily for the quality, purity or physical characteristics (although marginally, this as well), but rather for the control of ethics across the supply chain. Hence commodities end up not being just metal but also metals that were produced acceptably, therefore they become non-fungible.

Going further, oil has always been non-fungible due to its chemical properties, but now electrical energy can also be traced, and its price might depend not only on the delivery time but also on its origin (solar, wind, hydro, coal, nuclear).

Loyalty program points

Here, the frontier between privately issued money

FIGURE 16:

GOLD VS BTC PRICE



Source: businessinsider

FIGURE 17:

DAILY PERCENT CHANGE IN THE PRICE OF BTC

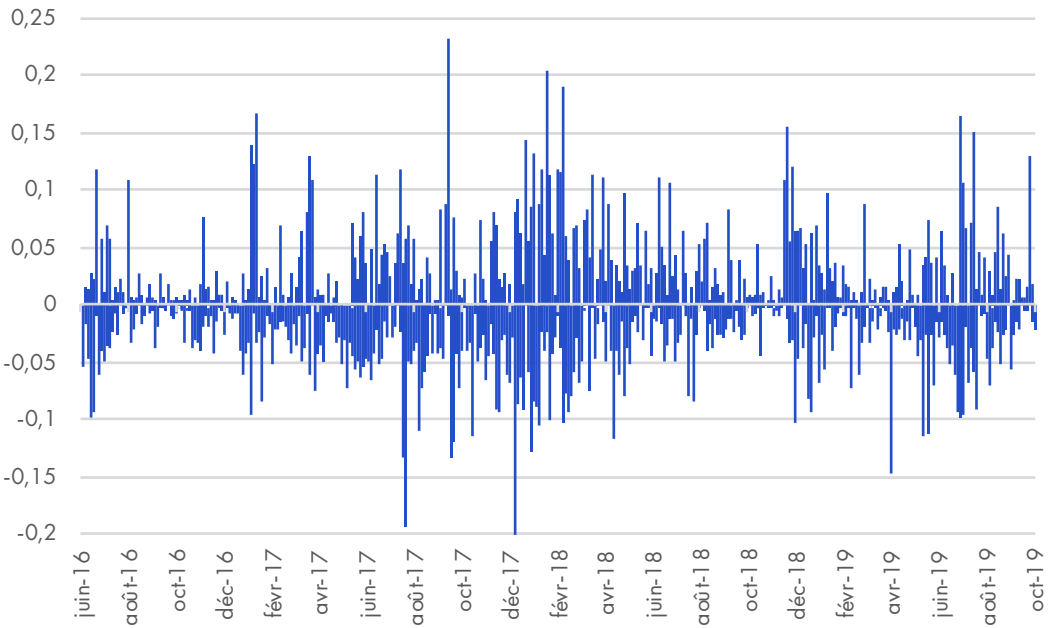
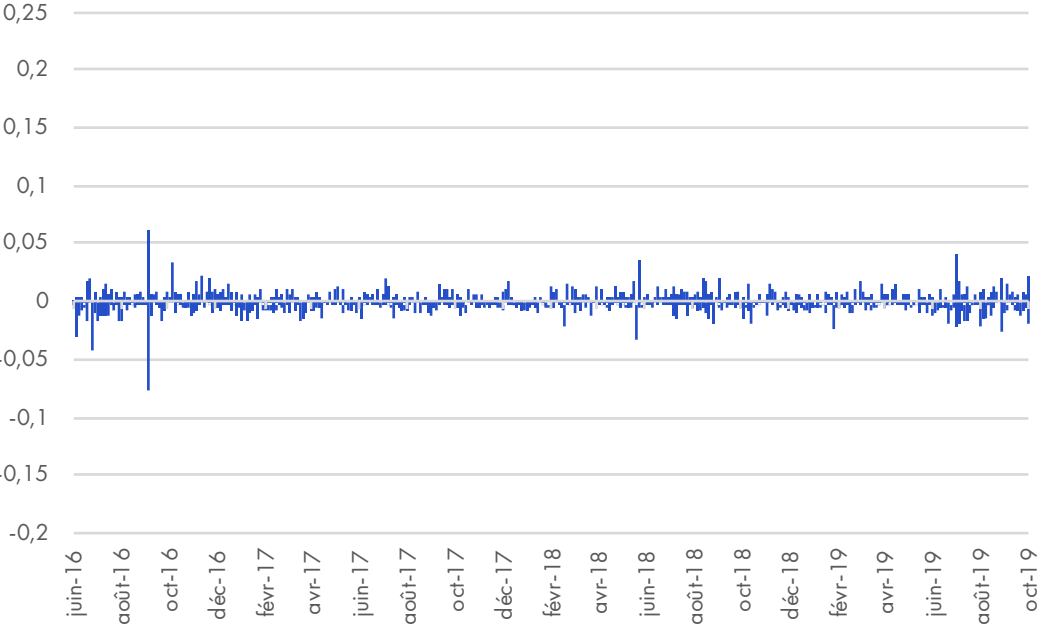


FIGURE 18:

DAILY PERCENT CHANGE IN THE PRICE OF GOLD



and coupons is becoming quite blurred. 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 making it challenging to separate functionalities.

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

Similar to real estate, the concept has not changed much, but the tokenization of collectible art is making its way in the minds of the market actors.

P – PAYMENT FUNCTIONALITY

Acceptance in retail

A significant challenge remains: For cryptocurrencies to get serious traction, the public needs to know which retailers and in which circumstances they can reliably use cryptos as direct payment for a service or product.

Indicators show that the rhythm of merchants taking the step to accept cryptocurrencies is increasing (almost tenfold year on year for Bitcoin Cash, according to a source). The reason quoted by merchants is the near-zero fee involved, contrary to the fees charged by Visa and Mastercard (that the customer does not see). The real obstacle to broader and faster acceptance is volatility. Also, retailers have a fundamental incentive to participate: if consumers want to pay in cryptocurrencies, retailers want to find a way to accept the value offered.

Let us gather some significant examples of Bitcoin and other cryptocurrency acceptance:

- In Japan, it is not uncommon to see shops displaying a sign, “Bitcoin accepted here”, and often next to another sign stating acceptance of Ether.

- Since April 2019, the Grand Dolder, a 5-star hotel close to Zürich, has been accepting Bitcoin – a high-end luxury establishment making a move to attract crypto-rich people. We believe this is pretty interesting to witness, as it shows that there

is a dedicated segmentation being put in place to serve this segment of customers! This is by no means insignificant, in our view, and is in line with real estate development in Dubai aimed at Bitcoin holders, which we reported some time ago.

- A pizza deliverer in Rio, a hairdresser in the UK, a bar in Québec, a telco in the US, a pub in KL, a restaurant in NY, a laundry in Romania, etc. are random examples of commerce embracing cryptocurrencies – probably as a differentiator, but often also as militant declaration, one would bet.

Libra

Now is finally the time to dive into this specific case. The publication of the Libra whitepaper is arguably the single most crucial piece of news of this quarter. It is an essential event in many senses, so let us discuss each in detail.

Media coverage and impact

First, one can observe that since its disclosure, the Libra project has attracted much attention from the crypto sphere, as well as from the mainstream media. Many facts indicate that observers in the cryptosphere are all acknowledging the importance of the move:

- The truth is that the price of Bitcoin surged tremendously right after the Libra whitepaper was released. So much is happening with Bitcoin that it is sometimes hard to find reasons for the price movements, but here, the correlation looks pretty evident.

- During June’s Crypto Valley Conference, no single speech could finish without a person in the audience asking a question about the impact of Libra on the topic.

- The number of articles published in Libra far exceeds any other blockchain topic. The space that we are allocating to Libra in this Quarterly serves to demonstrate further the conceptual outreach of their whitepaper. This buzz, in itself, indicates that something special is going on.

LIBRA IS AN INITIATIVE
THAT HAS NO
PRECEDENT, WHICH
IMPLIES POTENTIALLY
SIGNIFICANT CHANGES
TO THE WORLD'S
FINANCIAL SYSTEM

- Politics stepped in very fast, and Zuckerberg got a letter from the US Congress asking him to put the project on hold until it could be properly debated in the public arena.

So, is all this buzz justified? In our view, yes. As we will see in the following paragraphs, Libra is an initiative that has no precedent, which implies potentially significant changes to the world's financial system, in terms of macroeconomics, the role of central banks, and even states. In short, it theoretically extends well beyond just Facebook to many other fields.

Nature of the Libra

So, let's get to it. Fundamentally, what is the Libra token intended to be? Let's review this by characteristics, which will be a helpful test of our classification framework.

1. Ownership representation function - the intended nature of Libra is a stabilized representation of value, suitable for payment and a store of wealth. In this sense, it is trying to address a need that neither native blockchain units of account (especially BTC) nor proposed tokenized fiat has been suitable for, up to now.

The way to achieve this is to proclaim that each unit of Libra will be backed by an elementary unit of a basket of widely recognized and utilized exchange and value storage media, namely a subset of central bank fiat. We can expect that this basket will be designed to include weighted proportions of USD (mainly), EUR, JPY, etc.

So, a holder of a Libra will be entitled to approach the Libra Association and ask for the redemption of some fiat money in exchange for the token. The Libra Association is hence, a "buyer of last resort" [as opposed to a central bank is a "lender of last

resort"].

As a result, Libra will be fully collateralized; so, obtaining, spending and handling Libra will be homogeneous to receiving, spending, managing a type of note that is a mix of major central bank-issued fiat. Its value will evolve linearly with the combined relative value of the underlying fiat assets – and one interesting point to make immediately is that this mixing is likely to make the Libra more stable than any of the individual fiat currencies it is backed by.

