Volume 1 | Issue 1
11 November 2018

The State of Crypto

Industry analysis

Welcome to the first State of Crypto report 1/2018 by Argentas

Introduction

This report has been prepared as a general overview of the current state of the crypto industry and is not a sell or buy recommendation of any particular cryptocurrency, token, other digital asset or blockchain startup or other related company. The report is for sharing thoughts and ideas with anyone interested, to spread information, incite discussion and provoke debate about these very interesting topics, where many issues indeed must be subject to vigorous debate to be able to take them forward – definitely, more information is generally needed for people to fully understand this new and fascinating area of financial technology that has vast potential to improve lives globally.

This report does not go through the bitcoin or blockchain basics, as there are plenty of existing sources for such educational purposes, but critically observes and discusses the current state of the crypto sector with a focus on a few current topics, and outlines the some future directions for development. As this nascent technology moves and evolves fast, the scenarios may change fast, and the views presented in this report may turn out to be obsolete; however, it is likely that certain fundamental long-term views based on economic, financial and commercial realities will remain valid.

Executive summary

This report will discuss the following topics:

1. **Current crypto market situation – market stagnates: what are the reasons behind**
2. **Decreasing retail interest, growing institutional investor interest in crypto assets**
3. **Status of the ICO market for project funding – is the boom over?**
4. **Global loss of privacy: the potential of privacy-oriented cryptocurrencies**
5. **The competition for the world's payments – crypto vs. traditional solutions**
6. **Bad public policies and economic mismanagement driving crypto deposits**
7. **Regulatory approach: not wise to kill the goose laying the golden eggs**
8. **Crypto valuation – monetary economics vs. tokenomics**
9. **The winning blockchain startup: building ecosystems from the ground up**
10. **Will bitcoin remain, or will it be the "*Sony Betamax vs. VHS tape*"?**

Brief conclusions are presented at the end of the report. By no means is the coverage of these immense topics complete, as it only raises a few points regarding each of them.

The Argentas Team invites the readers to give their feedback, ideas and thoughts to advance this common cause of taking the crypto industry forward via the social media channels of Argentas at Twitter, Facebook and Telegram – all links are available on the Argentas website at argentas.io.