How the basket of backing assets will evolve in the future is unknown at this stage, but it is highly likely that, at some point in time, other valuables could be included, such as precious metals, commodities, stocks, real estate, Bitcoin, etc., in an effort to diversify or even distinguish the currency completely from central bank fiat.

2. Infrastructure function - one year ahead of the forecast Libra launch date (projected to be in the first half of 2020), it is unclear, technically, how the Libra is going to be minted and burnt by the Association. But, as this is going to be a permissioned DLT (and by all means, not a typical blockchain), apparently, the computation effort is going to be supported by a limited number of nodes, with an operational cost that should be (at least in the beginning) negligible, compared to the financial gains on the management of the collateral. Therefore, we may (at least functionally) consider the Libra as the native, if not a primary, unit of account within their DLT ecosystem.

Importantly, Libra plans to provide an execution environment, that is, allow for programmable money in the sense of Ethereum. While this potentially raises a technical issue in terms of throughput rate, if the system reaches mainstream adoption, this choice makes much sense from a business perspective. Hence, Libra is being developed to have a significant potential to impact business models immediately and is positioned to be in direct competition with Ethereum, with its philosophy. The language to be used to code Libra automated transfer will be "Move", supposedly easier than Solidity.

3. Payment function - the clear intent of the Libra initiative is to provide a stable international digital currency to billions of global citizens. The peg to fiat currencies qualifies it immediately as a medium of exchange and a mid-term store of value for individuals – as well as companies.

In the whitepaper, the authors focus heavily on the quite humanitarian goal to "bank the unbanked" – and indeed, as soon as you enable especially poor individuals to own and handle their assets directly through their mobile wallet, you are then allowing them to participate in this new financial system. So objectively, why not? And if one does not agree with this approach, then we can ask, why have governments not yet solved this problem? Well, not so fast. The main reason why some people are excluded from the financial system (in addition to being poor, and not profitable enough to serve) is that they are not in a situation to comply with a lot of checks and controls, that have to do, mostly, with identity management and trustworthiness.

We will touch on that a bit later when we look at the regulatory perspective. But irrespective, that does not change the fact that the use case for payment and value storage is evident, especially within the Facebook social networks and all the various part-takers in many industries (Uber, Spotify, Iliad, Napster, etc.).

To conclude on the nature of Libra: in our analysis framework, Libra is [Infrastructure – Execution environment] [Ownership] [Payment] [non Anonymous] [non Financing].

Of course, this is different from Bitcoin, which is mostly non-ownership. Being a property title is certainly neither good nor bad, in itself, for a cryptocurrency: they are just a different class of tokens, each with their use case, reasons for being, and enthusiasts. They shall exist along with ones from the others.

Long story short, with the Libra, we are dealing with a new kind of animal, one that fills a category that was, until now, empty in our Mendelev-like

approach to tokens zoology classification. [For recall, the classification of the chemical elements of Dmitri Mendelev had empty slots that eventually got discovered later on.]

In other words, such a tokenized mixed-fiat tool is unlikely to be the "Bitcoin killer", despite what has been written in some articles, because of the significant differences in their nature: a US dollar will always be a US dollar. When packaged with other currencies in Libra, there will be an additional uncertainty of this foundation intermediary, but that is all, whereas Bitcoin, for instance, remains not backed and specific in its positioning, or a TenX token is homogeneous to a part of profit sharing.

Governance and decentralization

Facebook is very much THE entity that originated the Libra initiative, but they have been intelligent enough, this time, to realize it would have been a bad idea to be the only protagonist. So they decided to partner with other large companies to make it happen. As a consequence, Libra is de facto, objectively, separate from Facebook, which is going to be just one among many entities involved in its management.

In principle, this is not bad; in practice, we shall see, but in principle, the claimed intent is to make Libra a distributed structure.

But these governance aspects raise quite a few concerns, which are especially sensitive because the payment data in Libra is going to be valuable information available to the operators of the network, and we can safely estimate it will have tremendous value. Facebook and the other participants claim that they are going to prohibit themselves from matching Libra's blockchain with their databases. Whether or not they will resist this in the medium term, especially given Facebook's track record in exploiting users' data, is left to the reader's assessment. But this is pretty much the reason why Facebook decided not to try to do it all on their own – and some criticize the seriousness of the other Association members, whose involvement, they believe, is intended purely to make Facebook

look less predominant.

Formally, the non-profit association, based in Geneva, Switzerland, is going to be managing the system.

Also, to be precise, the Libra ecosystem is not just the Libra; it is a dual coin ecosystem – something quite typical of any stable coin. The other “token” is about sharing the decision-making power among the network’s participating companies and sharing the benefits derived from the immobilized financial assets that form Libra’s collateral. And this is a critical point that has not received much exposure in the various articles on the topic: if Libra gets traction, then the amount of fiat money, which is the assets side of the balance sheet of the Association, may become quite significant. In turn, the corporate participants that have paid cash to participate in Libra are likely to expect a return for their financial participation in creating this adventure. Instead of placing dollars, euros, and yen in a vault, the money is expected to be deposited in a classic bank account and be remunerated for that. It is unclear if the initial participants will benefit from the compounding effect, but most probably, they intend to. So, Facebook and its counterparts are likely planning to make substantial profits from this scheme, which is somewhat distant from the claimed philanthropic goal to bank the unbanked... They are taking care of their interests and those of their shareholders, but if we blame them for that, then there are a lot of similar things to blame in this capitalist world!

Technically speaking, the consensus mode is Proof of Stake among the consortium participants. The whitepaper claims that the ultimate goal is to pass from distributed to decentralized. However, no concrete path is elucidated to achieve this. No doubt, the move will not be smooth, if at all ultimately desirable for its creators, if Libra gains momentum.

Impact on the financial sector (banks)

In recent decades, the banking business has increasingly evolved into a job of managing books

– databases of assets and liabilities. Therefore, financial institutions have been under constant fear that GAFA, especially Google, might diversify into the banking sector.

With reason. Libra is expected to be a system that will compete with current payment facilities, which until now has been facilitated pretty much exclusively by banks. Importantly, the custody of assets will be managed by customers themselves, which has advantages and drawbacks. Among the benefits are the removal of intermediaries and associated fees, while among the drawbacks is the question of the security of assets, i.e., the management of private keys.

Anyway, with Libra, clearly, the management of payments will be facilitated by a blockchain. The banking ecosystem, which has not been able to transition to a fast and easy payment system, meanwhile is going to be under tremendous stress; and by the way, if it was not Libra, we could bet that another DLT-based initiative would have taken on the job!

Importantly, neither Facebook nor the Libra Association – nor anyone else in the Libra system – is willing (yet) to play the role of a bank, in the sense of creating money on accounting books each time a debt is recorded.

Another concern is that it is unclear what impact Libra will have on the dynamics of money circulation; at least in the short term, there will not be any lending, in Libra terms, which could lead to suggestions that the collateral fiat money immobilized by the Libra Association, will not be used to repay debts, and hence would be more like central bank money, leading central banks to take it into account when elaborating their policies...

Regulatory perspective

Libra is going to raise concerns around KYC/AML/CFT. The platform will have to be completely compliant with imposed regulations. In turn, this means that what will be going on, mainly regarding the origin of funds, will be controlled and scrutinized

by systems constructed by the Libra Association, then passed on to official bodies upon request.

And here immediately, we bump into a much-criticized three-line paragraph in the whitepaper. It mentions that the Libra Association plans to engineer a form of digital identity management on the DLT to comply, if not with all regulations in all jurisdictions, at least to be able to argue that KYC/AML/CFT are well taken care of. As large corporations manage it, as opposed to a completely decentralized no-head network like pure cryptocurrencies, for Libra, there is just no question that they will have to accommodate the relevant laws to avoid being banned.

So, how will access to the Libra ecosystem be given to an unbanked individual with no (or dodgy) ID and no (or no registered) home, even if they have a smartphone? This remains to be seen, despite maybe the best intentions in the world.

This also means, of course, that Libra is taking the opposite position to Satoshi Nakamoto’s vision of providing a means for populations to escape the control of governments and large corporations. This is also the crux of most of the criticism that has been directed at Libra from crypto communities. Let’s be factual: Libra is not Bitcoin; they are not in the same class, and there is appetite out there for both kinds of approaches. People are free to reject Libra if they wish, only effective adoption or not will tell in one sense or another.

Macroeconomics and regulations

This Libra initiative could have a significant potential impact on nothing less than the world’s monetary system. Depending on the traction it gets, it could become de facto the single most important thing since the Bretton Woods agreement.

If Libra succeeds, even with just a modest mass adoption, which is a likelihood given the amazingly broad user base of cutting-edge web companies taking part in the Association, then what are the impacts? Well, you could have a single non-profit

organization managed by for-profit companies that would be in charge of running a great, if not the greatest, payment and remittance system on the planet. The money used in that system would not depend on any single state-issued currency – slightly, it would rely partially on all of them, simultaneously. It would be entitled to decide which “national currencies” (whatever the meaning becomes) are good enough to be included in the basket, and in which proportion. This looks like an exciting challenge for everything that we are familiar with, for all that we know, in terms of the monetary system. Does it not?

Dear reader, make no mistake: when officials in the US, Singapore, France, etc. are formulating questions for Libra’s consortium members, or even expressing explicitly that no such system should be allowed to compete with national currencies, this means that governments already see this as a severe problem. What is at stake here is nothing less than the sovereignty of countries. This is especially true for the USD, the dominant sovereign currency on the planet, but it is not much less of a concern for other states.

If citizens have the convenience of holding their earnings or savings in Libras, Argentinian pesos, or Venezuelan bolivars, then their choice won’t be currencies issued by failed states.