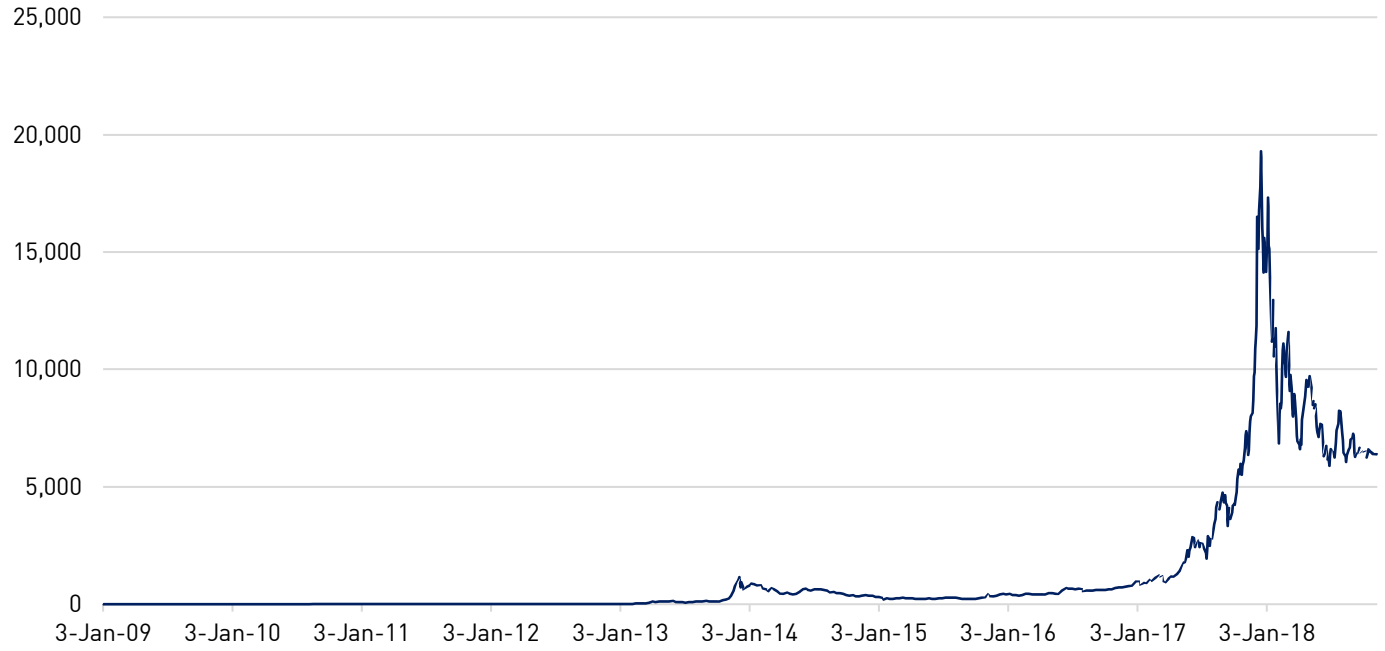

Chart 1: Bitcoin (BTC) USD price lifetime chart 3 Jan 2009 – 10 November 2018. Bitcoin price chart approximates the general market cap development of the cryptocurrency market, showing the sharp increase in 2017 and the equally sharp downfall in 2018; it should be noted that most of the current cryptocurrencies did not even exist before 2017 and 2018, when the number of listed cryptocurrencies and tokens have multiplied. Data source: Blockchain

1. The market is stagnating

Market down by ¾ in 2018

While the total market capitalization for all cryptocurrencies increased 33-fold during 2017 from USD 17 billion to USD 565 billion, in contrast to that, in 2018, the market capitalization has fallen by more than ¾ (77 percent) from the January peak of USD 831 billion down to ca. USD 192 billion in mid-August 2018 and remained around the level of USD 200 billion ever since (Source: Coinmarketcap).

Chart 2: Bitcoin (BTC) USD price chart 11 November 2017 – 10 November 2018. The price chart for 2018 demonstrates the decline from the peak of USD 19,499 down to the USD 6,000 level, where the price has remained over the past several months. Data source: Blockchain

Abnormally low volatility

While the market volatility was normally very high with 5-15 percent daily average, even with higher peak volatility levels occasionally experienced, recently, the volatility has dropped down to 1.1-1.6 percent over the past 30 days, as shown in Chart 3. This is abnormally low compared to the normally experienced levels of crypto trading volatility, also signaling a bear market with much less interest from traders.

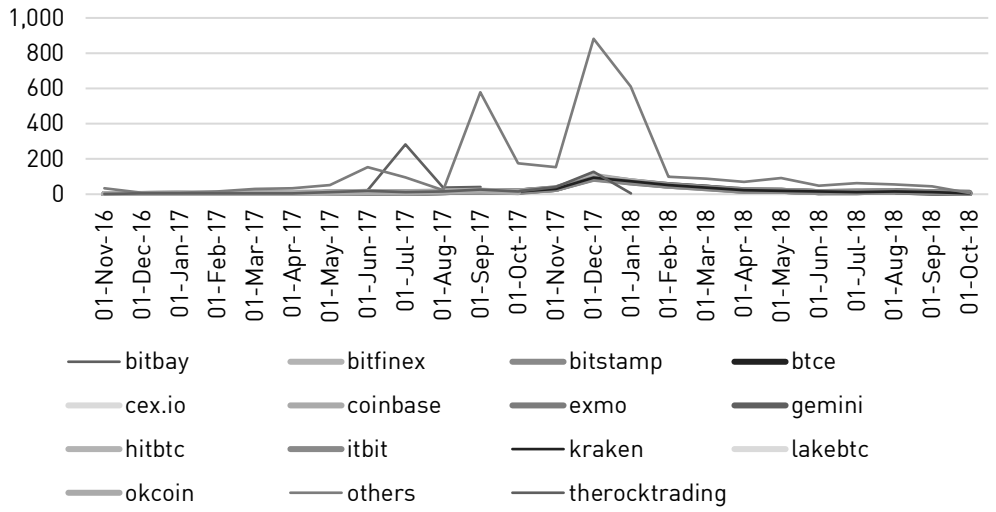

Chart 3: Bitcoin (BTC) USD trading volatility in major bitcoin exchanges for the past 2 years 11 November 2016 – 10 November 2018. The BTC trading volatility chart shows the dramatic increase in volatility in late 2017 and early 2018, as well as the decrease in volatility in line with the fall in the cryptocurrency market prices during 2018, implying a bear market with much less interest. Data source: Bitcoinity

Exchange trading volumes down by 80 percent

In many cryptocurrency exchanges the trading volumes have dropped even by 80 percent since December 2017 peak levels, signaling the fact that the interest towards cryptocurrencies has vastly diminished from the 2017 year-end frenzy, and the trading volumes have correlated very closely with the changes in the market capitalization, apparently having decreased approximately as much as the total market capitalization in percentage terms.

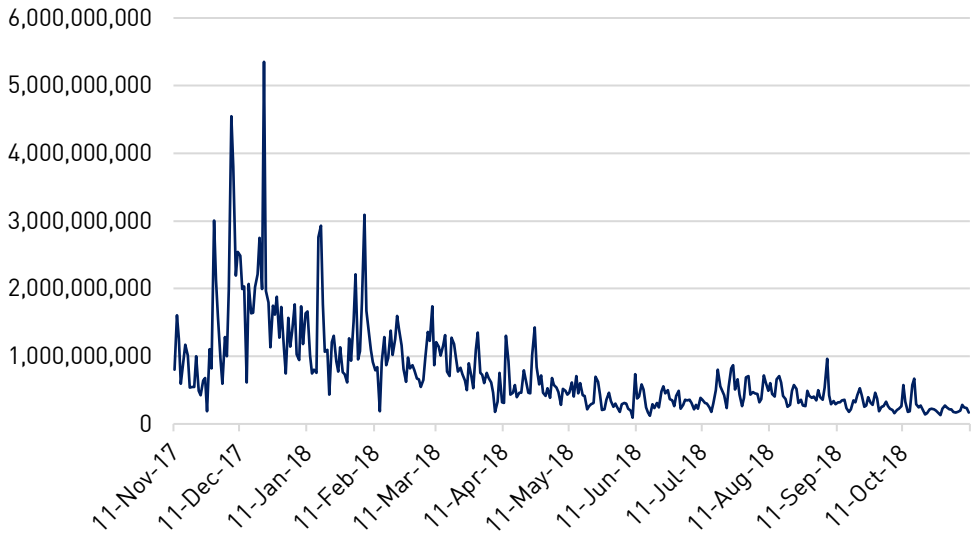

Chart 4: Bitcoin (BTC) USD trading volume in major exchanges 11 November 2017 – 10 November 2018. The BTC trading volume chart shows the dramatic peak in late 2017 and early 2018, as well as the gradual decline in the trading volumes in line with the fall in the cryptocurrency market prices during 2018 – when

the market capitalization decreased by almost 80 percent, the trading volume also fell by 80 percent during the same period. Lower trading volume and less active participation makes price formation less effective and affects the market recovery as well. Data source: Blockchain

Altcoins and tokens falling more than bitcoin

Many of the tokens sold in ICOs have lost even more of their value, 90-95 percent, some even all. This is also exacerbated by the combination of facts that most of them were very thinly traded, and when the projects cannot deliver any results that fast with any positive news maintaining interest and valuation, given that they were only starting to realize the plans presented in their white papers after having obtained funding, the token may completely crash regardless of whether the underlying project has any real substance or not. Additionally, ICOs have been plagued by the fact that there indeed have been many projects that were not solid at all, without any real substance, and some outright scams[1], which affects the general perception of all tokens, even if such bias based on a few bad ones is indeed not merited to be excessively generalized. To the contrary, under more difficult circumstances, the average project quality is expected to increase, since it is much more difficult to obtain funding, and projects on shaky grounds are less likely to succeed.

Return of bitcoin dominance

This relatively stronger fall of the token prices compared to the bitcoin price has also led to the recalibration of the so-called "bitcoin dominance" position, where the bitcoin share of the total market capitalization dropped to 1/3, or 33 percent, at the peak of the market, when many altcoins and tokens considered "hot" had their value inflated, thus pushing down the relative share of the bitcoin, also due to the fact that there are around 2,000 other cryptocurrencies or tokens than bitcoin, so such evolution was inevitable. However, when the tokens and altcoins lost relatively more value than bitcoin, the bitcoin has returned to its absolutely dominant position by a valuation that corresponds to more than half of the total crypto market capitalization, currently 52 percent.

Crypto exchanges getting squeezed

This market downfall during 2018 makes the life very difficult for many crypto exchanges, which will lead to a situation that many will have to either consolidate, combine with others and cut costs, or close down their operations altogether, if there is no sustainable volume to support ongoing operations. Many layoffs by major crypto exchanges such as Kraken as announced[2] signal that the recruitment trend of 2017 has also been reversed, when the exchanges will have to cut costs and improve the efficiency of their operations. Consolidation and shakeup of this nascent sector will be inevitable: it is likely that there will be fewer and on average bigger exchanges as a result of this coming consolidation period.

Similarities with the peak of the Internet bubble 1999-2000

There are significant similarities between the burst of the crypto market bubble in 2018 as there were almost 20 years ago – two economic cycles in between – in the burst of the Internet bubble at that time. While many crypto enthusiasts are too young to remember that or the youngest ones not even born back then, the overheating of the market was very similar, and the causes for the downfall equally similar.

---

[1] According to data provided by ICO Bench in their September/October 2018 ICO market report, ca. 11% of funding raised has represented such dubious projects, which is much less than many generalized headlines try to suggest, only one in ten

[2] Bloomberg reported on 6 September 2018 that Kraken lays of 57 employees, representing ca. 10% of their client services team. At the same time, Kraken insisted of growing up to 1,000 employees by year-end.