Let’s consider a medium-size country, say Malaysia, Chile, or the Czech Republic. Today, such a country routinely decides and enforces its own monetary and domestic tax policies. However, it does not have sufficient power to impose its views globally. If Libra is adopted in even a small number of countries, then maybe an increasing number of citizens within these countries will start relying on it. And then a not-so-minor proportion of merchants may start accepting it, in competition with a de facto, less stable and secure national currency. How would

GOVERNMENTS
ALREADY SEE THIS AS
A SEVERE PROBLEM.
WHAT IS AT STAKE HERE
IS NOTHING LESS THAN
THE SOVEREIGNTY OF
COUNTRIES

the governments of these countries react? Will they impose a ban on the Libra (and then logically, other cryptocurrencies)? How would they enforce the ban when there is no practical way to control it, in what will then be a black market? Will they abort their national currency and just let it decline, thereby abdicating their monetary policy to a handful of major nations?

Then, even more bizarre: in reality, some competition would exist among the currencies of major nations to gain more influence, as their portion of the Libra basket... Without a doubt, nations that currently issue the dominant currencies are unlikely to relinquish the power they have to repay their debt with money they can devalue as they please. Is it desirable that the distorted behavior of these powerful states comes to an end? Then, as the Libra will be based on a basket of fiat currencies, to some degree, it will be subject to the decisions of central bankers. Would this cause central bankers to adopt globally coordinated monetary policies? And/or, ultimately, would Libra diversify its collateral to gold, stocks, real estate, etc., as the credibility and actual value of fiat become undermined? One day, even Bitcoin may become part of the basket!

OK, let's not even attempt to answer all of that. But the crucial point is that today all these questions are on the desks of ministers of the 200 plus states on earth. If you think about it, that is the actual impact of the Libra. Even Bitcoin has not shaken the system in such a profound way. The least we can say is that the near future is going to be extremely interesting.

Conclusion

Irrespective of our opinion of Facebook, we have to recognize that this is a critical innovation, a move that cannot be ignored by central bankers or, indeed, any corporation that has been considering including cryptocurrency payment in its business model.

Interestingly, it looks like only a large corporation could come up with a Libra-like proposal. Only the sheer size of the conjunction of participants is conferring to Libra its outreach. No decentralized

initiative is even close to triggering so many questions and trouble for central bankers today. So, Libra is Libra precisely because it is Facebook and companies that are behind and engaging in it.

There is not so much technical innovation in the Libra, but the business and potential macroeconomic impacts are dominant, and no doubt they will have central bankers and governments thinking a lot in the next few months. Meanwhile, the greatest beneficiary will be Bitcoin! Introducing many users to cryptocurrency via a mainstream application like Libra will immediately benefit existing cryptocurrencies thanks to enhanced public exposure and apparent endorsement of blockchain by major corporations ("People may not like Zuckerberg, but no one thinks he's dumb" as Pompliano puts it.).

6 LATEST ADVANCEMENTS IN DLT TECHNOLOGIES

As usual, but especially in this section on technical updates, it is assumed that the reader is up to speed with studies covered in previous reports. Past Blockchain Quarterly issues are available upon request.

INVESTMENT IN DLT TECHNOLOGIES

Investment in technology has now dwindled compared to the money being directed to application ventures. As more or less specialized investment funds continue to pour millions of their investors into crypto-related endeavors, we observe that most are dealing with building businesses on top of platforms. A few native projects have been funded (e.g., Dfinity), but most of the technological research is currently being carried out thanks to the funding collected in 2016-2017.

CONSENSUS MODE – AND GOVERNANCE

[The consensus method on DLTs largely determines the scalability of the infrastructure, and in general scalability, features need to be governed carefully. Therefore, we discuss these topics mostly within the section on scalability.]

Technical developments on consensus modes

There is no shortage of progress on the proposal of alternative blockchains competing with Ethereum, EOS, Cardano, and others. Here are a few, and their broad terms:

- **Kadena:** This interesting attempt was proposed by a team of former JP Morgan and SEC employees to “use Proof of Work in a scalable way”. We are referring here to a permissioned blockchain, Kadena (cadena means “chain” in Spanish) and its public implementation, Chainweb. The proposed trick is to use a Bitcoin-like Proof of Work mechanism, that is applied to several sidechains that refer to each other’s block headers, so that they do not diverge, and where the side-chains can communicate with each other. Miners try to mine on all chains simultaneously, and as the difficulty index is lower for each independent chain, the throughput rate increases.
- **Dexon:** This is a specific implementation of dPoS, hence promising fast finality, low transaction fees, and high throughput with a governance council claiming no compromise on decentralization. They have highly ambitious intentions and are in frontal competition with Ethereum and others. They have also defined their language for smart-contracts, DexLang.
- **Avalanche:** The claim is to reach finality in less than two seconds, for up to 10,000 tps. The protocol is leaderless Byzantine fault-tolerant, inspired by epidemic protocols and gossip networks added to the

lessons learned from the classical PoW consensus mechanism of Satoshi Nakamoto. The concept relies a lot on metastability, that is, the system will converge towards a state, as opposed to being balanced.

In the challenge to transition from PoW to PoS (as Ethereum is trying to), one issue is to obtain true randomness for the base in several steps, especially the selection of validation nodes. If the system relies on pseudo-randomness only, it opens the door for an attacker to retro-engineer it and be able to foresee the future seeds and identify when one will be chosen to validate a block. Even if some reasonably-complicated algorithms are devised to make it, in principle, out of reach, research continues to improve the situation.

Governance

It’s always Tezos that focuses attention on the deployment of on-chain governance: they continue to roll out and test their infrastructure live, already with some feed-back analysis on the first on-chain vote implementation that occurred in June. Tezos developers appear to be satisfied with the representativity of the system, which in effect prevents large whales (owners of tokens in PoS) voting for upgrades, but also participants voting on behalf of a large number of people. This compares positively with MakerDAO’s implementation of voting, or Aragon, which is undermined by this phenomenon of plutocracy: governance by one whale. The feature that helps in Tezos is fundamentally the obligation of token holders to either vote themselves or delegate their vote. There is still quite a way to go for demonstration of on-chain governance though: Tezos users complain about too much friction to voting and people signaling their preferences. Inspiration might come from Cosmos, where a mechanism of overriding votes exists.

The vote on the EIP999 proposal on Ethereum is also instructive from a governance point of view. The debate is very controversial here, as it proposed unfreezing half a million Ether lost to about 600 wallets due to a Parity vulnerability in 2017. 55% of voters voted “no” to the proposal, but the polemics have not ended, because the vote was based on the amount of Ether owned. But this is in question because, for instance, another choice could have been to have one vote per participant. Then the keen interest of Ether holders is to vote against a decision that would somehow dilute them. Further, the Polkadot team is the most affected by the freeze, so the interests in presence are specific. A “yes” vote would have caused a hard fork, and consequently would have created a precedent for repairing faulty code, thus opening quite a Pandora’s box!

Hard forks

Hard forks are more common than perceived: but lately, they happen rather peacefully, with the pools of miners upgrading to the new code

without the original chain continuing. This is the case on Ethereum and also on Beam, Monero, etc..

SCALABILITY

Scalability in terms of transactions per unit of time

More than ever, scaling blockchain throughput depends on some sort of sharding, side-chaining, or child-chaining. To an extent, it's always the same story, deporting the throughput rate to parallel or attached chains.

Bitcoin SV has increased the block size from 128Mbites to 2Gbites, reaching a throughput rate of over 1000 TPS.

Lightning network for Bitcoin

On Bitcoin, as the adoption of the Lightning Network increases, so too, more micropayment channels will be added to the network. So, it is projected that ultimately, there will be millions of necessary on-chain transactions resulting from the opening and closing of channels, which will eventually again lead to congestion on the main Bitcoin chain, rendering the Lightning Network useless. Another issue is the locking in of funds by the two parties who want to cooperate in a channel. When both parties intend to transact more often, they will have to deal with rebalancing and refilling of channels regularly, which again increases interactions with the main chain. So, to try to solve this, developers have proposed a solution called "Scalable Funding of Bitcoin Micropayment Channel Networks" – a concept today commonly referred to as "Channel Factories". The idea is to place a new layer between the main BTC chain and the Lightning Network, to enable the creation of payment channels without recording transactions on the Bitcoin blockchain. Each channel factory will consist of a network of individuals who can initiate a single transaction on the Bitcoin blockchain and have the funds committed to the whole network. The funds deposited and shared among this group of individuals is then known as a "hooked transaction". Opening a channel factory is the same as opening payment channels in the Lightning Network. Once

the factory is open, it can be used as a base from which many more channels are created. In other words, channel factories are payment channels that can be used to create more payment channels.

Ethereum

Here are a few updates, awaiting the October 8th-11th DevCon in Osaka:

- Ethereum's implementation of PoS has been much anticipated. It had been planned to be finalized by the end of June 2019. To recap, two flagship components are to be implemented: Casper, which is the PoS algorithm to replace mining, and sharding.

- The expectation is improved scalability by a factor of 1,000, but sharding is expected to be the last feature to be launched because the consensus mode modification will intervene first so that the main net becomes the "beacon chain". What remains slightly unclear is whether, post-sharding, scalability in principle can be infinite, if we manage to have shards of shards not needing to communicate much with each other.

- The developers have expressed their satisfaction that they seem to be able to contain the whole Ethereum 2.0 in 1000 lines of code.

- Meanwhile, V. Buterin has admitted that the Ethereum blockchain is almost full, that is to say, right now, any significant throughput request augmentation would push users out.

IOTA

The Berlin-based IOTA team has unveiled what they consider a breakthrough in their direct acyclic graph solution. The solution's name is Coordicide because it is killing the previously necessary 'Coordinator'.

To recap, the "Coordinator" in IOTA was introduced in the infancy of the network to protect users' funds. In a tangled network like IOTA, where there are few participants in the network (in its 'infancy'), the problem indeed is that an attacker can try to create a vast number of nodes (a Sybil attack), so that it can take control of the validation of transactions.