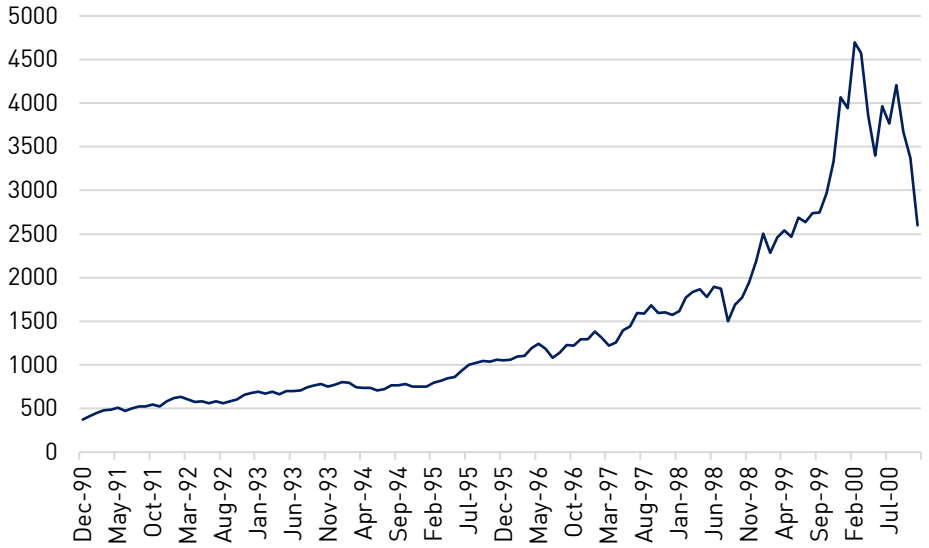

Chart 5: Nasdaq composite index November 1990 – November 2000. The bursting of the Internet bubble in spring 2000 looks very similar to the fall of the crypto market as from January 2018: initial market expectations did not match the underlying reality, but it took several years for those to materialize, but, at the same time, the most successful Internet companies ended up more successful than anyone could have ever imagined. Data source: Yahoo Finance

When it was thought back then that Internet can turn everything into gold in terms of the value of Internet startups, it was gradually discovered that it was too early for any serious Internet business to materialize at that time – it took a decade from the fashionable Nokia "WAP" early Internet phones to the modern smartphones via the leadership of Apple with its successful iPhone product: only in the late 2000's and early 2010's the world of mobile internet started being real. Even if the foundations for the success of some of the world's most successful Internet-related technology companies such as Amazon were laid back in late 1990's, it took a fairly long period after the initial bubble for the potential to start materializing. The cycles are getting shorter and shorter, however, so for the blockchain technologies to cause a material impact through real-life applications, it is expected to take clearly less time than what happened between the initial Internet boom and the business to actually materialize.

A key discovery here is that the best Internet startups and those transformed into Internet era companies, currently often known as FAANG, Facebook, Amazon, Apple, Netflix and Google, became incredibly strong and powerful indeed, when they built strong platforms and the time was ripe for their products and services to scale up. The same is likely to happen for the best blockchain and cryptocurrency startups leveraging distributed ledger technologies.

For the winners, it is important to adapt a long-term view and be patient, persistently focusing on the continuous development of the platform in question. Short-term focus will lead to failure. Any previous cycle demonstrates that the transformation will not happen overnight, but when it starts happening, it will gain momentum really fast, so there is no time to be lost despite of the currently bearish crypto market.

Current lack of operational use cases

Now, in the crypto market, it has been equally discovered that the underlying business, the economic activity justifying value, is not yet there, and for many observers, there is no clear view, no clear outlook for that either, how it would eventually happen. The current lack of use cases – not in the sense of having a lack of potential for really transformative and revolutionary use cases, but the lack of current real business applications of those technologies to generate real revenues and/or cost and time savings is one of the reasons behind the slowing down of the market. This is always related to the impatient nature of the market that discounts expectations at any given

moment into the price, however ambitious they may be: first, everyone gets so excited about the wonderful potential in the blockchain industry, and almost every asset in the sphere initially reaches an excessively high valuation, regardless of the individual asset quality (because many people look at the entire "space" rather than individual assets, making bets based on the generic view, and, at the same time, there are often insufficient data, technological competence and suitable financial tools to make any reliable assessment of an individual project) and then people awake into the reality, when they start estimating and calculating the cash flows or using other methods to justify the valuations: the business is not yet there, so the formulas end up being empty of content, the high valuations not being justified, and the market deflates.

Then, when the market starts realizing that there is very little current economic and commercial use of the technology, and no cash flows, no revenues are being generated by anything else than the startups facilitating transactions to buy and sell those digital assets themselves: the crypto exchanges. If the most prominent 'decentralized application' is the famed Crypto Kitties application on the Ethereum blockchain, where people can acquire and trade virtual pet kitties in the form of virtual collectible cards[3], this also tells much of the status of the underlying crypto economy: the real, serious activity is not yet there.