To prevent this from happening, a specialized node run by IOTA has been introduced in order to avoid this from happening again. For this reason, critics of IOTA that claimed it was not decentralized but under the control of its management to ensure transaction finality and prevent double-spends, were more than founded. IOTA has always claimed that they would shut down the Coordinator as soon as a sufficient number of transactions per second was reached in the live network, while also arguing that every node participating in the system could check that the Coordinator was indeed acting loyally.

The claim here is that thanks to this new mechanism, IOTA is becoming the first scalable, fully-decentralized distributed ledger technology, and with fees still low thanks to the tangle approach. Their press release states that "at the heart of the Coordicide solution is a modular system that adds flexibility across all aspects of the IOTA protocol. This brings benefits of increased scalability, faster transaction finality, and easier node maintenance, as well as a variety of unusual use cases. Data streaming services and other real-time applications become a real possibility with IOTA; use cases that are not feasible in other DLTs".

So, the Coordicide solution is to realize IOTA's promise as a lightweight and feeless ledger, overcoming the trilemma of scalability, security, and decentralization, which continues to limit other DLTs and blockchains. How does it work, however? Several features have been introduced.

- First, all nodes are identified thanks to a unique identifier, and a reputation system is used; each time a node makes a correct transaction, he gains 'mana', but this reputation is slashed if it intends to act in a malicious way (double spend).

- Another module is secure auto-peering, as peers are ultimately the only source of information. Here the mechanism is designed to make the peering of a given participant both local and unpredictable (in particular preventing an 'eclipse' attack; that is, isolating a node to attack it).

- Spam protection moves from a small, undistinguished PoW base to an 'adaptive rate control'. The difficulty of the puzzle for accepting a transaction depends on the mana and on the rate of transactions submitted to the network per amount of time.

- The choice of previous transactions on which a new transaction is pointing (or relying upon), that is, 'tips', is modified. It passes from a biased random walk to a voting layer to identify the appropriate parts of the tangle to attach transactions. Importantly, this evolution is supposed to solve the big problem that some healthy transactions could be left behind.

- But the core of Coordicide is a new voting module that works to reach consensus thanks to enhanced "proactive" communication between the nodes within the network ("shimmer"). The introduction of a voting mechanism brings the following benefits: instead of waiting until the situation resolves itself with more and more accepted transactions, the nodes are talking to each other and resolve the situation proactively; a node's vote is weighted according to its reputation (good actors have a more significant influence).

Cardano

A new release (1.6) is imminent. Details about staking are more precise: there will be two separate keys for spending and staking. If one decides to stake their ADA tokens, the tokens will never leave the wallet. Cardano will not require tokens to be locked in for a term – one can stake tokens at any time. This flexibility currently sets Cardano apart.

Others

- IOST voices its specific "proof of believability" (PoB) approach. Let's take a brief look at it: they have

BUTERIN HAS ADMITTED THAT THE ETHEREUM BLOCKCHAIN IS ALMOST FULL, ANY SIGNIFICANT THROUGHPUT REQUEST AUGMENTATION WOULD PUSH USERS OUT

implemented a reputation mechanism (Servi points, which are non-tradeable) in which the probability of a node being chosen to validate a transaction is proportional to its IOST stake, its Servi earned, and its transaction and action history.

- Alephium is a project aiming to scale to tens of thousands of transactions per second in an open, permissionless network. Its core algorithm, called BlockFlow, claims to combine sharding technology with DAG and utilizing a scalable UTXO (Unspent Transaction Output) model to resolve the inefficiency of sharding performance during cross-shard transactions. By breaking down smart contracts into token protocols and data protocols, Alephium intends to “allow developers to build dApps that support high concurrency scenarios while maintaining the Turing-complete functionality of smart contracts”.

- Harmony, which IEOed on Binance, implements a Fast Byzantine Fault Tolerant protocol, claimed to be ~100 times faster than Practical-BFT. Harmony also relies on a version of sharding similar to Zilliqa’s but also includes state sharding.

- Conflux: Founded by individuals initially working on scaling the Bitcoin protocol to thousands of transactions per second.

Scalability in terms of ledger sizes

Cardano is advancing research with the motto that “not everyone needs data”. The study is focused on exploring pruning, subscriptions, compression, partitioning, sidechains, and sharding.

INTEROPERABILITY

The European Union is fostering research on interoperability; one of the initiatives pushed is led by SIACHain and Quant Network, trying to link using Corda and Ethereum.

Various initiatives pop up now and then to bridge blockchains, please refer to earlier issues of Blockchain Quarterly for relevant technical mechanisms.

CONFIRMATION TIME: FINALIZATION MECHANISMS

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

LEDGER DATA STORAGE SOLUTIONS

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

PRIVACY – CONFIDENTIALITY

Mixing

Some “mixing” services have appeared to explore the possibility of grouping transactions with multiple inputs and outputs (such as Bitcoin), to obfuscate where the money is going.

The “fun” part is that regulators have immediately started to clamp down on these services! For instance, Bestmixer.io has been shut down by the Dutch regulator. This all too illustrates where the next crypto battle is being waged, as expected! By all means, states are not going to let go of their control over financial flows.

The actions of these official bodies are regarded as very serious 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

- Grin has received an anonymous donation of 50 BTC. That may help speed-up whatever the community would like!

- Beam has successfully conducted a hard fork in mid-August.

- The market capitalization of MW tokens is still very low, with a considerable potential to increase.

Zero-Knowledge Proof

ZKP is increasingly being integrated into new chain proposals and distributed applications.

IDENTITY & PERSONAL DATA MANAGEMENT

Identity and personal data management are becoming a big topic, one that justifies a specific technical section. As we have not yet delved into this topic, we’ll do so now.

Let us first recap what identity management is, in a classical sense.

- First, what is identity? Let’s say it is a set of metadata that is associated with a human being, e.g., name, sex, date/place of birth, address, etc.; some of these are assumed to be fixed, and some can change over time. By extension, personal data are an extended set of data that relate to a specific individual, with particular outreach (scholar, medical, etc.).

- Then, the way the identity data is stored or accessed is very diverse: it can be an official document; it can be self-declared information associated with an online account in a merchant’s database (paper or electronic); it can be recorded in churches that attest to births and marriages. In principle, all these records could be cross-compared, and the aggregated data should indicate the same thing for the same characteristic recorded.

- Finally, whenever there is a need for authentication, the way identity is proven is also diverse, and depends on the available means of verifying identity. When and why do we need to verify identity in the first place? Usually, when an individual is attempting to gain access to something or obtain a service they are entitled to, but one that would be denied if the person is not authorized. And as human beings always try to cheat established contracts, a valid identification of the requesting individual is necessary. The verifier is going to check a claim of an individual against, say, a reference view of the data. Apparently, biometric authentication enables official passport documents to be tested; the monkey standing there is the same as the monkey that went to the official administration to establish the record, and recognizing that the passport is a document that

is very difficult to counterfeit, the probability that the rest of the information is accurate is reasonably high. When attempting to access a secure website, a password is required that matches the one specified at the time of registration, and with 2-factor authentication, again, only the person who set up the account is supposed to have access. But in every case, the verifier needs some grounds on which to acknowledge the claimed identity.

So, in this context, what is blockchain offering when the proposal is made to manage identities and private data with it? First, let us summarize the current initiatives in the domain. We will discuss the following “services”, “functionalities,” and “use cases”:

- Providing an official on-chain identity; that is, with cryptographic proof that it has been established thanks to an official check and commitment to the data.

- Providing third-party insurance on the personal data of individuals; the most interesting application is to provide a KYC service.

- I am proposing that users take back control of their data, in the sense that they should own it and give access to entities that request it, potentially for remuneration — consequently, the decentralization of the storage of user data.

- They are proving one’s legitimacy without even disclosing the information itself, e.g., a night club being able to confirm that a person is above the minimum age without having access to the person’s actual age. The implementation of this relies on Zero-Knowledge Proof algorithms. It can be seen as an additional layer able to be implemented once the digital identity has been added to the blockchain.

Data protection regulations are a running concern in the blockchain arena. Intuitively, blockchain is not a right candidate to deal with identity and private data, because what gets written to a public

blockchain is accessible to everyone, and remains so forever. The mere fact that an entry exists in a register is considered private data under GDPR law.

So let's consider an interesting and concrete example of how some propose to make it function – a trial conducted by the city of Zug, Switzerland, where the government is considering providing citizens with a “digital, decentralized identity” thanks to a system based on Ethereum called uPort and developed by Consensys. The objective is that, for any situation where identity verification is required, the verifier would scan a QR code provided by the prover. Three features were targeted for the development of the service: digital (all automated), decentralized (no third-party database), and sovereign (that is, “Your identity is under your control and not under the government’s control, and it is all in your phone”). To establish this official on-chain identity, the following occurs:

- The individual first gets the uPort app. The next step consists of creating then managing a private key for the individual on the Ethereum blockchain, as any wallet would do.

- Then two smart-contracts are created by the app on the blockchain: a “Controller contract” that itself is controlling a contract where the identity data is accessible. This complication has been imagined for several reasons: (i) to enable recovery of the identity in case the smartphone wallet is lost, (ii) to allow for transfer of the ownership of the identity, and (iii) to prevent an identity from being totally and definitively open should the private key be disclosed. The controller smart-contract contains, in addition to access control logic, an access key to the identity smart-contract. So, it is replaceable as soon as one can create a new controller smart-contract that is fed with the access key again, thanks to a seed that is the real ultimate password controlled by the smart-phone application, and that the user has to keep safe. But either way, this is not central – the main idea is that an Ethereum address would represent identity.