This is again a parallel situation compared to that of the Internet boom of the late 1990's: there was a lot of excitement but little actual commercial use. The business, the volumes were not yet there. The market had to crash first, and the less solid ventures with less or no substance fail in the aftermath, and the strong ones remain and emerge. Wheat had to be separated from the chaff. This is what is happening, and what will happen in the crypto market as well, now that the phase of the initial hype has passed.

There is no doubt that the best blockchain startups will equally rise to prominence – those with real substance – when the real commercial application of that technology starts gaining pace. Potentially, that can be quite soon. When this starts happening, the value of the strongest and best cryptocurrencies and blockchain startups will be reaching very significant levels, when the real-life applications and their scalability can be detected.

Even without use cases, USD 200 billion market cap ridiculously low

If it is considered that the total value of money in the world is around USD 37 trillion (narrow money i.e. world's coins, banknotes and checking deposits) or USD 90 trillion (broad money i.e. the previous plus saving and time deposits and money market accounts)[4], and that of gold around USD 8 trillion, the cryptocurrency market capitalization is ridiculously low, compared to what it can represent as the future form of truly digital money. For it to be in any logical proportion as the "currency/currencies of the Internet", the value of the cryptocurrencies should be many times over the total market capitalization today. To get it where it should logically be, it may take the emergence of entirely 'unborn' cryptocurrencies of the next generation, as well as the natural growth of the underlying crypto economy to increase the absolute and relative share of the cryptocurrencies among the world's currencies.

Even the EU report on virtual currencies expects them to seriously compete and even substitute fiat currencies in the future: "*One cannot rule out that future progress in the*

[3] A buyer paid ETH 600 or ca. USD 170,000 for the most expensive Crypto Kitty "Dragon" even in September 2018, after the boom period, based on Crypto Kitty data on the Ethereum blockchain. Source: thenextweb

[4] The Money Project (http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/)

area of information technologies can bring even more transparent, safe, and easier to use variants of VCs. This might increase the chances for VCs to effectively compete with sovereign currencies, including the major ones."[5] When the virtual or crypto currencies achieve that to more significant extent, it is obvious that their relative and absolute valuation is at an entirely different, higher level compared to today's market capitalizations.

Success of startups building the trading and mining infrastructure

If the current market capitalizations of cryptocurrencies and the valuations of the most successful startups in the area are considered, after bitcoin, Ethereum and ripple USD 111, 22 and 20 billion[6], respectively, the next ones in the list would not be cryptocurrencies but actual businesses in that area. Bitmain, the manufacturer of mining equipment i.e. computers dedicated to cryptocurrency mining, is valued at USD 18 billion in its planned IPO[7]. The largest cryptocurrency by trading volume Binance expects a profit of USD 500 million to USD 1 billion in 2018[8], which would indicate a multibillion valuation. Coinbase, the largest US cryptocurrency exchange, was valued at USD 8 billion in its latest fundraising round of USD 300 million in October 2018[9]. This demonstrates that the only actors in the sphere that have so far attained significant valuations are those that have provided the infrastructure for the cryptocurrency-related transactions in terms of mining and exchange activities, which activity attracted vast numbers of users and clients at the peak, but has gone down in both respects too: both the trading volumes and the sales of mining equipment have dramatically decreased from the peak levels around the turn of the year. It may be that some of those valuations have already decreased, as the forecasts have also gone down from the peak levels, directly affecting valuations calculated on the discounted cash flow basis. As it is seen that cryptocurrencies and other applications of blockchain technologies are here to stay, the valuations of the major players in that sphere are likely to remain high despite of the current bear market, because they have established very strong positions, and are likely to be able to reap the fruit, once the market picks up again.

Market stagnation leading to consolidation and failures among exchanges, mining equipment providers and mining farms

Now, however, as the market is stagnant and valuations are down (also affecting mining revenues in the same proportion, squeezing margins), and the market for crypto exchanges and mining equipment providers already crowded, it is not likely that entering such market would be a wise move at this point in time. While the situation may change, if the market starts growing again in terms of trading volume and valuations, now it is rather the time for consolidation and cost cutting in that area. Again, it is likely that there will be fewer and larger players, when the dust settles. The strongest ones have been those that were founded early on in the crypto market cycle such as Coinbase and Binance among exchanges, and Bitmain in mining equipment. Now, given the concern for massive electricity consumption of cryptocurrencies being "mined" because of their their proof-of-work or proof-of-stake protocol-level approach to resolve complex mathematical challenges to 'prove their work or stake', it is likely that new, successful cryptocurrencies will be less of those mined, or

[5] "*Virtual currencies and central banks monetary policy: challenges ahead*" European Parliament July 2018

[6] According to Coinmarketcap on 11 November 2018

[7] "*Crypto Unicorn Bitmain Weighs $18 Billion IPO, One of World's Largest*", Coindesk on 21 August 2018

[8] "*World's Largest Crypto Exchange Eyes $1 Billion Profit Amid Rout*", Bloomberg on 6 July 2018

[9] "*Coinbase Hits $8 Billion Valuation After $300 Million Raise*", Coindesk on 30 October 2018

structured so that mining will not be consuming such excessive amounts of energy. This will then require the mining equipment providers to adjust as well, which will lead to consolidation, failures (which may already occur due to the dramatic decrease in units shipped and prices dropped due to the market fall, with the lower cryptocurrency prices making mining much less attractive as shown in Chart 6 below, because it is already dominated by powerful mining farms that make it very hard for any individual miners to gain anything material at all) and due to emergence of new types of players. The same that is happening to exchanges and mining equipment providers is likely to happen to mining farms too: in many places, operations were set based on an expectation of the bitcoin price around USD 10,000-20,000, and now, the price has stagnated around USD 6,000 with no material improvement in sight. When the cost of mining a bitcoin is currently estimated at around USD 5,000 per bitcoin in countries such as USA, Russia and Iceland[10], it may still be slightly profitable at the current levels of USD 6,000 per bitcoin, but the margins have dramatically fallen from the peak levels, and any business plan based on the peak levels is doomed to fail.

Chart 6: BTC mining revenue in USD - the total value of coinbase block rewards and transaction fees paid to miners 11 November 2017 – 10 November 2018. The mining revenues of miners have equally suffered, when BTC price has come down, decreasing attractiveness of mining, and, subsequently, decreasing the sales of mining equipment that has suffered in similar proportion, putting pressure not only on the mining equipment volumes but also prices, which is a very difficult combination for companies like Bitmain.

No success among projects building on other existing blockchains

At the same time, it can be observed that none of those projects that conducted a successful ICO building an application or other product or service upon an existing blockchain, mainly Ethereum, is among the top blockchain startups. It can be questioned, if that will ever be the case, to be successful in building upon an infrastructure that itself is flawed like Ethereum. So far the fact is that no one has been successful beyond the initial fundraising – the only successful startups have either built their own blockchain and cryptocurrency, or a real infrastructure for the crypto industry such as crypto exchanges and mining equipment manufacturers as mentioned. Again, the most successful application on the Ethereum blockchain has

[10] "*Here's how much it costs to mine a single bitcoin in your country*" Marketwatch/Cryptowatch on 11 May 2018, with the cost per bitcoin mined ranging between USD 531 and 26,170 between countries

been the Crypto Kitties virtual card collectible application, demonstrating that there is no serious commercial activity on those blockchains like Ethereum. So successful blockchain startups are not those leveraging existing blockchains, but those building their platforms and products and services from the ground up, which is the harder way, but the only way to be successful. That must be the focus of successful startups: build in from the ground up, with persistence and with a thorough quality.

2. Retail investment down, institutions coming in

2018 crypto bear market and losses suffered have led to retail investor exit

Market statistics also tell that the fall in trading volumes is correlated with the dramatic fall in the retail investor interest in cryptocurrencies, also signaled by the decrease in related google keyword searches, as shown in Chart 7 below. Those who only entered the cryptocurrency market at the peak of December 2017-January 2018 and made their purchases then, have nursed heavy losses, especially, if they bought at the peak and kept their holdings all the way.

While many retail investors have exited the crypto market after a very short experience that may have been very successful, if they have participated by mid-2017 or before, but if they only entered the market at the peak December 2017 – January 2018, their experience is likely of having been painful, lowering their interest to return to the market, especially, when the market currently lacks momentum.

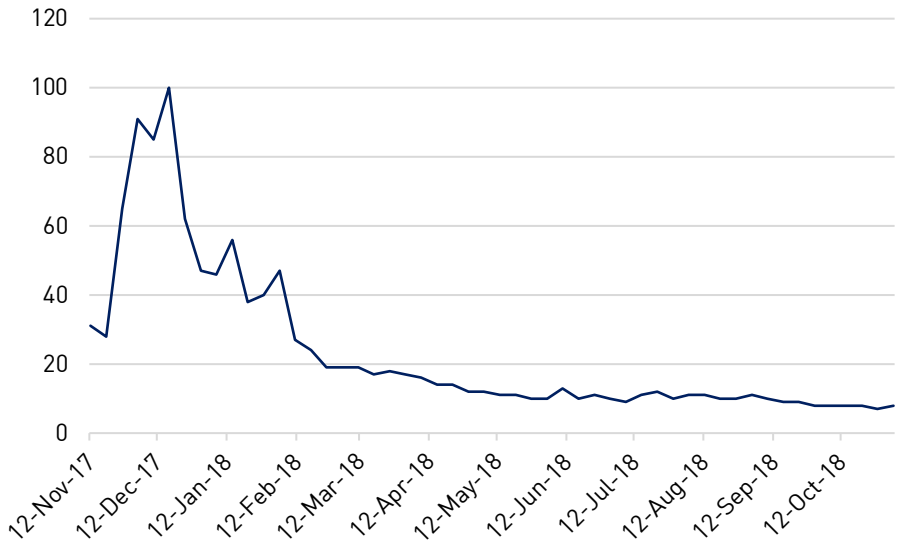

Chart 7: Google 'bitcoin' keyword searches 11 November 2017 – 10 November 2018. Relative scale, with 100 indicating the peak level of interest: as it can be seen, the level of interest has decreased by more than 90 percent.