- Users then create their data/identity information

record by entering the data using the application, which in turn, just creates a JSON profile object which it uploads to IPFS. And then it creates an entry in a specific and unique smart-contract, the uPort registry smart-contract. There, the hash of the identity is recorded. So, the data is stored off-chain, but the hash is on-chain, ensuring that the information is not tampered with.

- Importantly, the permanent identity smart-contract does not contain data, it is dedicated to being the signing authority when the individual in control of it wants to prove their identity. This smart-contract can then delegate the signature if it's in a smartphone wallet.

- It is also important to point out that in this process, the identity data is not encrypted; the main concern is to address the need for individuals to be able to prove they have sole control of that identity. We can, of course, think of a way to achieve this thanks to encryption of the data in IPFS.

- At this point, users have a uPort identity and need to connect to Zug's public administration webpage where they are provided with a QR Code that is scanned with the uPort application. This triggers the sending of the identity data to the administration, i.e., a civil officer of Zug, authenticated on the blockchain as such. The official checks that the data proposed are by the off-chain Zug public registers, and if so, at the time validates the physical visit of the requester. What happens is that the personal identification data of the citizen is combined with the QR code, hashed, and sent to the Ethereum's smart-contract, where it is available for the officer to see and compare with the administration's version of the data, combined and hashed.

- Then, when this is done, for a routine identity control, the user would scan a QR code provided by the verification entity, which is a package of data containing their address/identification on the blockchain, and the request for the required information. The user can then provide the required information through a display interface that does not stay in memory, and by combining it with the initial

hash publicly available, it can be checked that it is the same information that has been validated by the civil authority.

- In effect, proving your identity narrows down to the same thing as knowing a private key (equivalent to a password) or owning a device that holds it. So, where is the real innovation? It's quite different, in essence. For example, you could have one or a limited number of verified identification providers for the services where identification matters. So clearly, it is crucial to have an efficient way to keep the key (or password) safe, with potentially a high cost if it is lost.

- Using blockchain for personal data management increases the security of authentication concerning the classic login/password process.

- Note that, in turn, this can lead to some issues, because, if several terminals are holding this identity, then several individuals may be able to claim this identity unduly.

CRYPTOGRAPHIC ROBUSTNESS – QUANTUM COMPUTING EVOLUTIONS

Without revisiting the functioning and potential impact of quantum computing, let us state here that there is no shortage of frenzied press releases and technical development claims from firms involved in making this a reality. So, the inception of quantum computing is just a matter of time, which may be shorter than expected.

VOLATILITY

Analysis of volatility

Volatility was down throughout the bear market, and resumed with very violent moves, especially the price of Bitcoin, on June 25-26. Observers who were starting to comment that cryptocurrencies were finally starting to behave a bit more calmly, on their way to becoming suitable exchange and a store of value, are reconsidering their views.

Stablecoins

The thrilling Tether saga continued spectacularly – we have repeatedly observed the doubtfulness of Tether's management in these columns. On April 25th, the New York Attorney General's office said the team behind the crypto exchange, Bitfinex, which shares a parent company with Tether (iFinex), used funds from Tether to hide up to \$850 million in (alleged) losses. While this is not the same as a hack, the effect would be the same if this money is lost.

Bitfinex has claimed that it was due to some funds being seized in the UK, the US, Poland and Portugal (fun fact! these countries follow each other in alphabetical order, 2 by 2 – but let's not assume that they have been picked non-randomly), hence the exchange was unable to allow for funds to be withdrawn by users. To solve the issue, an agreement was reached between the two sister companies so that Tether would send money to Bitfinex. Just like that – merely an accounting operation.

So today, assuming that Tether was previously fully backed (which nobody can confirm), US\$850 million of the treasure is missing. Compared to a market cap of US\$2.7 billion, this is still a ~70% backing, so it is not too bad, after all. Somehow, if it were all logical after the market integrated the news, one USDT should trade at US\$0.70. But this is not the case: it has generally maintained 1:1, so far. The question is, why?

Maybe Cardano's Hoskinson gives us the key here, stating: “Well, at least Tether has more backing than my bank account.” It cannot be disputed that commercial banks have had almost non-existent obligations in terms of collateral at hand since the end of Bretton Woods, not to mention the situation of central banks. So, the backing is not such a problem, as long as users keep using it as a reference standard,

NEW YORK ATTORNEY
GENERAL'S OFFICE SAID:
'BITFINEX USED FUNDS
FROM TETHER TO HIDE
UP TO \$850 MILLION IN
(ALLEGED) LOSSES'

WE OBSERVE REPEATED CALLS TO STANDARDIZE DLT-BASED INFRASTRUCTURES FOR GIVEN SECTORS, WITH POWER GENERATION BEING ONE OF THE MOST PROMINENT

and there is sufficient margin so that people who wish to exit can do so at the nominal rate. Is the situation dangerous? At some point, indeed. Is it new? Not at all. Should it be changed? Each will have an opinion. This debate of fractional reserves is poised to be started again, raising full concern.

Okay, with that said, are we sure that the situation is sorted out? Honestly, we are quite doubtful. Given the track record of the unreliability of

BitFinex and Tether's management, it would be surprising for them to be out of the woods "so easily". The parent company of both even made a move to issue their token...

Finally, let's consider: what does this Tether situation imply? Today, it is still widely used in trading, so much so that 80% of

Bitcoin trading is funded using USDT, on platforms that do not support fiat at all. The convenience of Tether is huge and desperately needed. So far, no other stablecoin has managed to challenge its position. Tether's market cap is still about 10 times that of TrueUSD and USD Coin, and DAI is less than USD\$100 million. What would happen if USDT collapsed? Well, those holding it would have worthless tokens, or worth the collateral that a liquidator will have at hand to distribute to them. Today, USDT is 1.5% of the total coin market cap, which fluctuates much more in a single day, so it would, in effect, mostly be unnoticed if it were wiped out. Of course, the turmoil would impact markets. But then auditable stablecoins would benefit from the space left (they have been prepared, for some time, to do so), and everything would resume peacefully – most probably.

Apart from Tether, a few other stablecoins appear on the market now and then, backed by various fiats, such as the Brazilian real and British pound,

etc.

Also, a stablecoin backed by XRP is being developed by Kava Labs. USDX, its intended name, will be implemented as a Cosmos Zone designed to peg XRP and issue the XRP-collateralized token.

STANDARDIZATION

We observe repeated calls to standardize DLT-based infrastructures for given sectors, with power generation being one of the most prominent due to the complexity of the supply chains, as they currently exist, and due to the new functionalities that are feasible, thanks to the use of DLTs. But other sectors, such as the shipping industry, are actively discussing standardization.

MALICIOUS ACTIVITIES

Double spending – 51% attack

In the corporate world, blockchain experts are increasingly voicing their concerns that the risk associated with malicious actor taking control of a public blockchain on which their business would be running is simply not an acceptable situation, a risk that just cannot be considered when choosing the infrastructure on which to build their economic ecosystem with other stakeholders. In this sense, the 51% attack threat is quite a motivator for the establishment of consortiums governing permissioned blockchains.

Market manipulations

Crypto markets are still mainly as wild and unregulated as they have always been, and KYC has not changed the behavior of traders that would be punishable on regular stock exchanges. The question of whether it is legitimate for regulators to intervene in a space where people are playing one against the other is a philosophical one, but we believe that regulation is required when we observe people losing their money purely due to the efforts of some individuals, whose actions are designed and undertaken to achieve precisely that.

As the police saying goes, "investigate those who profit from crime". One emblematic example of this is the alleged behavior of BitMEX, a platform that offers futures contracts. It generates much traffic and is very profitable. The platform takes its index prices from other exchanges (Bitstamp, Kraken, Coinbase), so a price shock on Bitstamp can result in many contracts being liquidated if traders can not honor the resulting margin calls. It is suspected that BitMEX plays on this by taking the opposite positions to its clients and acting deliberately on the reference crypto exchanges to create the event.

In general, when one observes unusual price volatility in the markets, it is hard not to think many actors are trying to influence the crowd with technical analysis signals that traders look for, such as trend line breaks, and moving average crossovers. They probably succeed occasionally.

Thefts, hacks, frauds, and scams

It has been Binance's turn to be hacked: €35M were stolen, or 7000 Bitcoin. The security breach allowed attackers to access the credentials of users, including their two-factor identification codes. The most interesting part of the story was the idea (proposed by the Bitcoin community) to try to convince the majority of mining pools to roll back the ledger, that is, to re-write the chain discarding the theft transaction. However, Binance's CEO decided not to go that way for the sake of maintaining the credibility of Bitcoin. Some observers also commented that the Binance hack might have been self-inflicted, as they were able to correct the breach very quickly, and it was a manipulation to cause the price of BNB, which had been rising too sharply, to fall before resuming the uptrend...

In Poland, the Coinroom crypto exchange shut down, and management escaped with customers' funds. An e-mail had been sent to clients urging them to withdraw funds urgently, as their contract was being terminated.

RemixPoint, a Japanese exchange, also lost almost €30M in a hack at the end of July.

The Criminal Investigation Department in Gujarat, India, has exposed a former promoter of the BitConnect scam, which collapsed in January 2018. The scammer was luring people to invest in "Regal Coin," promising unrealistic returns as high as 5000%. The estimated amount of the scam is hundreds of thousands of euros. It looks like authorities are now faster at recognizing Ponzi...

Otherwise, we have not yet mentioned it, but cryptocurrencies have indeed transformed the kidnapping/ransoming business, as it has become much easier to ask for funds to be sent to an anonymous crypto address, Monero or ZCash for example.

More generally, if we are always holding our private keys to a portion of our wealth, this can be seen as a return to the Middle Ages when it was not safe to travel by road, because thieves could easily threaten a person, and steal their gold. So too today, you could be in a similar situation of having to transfer crypto money fast and anonymously to an offender immediately.