The year 2018 has offered many short-term opportunities for active traders to benefit from occasional momentum up or down, but to be successful in such swings requires very active market monitoring and trading skills to benefit from it; for any buy-and-hold investor the year 2018 has not been beneficial at all, other than in some very time-sensitive situations that may have offered opportunities to acquire cryptocurrencies at levels that still remain profitable up to date, but as the market is not showing any signs of improvement, there is no current attraction to join the market either: according to Coindesk research, ca. ¾ of survey participants thought that it is possible to become a

crypto millionaire in 2017, but in 2018 only a very small percentage of participants thought so.[11]

There is a certain smaller segment of those who have been present in the market for several years and have got used to substantial swings, and those that have holdings acquired several years ago and may have cashed them in at least partially to reduce their risk exposure, still have a very strong, positive net position, but such group is smaller than the vast volumes of retail buyers that were attracted by the boom towards the end of 2017.

Institutional investor interest increasing

Contrary to the at least momentarily decreasing retail investor interest, the interest of institutional investors towards the crypto market has been on the increase. From an institutional perspective, the crypto asset class is seen as an interesting new area of growth that also functions as a tool to diversify portfolios into this entirely new asset class.

If and when significant institutional money starts pouring into the market, the valuations of crypto assets are likely to increase, because the demand for such assets that qualify for institutional purchases (directly or through various instruments such as crypto and index investment funds, and derivatives products) will put upward pressure on the prices, and since the market size is fairly small, that pressure can have impact very quickly on the valuation levels.

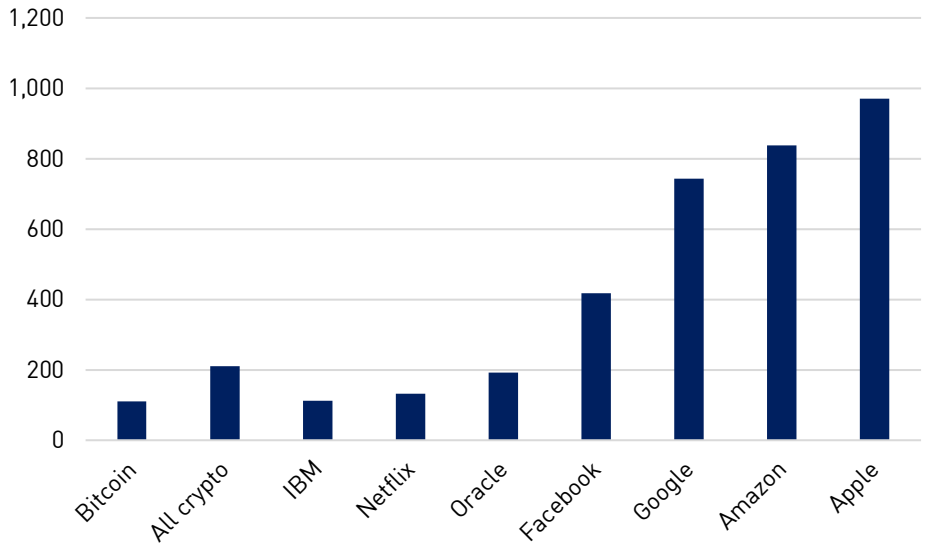

Chart 8: Bitcoin and total cryptocurrency market capitalization in USD billion vs. market capitalization of the FAANG and IBM, Oracle. To put things into perspective, bitcoin and the total cryptocurrency market capitalization can be compared to those of the FAANG and other similar market capitalizations: as at 11 November 2018, bitcoin market capital virtually equals that of IBM and all crypto is very close to that of Oracle, some of the major technology companies of the past generation. Data sources: Coinmarketcap, Yahoo Finance

It must be noted that the current total market capitalization of all cryptocurrencies, around USD 200 billion, only corresponds to the total market capitalization of a single global corporation like Oracle (as shown in the Chart 8 above) that is very large but not among the very largest in the world. While the total crypto currency market

[11] "*The State of Blockchain Q2/2018*" by Coindesk

capitalization in the beginning of the year ca. USD 830 billion was close to par with that of the largest corporations in the world like Amazon, or corresponded to the total money supply of a mid-sized country like Spain, now, the figures are again much smaller. This also poses limitations to institutional investors, when the whole asset class is only USD 200 billion, and half of it, more than USD 100 billion, is a single asset, bitcoin, with the top ten taking about 4/5 of the combined market capitalization, leaving only USD 30-40 billion to be distributed among the 2,000 other cryptocurrencies and tokens.