Mining malware

More sophisticated mining malware continues to spread on the internet. To deal with this, Firefox now provides an add-on option to block crypto-mining scripts automatically.

Pump and dumps

As we previously explained, a pump and dump entails the following: a group of (anonymous) individuals creates social media channels, mostly on Telegram, and gathers as many followers as possible. This crowd is then told the precise moment when a pump is scheduled and is given an expected return – but, the identity of the target token is not disclosed yet. At the expected pump time, the target token is revealed, and the pump starts. Usually, it's a meaningless shitcoin with low but sufficient volume. Typically, the price goes up in minutes, before going down a bit slower, in tens of minutes, back to more or less the initial level. The instigators of the pump and dump make money because they buy the chosen

coin before they launch the pump; they then sell (dump) at a higher price, while the slowest followers are trapped and are the ones losing money (or are stuck with the token).

Some researchers have studied several hundred pump and dumps that have occurred during recent years. They then trained a robot to try to detect these maneuvers upfront. After testing a resulting strategy, they claim that they can generate a return of 80% in only three weeks. It is not clear why they are publishing this research, though, instead of just exploiting it...

SYNERGIES WITH OTHER TECHNOLOGIES

IoT synergy

Not surprisingly, much attention is being given to companies that specialize in deploying IoT sensors and actuators that are authenticated on the blockchain. A German company, Slock.it, is one of them. It was acquired in June by Blockchains, LLC, a Nevada company with a project to build a blockchain-enabled smart city in Nevada.

Artificial intelligence

Blockchain and AI are separable, as we have previously mentioned, however, in some industries, they are increasingly being perceived as complementary, which is good.

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 flow of projects announced that use Hyperledger and Corda is continuing at a reasonable pace.

CONCLUSION OF THE TECHNICAL DEVELOPMENTS

As time elapses since the inception of the technology, new DLT innovations are, of course, becoming more challenging to find. However, as more intelligent researchers and relentless developers have been attracted in the domain, the amount of expended effort has dramatically increased as well, which, up to now, has enabled technical progress to keep a reasonable pace. This is illustrated this quarter by the progress made by IOTA and channel factories.

7 OVERVIEW BY COUNTRY

ASIA

JAPAN

- The Financial Services Agency of Japan recently declared that it would increase its oversight of cryptocurrency exchanges to stamp out money laundering. With the Financial Action Task Force (FATF) visiting the country in the fall of 2019, Japan hopes to gain a favorable rating from the intergovernmental body.

- E-commerce firm Rakuten launched its own cryptocurrencies exchange.

SOUTH KOREA

- Shinhan Bank signed a memorandum of understanding with financial technology start-up, Ground X, and blockchain developer, Hexlant, to develop a blockchain security system.

- Observers have witnessed a growing number of Korean blockchain projects leaving the country. Reasons for this include stricter internal controls on cryptocurrency exchanges, wherein investors are not able to make or withdraw deposits in Korean won on Korean exchanges, resulting in low transaction volumes.

CHINA (MAINLAND)

- Overall, regardless of the controls on cryptocurrencies (and currencies in general), China has been identified by international observers as taking the lead, in technological terms, as far as blockchain is concerned. This comment is also valid of 5G and artificial intelligence; the Chinese State Council has included a focus on these technologies in the nation's 13th Five-Year Plan, and in 2018, President Xi Jinping said, "China seeks to lead in innovation worldwide", citing blockchain, AI, the internet of things and other technologies, as the driving forces. This says a lot about China's national goal to reach and stay at the forefront of technological innovation in fields that have been identified as strategically important to the country's near-term future. China, with its vast talent + capital resource, is succeeding in taking the lead.

- Chinese universities are imitating other initiatives (such as MIT) to issue diplomas to their graduates with student credentials registered on a blockchain.

- A Chinese court has ruled that Bitcoin is "virtual property". This is a recognition that Bitcoin ownership is legal in China.

- A blockchain invoicing system has been tested by Shenzhen city, to track official purchases, and to fight tax evasion. In one year of operation, the system handled six million invoices to the value of half a billion euros, involving 5300 companies.

- State-run China Telecom announced its 5G-era SIM cards will be blockchain ready (for Ethereum, that is, Ether and Ethereum-deployed tokens), and will even allow devices to act as nodes. The researchers declared that, in their view, Blockchain is "the only technology that can enable users to secure their data in the coming 5G era, regardless of the data's volume, variety or dimension."

- Finally, China is said to be finalizing its crypto-renminbi, which could be issued to seven institutions, including Tencent and Alibaba, as early as next November.

CHINA (HONG KONG)

The recent social unrest in Hong Kong has sparked local interest in the money that is not under the control of the government, especially cryptos that are anonymous (ZCash, Monero). This has been fueled by fear generated by the arrest of activists identified by the authorities on the social networks. This, in turn, has led to a market premium in Hong Kong for these crypto-assets on exchanges. This observation is further indication that cryptocurrencies receive a keen interest wherever there is political uncertainty or failure of a state. Similar to the way that Facebook and Telegram helped to organize the Arabic Spring, cryptocurrencies have a role to play in struggles against oppression worldwide. Note: importantly, cryptocurrencies are not currently banned in Hong Kong, as they are on the mainland.

PHILIPPINES

- The chief of the Philippines' central bank has warned of the risks of increased cryptocurrency use in the country. Their primary concern is the risk of terrorism financing.

- The UnionBank has performed a pilot for blockchain-based remittances – a crucial source of wealth for the country, given the number of Filipinos working abroad: in this case, the test was conducted with money originating in Singapore.

SINGAPORE

The central bank of Singapore and its Canadian counterpart (MAS and BoC) have conducted a very interesting trial. Both banks have different DLT systems that they rely on: Corda for MAS and Quorum for BoC.

The test involved successfully executing a payment versus payment operation (PvP), thanks to a hashed time-locked contract, that worked without the use of an intermediary.

THAILAND

- Thanks to its proactive enactment of cryptocurrency laws related to the offering of digital assets and existing pure cryptocurrencies, Thailand is increasingly being viewed as a haven for crypto-related businesses.

- The Bank of Thailand has built a prototype solution to settle interbank transactions on a blockchain. Although not yet available to the public, it is still a significant step taken by Thailand.

MALAYSIA

- The Malaysian securities regulator has registered the operations of three exchanges: Luno Malaysia, Synergy Technologies, and Tokenize Technology, giving them 9 months to comply with all regulatory requirements fully.

- Overall, the administrative signals given by the Malaysian government are now more positive.

INDIA

- Officials are blowing hot and cold in India. The official position is very messy, which is in sharp contrast, for example, with the clear view taken by the government of China. After showing some signs of softening, the Indian regulator demonstrated once again that the country is divided at the highest level concerning the issue, saying it was considering a full ban of all cryptocurrencies – “One step forward, two steps back”, as the saying goes. As of early June, fears of a blanket ban were rampant, but as the second term of N. Modi started, no such action materialized. On the same day, an Indian panel, under the responsibility of the Ministry of Electronics and Information Technology, proposed fines and up to 10 years jail time for using cryptocurrencies in the country. And the same day

you hear an official saying that there is no official ban of cryptocurrencies in India... the soap opera continues.

- An Indian delegation visited Crypto Valley in Zug, Switzerland, to exchange views with Swiss officials and gain insight that could assist in making wise decisions back on the subcontinent. The take-away for the delegation seems to have been a validation that states can take advantage of the technology to gain efficiency, but, in India, this would require deep reform beforehand (or simultaneously), of systems including education, taxation, etc.

IRAN

Iran’s government is close to passing a bill that finalizes regulation for cryptocurrencies. Mining activity will be allowed, although subject to official approval and an energy fee. The ban on cryptocurrencies will also be lifted, although payments made with cryptocurrencies are still not legal – at least ownership of crypto assets is not prohibited.

UNITED ARAB EMIRATES

- Dubai continues to make headlines about being at the forefront of smart city technology. Blockchain is, in that sense, only a part of the effort of the emirate. Several initiatives have been proposed to study ways in which blockchain can transform the city.

- On the financial sector side, instruments of Islamic finance (sukuks, etc.) can be tokenized, just like any other financial instrument. Discussions are being held in Dubai to provide this service, based on Corda.

ISRAEL

- The Israeli Supreme Court has ruled in favor of a crypto business that was denied the continuation of traditional banking services. Bank Leumi was ordered to keep Bits of Gold’s (the country’s biggest crypto exchange) account open.

- While the “start-up nation” lives up to its reputation by having many thriving DLT-related ventures, the country is increasingly critical of the burdensome

bureaucracy that impairs the faster development of business.

EUROPE

RUSSIA

- Dmitri Medvedev, the Russian Prime Minister, has expressed the view that “as cryptocurrencies lose popularity, regulation isn’t a priority.” Maybe he has spoken too fast...

- In applying Federal Law No. 115, “On Combating Money Laundering and Terrorism Financing”, Sberbank is demanding its clients provide data on their cryptocurrency revenues.

- Russia is considering using gold-backed cryptocurrency for settlements of fiscal balances with international partners. What is careful about Russians is that they are pragmatic and do not hesitate to go in boldly when it is evident that to do so makes sense. We have already repeatedly stated how convinced we are that Gold will make a big come back as a currency, and it looks like this Russian initiative supports this belief. Let’s carefully monitor how this develops; no doubt, the US will fight it with all their strength to maintain the predominant role of the dollar.

- A different piece of news comes from a Duma committee, which is debating whether mining activities should be banned (and people engaging in being fined).

SWITZERLAND

- SIX, a Swiss exchange, is considering issuing its token using an Initial Digital Offering. They have chosen Corda as the technology, mainly due to the requirement to implement transaction privacy. The resulting exchange, to be named SDX, is the result of significant investment. SIX is continuously approached by various entities in attempts to issue

warrants, structured products, real estate funds, etc. This indicates that SIX and its clients consider it is merely a matter of time before tokens will replace shares.

- Avenir Suisse, a think tank, released a report urging the Swiss National Bank (SNB) to start working on a national cryptocurrency. In their view, “It would facilitate tokenized securities trading if the National Bank and major players in the industry were to drive the development of a Swiss franc token.”

UKRAINE

Engineers at a nuclear power plant have been arrested for mining cryptocurrencies with a supercomputer. Connecting it to the internet was in breach of the plant’s safety.

UNITED KINGDOM

- The London Stock Exchange has outlined how it will be using DLT. It has invested in a start-up that claims to have created the first “automated” crypto-denominated bond – it is unclear why the LSE considers that such an instrument is technically challenging to develop. The exchange can “see a use for blockchain in processes like issuing securities and settling trades.” Really? LOL. These guys are geniuses.

- The Bank of England has declared that it intends to open its vaults to tech companies. This means that it plans to provide a custody service for stablecoins to store reserve assets directly in its facilities. That is quite a recognition and legitimizes initiatives on fiat-collateralized tokens.

- Prime Factor Capital is the first crypto hedge fund registered as such by the Financial Conduct Authority of the UK and is thereby explicitly authorized to invest exclusively in crypto assets.

SWEDEN

Sweden has gone further than any other society in removing cash from circulation: less than 20% of businesses accept coins and notes, which accounts for less than 2% of transactions in the country. Talk about issuing an e-krona by the Riksbank (central bank of Sweden) is not as prevalent as it was in early 2018, but plans are still in place to do it; it is now merely a political decision to start the experiment.

PORTUGAL

Authorities have confirmed that crypto trading and crypto payments are tax-free in Portugal.

ITALY

The Ministry of Economic Development is reported to have urged the Agency for digital technology (Agid) to adopt fintech to define legal guidelines for blockchain innovations. The regulatory environment is intended to be designed for various blockchain innovations, including cryptocurrency.

FRANCE

Loi Pacte has been validated by Conseil Constitutionnel, and Autorité des Marchés Financier (AMF) is now in a situation to study ICO projects to verify those that are compliant with its guidelines. These projects are to be whitelisted by the watchdog and will benefit from this publicity: they receive an official “visa”.

French ECB policymaker François Villeroy de Galhau has said that stablecoins linked to real currencies are “promising”, and he is following the development of these tokens closely.

GERMANY

Members of the ruling CDU/CSU party have declared that it is studying the feasibility of introducing a tokenized euro in its public services.

MALTA

After diplomas, Malta intends to promote the recording of rental agreements on blockchain. It’s a familiar theme: to try to force some usage of the technology domestically to justify the perception of being the blockchain island, where progress is achieved first.

that neither cryptocurrencies nor the agreements between exchanges and users constitute a security.

- The business-friendly tone adopted by Hydro Québec towards the crypto-mining industry is confirmed: an auction for an allocation of 300 MW of power targeting this business segment was recently conducted.

MEXICO

The development of exchanges is reported to be soaring, particularly in Mexico. This is consistent with the rest of Latin America.

BAHAMAS

The Bahamas Securities Regulator has proposed rules for token sales: that is, crypto-assets that are not deemed securities. These rules include imposing disclosure requirements for project proposals, and anti-money laundering precautions.

BERMUDA

Bermuda’s officials are actively promoting their dominion as a fintech hub. Their meetings with prominent blockchain entrepreneurs and companies have gained some exposure.

UNITED STATES OF AMERICA

- The US is a significant player in the DLT field due to the sheer size of its economy, the advanced education of its population, and the large and unprecedented amount of available capital. However, in no small extent, it appears to be an “incumbent” superpower that has a position to lose by having China and other nations make faster progress, and more willingly embrace all sorts of disruptions promised by DLT. The least of which is, of course, the challenge it poses to the USD-dominated world monetary system, which is used by D. Trump and his administration as an all-out weapon in the trade wars they are waging. Most of the criticism towards cryptocurrencies comes from the US, led by JP Morgan’s Jamie Dimon, followed by PE/

VCs and fund managers like Berkshire Hathaway’s Warren Buffet, who regularly express their disgust. Even most tech gurus, like Bill Gates and Elon Musk, display mixed feelings, as do the Fed’s and SEC’s officers, of course. As a consequence, it looks like, by their standards, the US is lagging in the DLT revolution. Some local observers have expressed concerns that the country is losing the race right now if it does not react.

- Moody’s has expressed concerns about a systemic risk that the usage of cryptocurrencies would impose on the financial system, due to a “counterparty concentration risk” when using blockchain. Well, while this may be a correct observation, it looks like it will always be less concentrated than the USD!

- Recent interactions with the SEC have shown that their officials have a high level of knowledge, even in the technical aspects of smart contracts. That proves the institution is resolutely studying crypto assets.

- Utah is considering notarizing vehicle registrations on a blockchain, with benefits that include a substantial cost saving, compared with the current process.

- Coinbase has published a “United States of Crypto” document, with bullish views. Unsurprisingly, they report an increasing awareness. The most impressive figure is undoubtedly that 15% of Americans polled say they are somewhat likely or very likely to buy cryptocurrencies.

- Following Libra’s announcement, there were many reactions in the US. President Trump tweeted that he was not exactly a fan of bitcoin and cryptocurrencies, nevertheless some observers see this position as an indication of awareness that cryptocurrencies are achieving mainstream acceptance and affecting decisions at the highest level. The US Congress was impressively quick in sending a letter to Facebook’s CEO, requesting that a hold be placed on Libra until the consequences this cryptocurrency can be established. Repeated hearings of Congress have been scheduled and conducted, with the concern

NORTH AMERICA

CANADA

- A government agency is reported to have asked Deloitte and LiteLink to work on a blockchain supply tracking solution.

- Canadian and US regulators have fined Mr. Tapscott, CEO of NextBlock Global, for breaching the securities law – namely, having made a false statement in their US\$16 fundraising effort.

- Several Canadian banks, including CIBC, Desjardins, RBC, and Scotiabank, are launching

the use of Verified.Me, a blockchain-powered identity verification solution from SecureKey. This is an attempt to give customers control of their identity data.

- The Canadian Securities Administrators and the Investment Industry Regulatory Organization of Canada have released papers for public feedback, on proposed cryptocurrency regulations, to which the principal exchange, Kraken, has replied with significant disagreement and heavy criticism. One of Kraken’s primary concerns in its reply is

that Libra could endanger the financial system, not only due to AML/CFT concerns (classic) but most importantly, due to the fear of a loss of sovereignty – and this is new.

- The US Air Force has signed contracts with two blockchain companies: Simba Chain and Constellation. The goal is to “securely unlock traditionally siloed and non-accessible data and data sources”.

SOUTH AMERICA

VENEZUELA

A pharmacy chain, Farmarket, is now accepting Dash cryptocurrency. Traki, a department store chain, has announced that it will implement the PundiX payment solution, which acts as a financial intermediary, but enables the seamless spending of cryptocurrencies.

Maduro is still in charge, despite the unresolved political crisis. His opponent, Guaido, has claimed power, but discussions are at a dead-end. Meanwhile, the infrastructure around the Petro is advancing, and the national airline has started to accept the Petro.

BRAZIL

- Brazil has established a committee composed of 34 members to advise on cryptocurrency regulation. However, President Jair Bolsonaro publicly expressed his doubts on Bitcoin after approving the suspension of a crypto project to provide banking services to indigenous people - despite admitting that he does not know much about the technology.

- The municipality of São Paulo has decided to use a blockchain for its public works projects. The Secretariat of Urban Infrastructure and Works has contracted a blockchain firm, Construtivo, to implement a technological solution to register data related to all construction projects in the city. This initiative follows the closure of several roads and bridges due to poor quality and is an effort to introduce more transparency.

- On September 1st, 2019, Álvaro de Medeiros Mendonça became the first new-born to be registered on a blockchain. The notary service is based on a Growth-Tech implementation of an IBM technology. The child registration process has three stages. First is the “Live Birth Statement” produced by the hospital. The parents then create a digital identity on the platform, after which the information is sent to the notary office to finalize the certificate. Even if the goal is to make the process fast and efficient, thus eliminating oppressive administration, it remains to be seen how this company plans to manage all this personal data on this platform.

- The payment processor, Cielo, with 1.4 million point-of-sale devices, has announced it is now supporting Bitcoin and other cryptocurrencies. Later in 2019, customers will be able to use an app to purchase cryptos. This is a considerable facilitation that will enable 200 million individuals to access cryptocurrencies.

ARGENTINA

More positive comments are being expressed around Argentina’s crypto and blockchain scene. Technologically, it is not clear how the country will emerge from its severe economic crisis, but what is certain is that the Argentinian currency is likely to depreciate further due to the very high inflation rate, compared to foreign fiat (and especially, of course, the USD). This is fueling the interest of the Argentinian population in adopting Bitcoin and other cryptocurrencies.

AFRICA

EGYPT

The strict ban has been lifted, thereby allowing for licensed cryptocurrency companies. This ends a situation that arose after a fatwah was issued by the Grand Mufti of Egypt, who identified cryptocurrencies as being too volatile and prone to scams, and therefore not compliant with Islamic law. The passing of the bill gives the board of directors of the Central Bank of Egypt the right to regulate cryptocurrencies, and issue several potentially expensive licenses that will be required to do business.

TUNISIA

The country is trying to become a blockchain hub, though it is not very visible on the radars.

KENYA

More than 6,000 farmers in Kenya use the Shamba Records platform. It provides users with data collection, mapping, and payment aggregation. It proposes to make local farming more efficient and allow farmers to access financial services more efficiently.

SOUTH AFRICA

South Africa’s United Africa Blockchain Association has announced a plan to train one million African individuals in blockchain, starting with a “train the trainers” program.

OCEANIA

NEW ZEALAND

New Zealand now allows employee wages to be paid in cryptocurrency. This can be considered as a relatively progressive move in the Pacific!

AUSTRALIA

- The Australian Securities and Investments Commission (ASIC) has published an update on how it intends to regulate crypto-related businesses and ICOs. The requirements outlined include the need to be licensed if the issued crypto assets are securities.

- The ASX, the country’s stock exchange, has invited clients to test its newly developed blockchain-enabled alternative securities management system. It is a work-in-progress that started in 2017, with a

company, Digital Asset, working on it. A live roll-out is expected in 2021. Australians are among the most aggressive in this application field.

- The Australian Tax Office has started compiling records from cryptocurrency exchanges to remind traders of their tax obligations.

- Talks about transitioning to a cashless society are gaining momentum in Australia, at the same time that increased control is being imposed on transactions: cash payments will be limited to AUD\$10k if a bill passes. This will clear the way for some cryptocurrency usage, although possibly only tokenized fiat.

COUNTY RANKING CRITERIA

To conclude this section, we would like to outline a range of criteria that we are going to use in the next Quarterly reviews to evaluate front-running countries in the adoption of crypto assets:

- Allowed possession of cryptocurrencies.
- Allowed fiat to be traded for cryptocurrencies.
- Allowed mining of cryptocurrencies (or various restrictions).
- Allowed utility tokens to be offered to the public (ICO).
- Allowed tokenized securities to be offered to the public (STO).
- Ratified laws to regulate financial institutions, to clarify how to handle crypto assets.
- Introduced licensing framework for crypto-exchanges.
- Introduced extraterritoriality of crypto laws for services offered to its citizens.
- Enforced other countries' crypto laws.
- Defined tax rate on crypto asset gains.
- Imposed anti-money laundering, and counter-terrorism financing regulations on financial institutions.

CONCLUSION: MID-TERM CONSIDERATIONS

Enthusiasm surged again in the second quarter of 2019, and, as could have been expected, this was followed by a consolidation phase. The extremely volatile behavior of the Bitcoin price in the past three months invites a comparison with the price action seen in 2014-2017. However, where the market goes from here is difficult to judge, all the more so because drawing convincing technical analysis projections without sufficient history becomes hazardous.

In support of a further mid-term expansion, we have: the accommodating monetary policy that central bankers continue to pursue; growth in exchange volumes, a convincing reversal of the 2018 downtrend; a range of circumstantial expectations, such as the first BTC ETF, halving of the BTC reward; due delivery of technical solutions and start-up products and services; and a growing appetite for cryptos in the less-wealthy developing world, where slack institutions are not in a position to enforce the use of fiat. On top of this, institutional investors are not yet really active, whereas they may enhance manifold the effects of a bull run if it is triggered.

The following factors are in opposition to this view: the impossibility for central governments to relinquish the privilege of controlling money supply and interest rates, especially in authoritarian and Western countries; a possible general economic downturn, the effects of which are difficult to predict, particularly on cryptos; the fight against PoW energy waste; the collapse of the ICO utility token fundraising model.

So, all in all, we would tend to be positive for the mid-term, depending on the crypto-asset category – Infrastructure being more appealing at the moment than Fundraising, Anonymous being risky in a regulatory context, Execution still being challenging to value.

We continue to have more things to say, business-wise and monetary-wise than technically-wise. This will likely continue because when scalability, governance, and other issues are solved, one will no longer look at how DLTs work; they will be embedded as the base layer of infrastructure stacks. Standardization initiatives are just starting in each eco-system (supply chain, etc.), and we expect these endeavors to continue. The real question remains; when will we see wide-spread public adoption of fully decentralized cryptocurrencies for regular payments, at least in some societies? Only then will monetary usage be capable of inflating the prices of non-collateralized crypto assets, and shake the global post-Bretton-Woods system.

BIBLIOGRAPHY

1. <https://www.nytimes.com/2019/04/23/technology/bitcoin-tulip-mania-internet.html>
2. <https://www.forbes.com/sites/darrynpollock/2019/04/29/high-frequency-trading-researcher-publishes-findings-on-jpmorgan-blockchain-spin-off/#6fec76a29155>
3. <https://www.coindesk.com/societe-generales-work-with-public-ethereum-is-a-big-deal>
4. <https://www.nextgov.com/ideas/2019/04/can-blockchain-finally-bring-centralized-source-truth-government/156601/>
5. <https://www.forbes.com/sites/nataliakarayaneva/2019/05/02/will-blockchain-make-poverty-obsolete-what-is-the-root-of-all-evil/#195f2d475e68>
6. <https://www.forbes.com/sites/stevenehrlich/2019/05/02/after-an-850-million-controversy-what-everyone-should-know-about-bitfinex-tether-and-stablecoins/#24ac1756492>
7. <https://www.coindesk.com/bots-exploiting-decentralized-crypto-exchanges-report>
8. <https://www.computerworld.com/article/3399961/salesforce-offers-blockchain-lite-to-entice-users.html>
9. <https://www.cryptopolitan.com/blockchain-skill-shortage-australia-cant-keep-up-with-surging-demand/>
10. <https://www.coindesk.com/tezos-is-about-to-enact-its-first-ever-on-chain-blockchain-update>
11. <https://www.bitcoinmarketjournal.com/blockchain-consultants/>
12. <https://cointelegraph.com/news/cryptocurrency-mixers-and-why-governments-may-want-to-shut-them-down>
13. <https://www.forbes.com/sites/eliboufis/2019/05/10/heres-what-investors-need-to-know-about-cryptocurrency/#10b4b7ba5f0e>
14. <https://www.forbes.com/sites/billybambrough/2019/05/30/how-billionaires-are-buying-up-bitcoin/#4e473774208c>
15. <https://www.bloomberg.com/news/articles/2019-05-31/bitcoin-s-rally-masks-uncomfortable-fact-almost-nobody-uses-it>
16. <https://coordicide.iota.org/>
17. <https://zycrypto.com/attaining-full-lightning-network-scalability-with-channel-factories/>
18. <https://cointelegraph.com/news/lambos-bling-and-mansions-what-purchases-do-crypto-millionaire-make>
19. <https://cointelegraph.com/news/crypto-italy-institutions-politics-business-and-society>
20. <https://blockonomi.com/harmony-one-guide/>
21. <https://cointelegraph.com/news/research-ico-sector-signals-uptick-after-crypto-winter>
22. <https://cointelegraph.com/news/research-ico-market-down-almost-100-from-a-year-ago-raised-40-million-in-q1-2019>
23. <https://www.apnews.com/accesswire/54f7a7818b2e3561040579dd8202f754>
24. <https://beincrypto.com/bitcoin-mining-difficulty-high/amp/>
25. <https://www.internationalinvestment.net/news/4002520/crypto-hedge-funds-grew-bitcoin-slumped-report>
26. <https://ambcrypto.com/hsbc-seventh-largest-bank-in-the-world-rumoured-to-be-blocking-cryptocurrency-transactions/>
27. <https://www.forbes.com/sites/nikkibaird/2019/06/27/retail-blockchain-deep-dive-payments/#1d781bf72d3d>
28. <https://www.forbes.com/sites/ktorpey/2019/07/02/the-overlooked-reason-the-united-states-would-struggle-to-ban-bitcoin/#6258344344a9>
29. <https://cointelegraph.com/news/pompliano-75-confident-bitcoin-price-is-100-000-by-end-of-2021>
30. <https://www.disruptordaily.com/blockchain-use-cases-identity-management/>
31. <https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702>
32. <https://medium.com/uport/what-is-a-uport-identity-b790b065809c>
33. <https://www.forbes.com/sites/forbestechcouncil/2019/08/07/digital-assets-beyond-bitcoin-three-blockchain-opportunities-in-tech/#6de5924774b9>
34. <https://finance.yahoo.com/news/finally-finding-friends-story-blockchain-140054539.html>
35. <https://www.forbes.com/sites/janicebryanthowroyd/2019/08/05/how-blockchain-could-create-more-efficient-and-effective-workplaces/#325fbde2ef6e>
36. <https://cointelegraph.com/news/who-is-david-marcus-bitcoin-believer-turned-facebooks-libra-boss>
37. <https://www.forbes.com/sites/rogerhuang/2019/08/11/as-protests-in-hong-kong-surge-so-does-demand-for-cryptocurrency/#50e5a3f675f6>
38. <https://www.coindesk.com/trumps-currency-war-with-china-is-bitcoins-do-or-die-moment>
39. <https://cointelegraph.com/news/crypto-vs-cash-which-countries-expect-to-go-digital-soon>
40. <https://cointelegraph.com/news/crypto-startups-still-raising-millions-in-capital-despite-ico-decline>
41. <https://observer.com/2019/08/art-market-sharing-economy-digital-vive-snark-art-noow/>
42. <https://cointelegraph.com/news/biggest-crypto-hedge-funds-and-what-they-tell-about-the-market>
43. <https://www.brinknews.com/blockchain-promised-a-revolution-itll-have-to-clear-three-governance-hurdles-first/>

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

For more information and updates visit

blockchain-quarterly.com

Blockchain Quarterly is published by BQIntel, a data and analytics company, providing blockchain intelligence & insights for businesses. Blockchain Quarterly is part of our yearly subscription service. For more information on how to receive Blockchain Quarterly, request permission to republish content, or comment on content, please email us at research@bqintel.com.

Please see www.bqintel.com to learn more about our products and services.



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.

© 2019 bqintel. All rights reserved.