There are significant challenges, however, to reach wider institutional market participation. Due to being regulated and also subject to strict internal investment and compliance rules, there are several hurdles that need to be overcome for crypto asset investment to be possible for institutional investors.

Institutional concerns

Institutions' concerns relate to issues such as (i) lack of regulation and unclear status of cryptocurrencies, tokens and other related digital assets, (ii) need for secure custody and storage that meet institutional compliance requirements, (iii) limited number of institutionally acceptable crypto exchanges and other marketplaces to be able to access them, relating to both to the custody issues (institutional capabilities), quality of client KYC/AML processes and the regulatory status of such exchanges (also depending on the country of the institution and the exchange, as there are significant differences), (iv) need for institutionally acceptable, robust crypto asset storage solutions, and (v) the overall need for reliable information and improved level of understanding and education on crypto assets among institutional investors; and also, (vi) the lack of existing crypto investment products such as institutionally acceptable crypto investment funds and ETFs (Exchange Traded Funds, a form of securities index product reflecting the value of an underlying basket of assets, often synthetically via derivatives positions) lowers the institutional appetite. Equally, (vii) the limited amount of quality derivatives products on crypto assets to both hedge i.e. protect a position and to take synthetic positions in crypto assets affects the institutional investment activity in such assets. Some have also been concerned of the fact that (viii) if a blockchain holds some transactions that have been used for illicit purposes, then the whole blockchain might be seen as 'tainted', but that is maybe too far-fetched, because then one could not touch e.g. bitcoin at all, as all bitcoin transactions since its genesis have been stored in the same blockchain – it would be the same as to think that one cannot touch a banknote, if any illicit payment has ever been made with it, which is impossible to trace, so, in parallel, the argument about a blockchain being 'tainted' because of a single transaction demonstrated being illicit is not of realism.

Vast opportunity for institutional crypto products and services

Many actors have recognized this fact and turned this challenge into opportunity, and have built or are building up products and services to cater for the institutional needs in terms of having access to crypto asset investing that is compliant with institutional requirements. Each of those areas that remains a challenge is an opportunity, and there are a number of actors, among both the crypto exchanges and similar crypto financial services providers, and the traditional players (such as Fidelity, one of the world's biggest fund managers, launching crypto asset trade execution and custody services[12], and Bloomberg, the leading financial information provider, launching crypto asset indices[13]) that have launched or indicated that they will launch services intended

[12] "*Fidelity launches new company for trading and storing cryptocurrencies*" Reuters on 5 October 2018

[13] "*Bloomberg and Galaxy Digital Capital Management Launch Cryptocurrency Benchmark Index*", Bloomberg on 9 May 2018

for institutional crypto investors. Increasing availability of necessary services that guarantee sufficient levels of compliance in order to avoid any legal risks that may otherwise exist will help to substantially increase institutional investment in crypto assets, and the more there is money pouring into this new asset class, the more there will be upward pressure on crypto asset prices.

The debacle around ETF acceptance

In 2018, there has been lot of movement back and forth around the acceptance by the ETF product by US SEC. A number of fund promoters have applied, and some applications have been rejected in September 2018, while the process continues[14] – the most well-known applicant has been the firm of the Winklevoss twins, who enriched themselves with claims made to Facebook, and used part of that money to buy bitcoin very successfully, becoming, at least momentarily, one of the first public faces of bitcoin billionaires. It is known that the crypto assets are here to stay, so it is inevitable that there will be a need to package such assets into different investment products in order to facilitate access and exposure to such assets but in a way that is simpler than acquiring crypto assets via crypto exchanges and holding them in dedicated wallets with their own cryptographic keys. ETFs and other crypto fund products, when approved, will equally cause significant amount of funds to flow into the crypto asset market, as the investor access will be so much simpler and often only necessitate a few clicks on an online bank or fund manager website to make such fund share purchase, without the hurdle of accessing such crypto assets directly, where the holding, unless permanently through a crypto exchange, will often require a number of separate wallets with separate sets of cryptographic keys to access them, which would all need to be securely stored. When money starts flowing into crypto fund products such as ETFs, it can be expected that significant volumes of crypto assets are either directly or through derivatives acquired by such funds, thus putting considerable upward pressure upon crypto prices.

One of the reasons of the crypto market having remained on a holding pattern is the market participants holding their breath, whether any of these ETF proposals finally gets accepted, as it would definitely result in a boost for the market sentiment and momentum, opening up the gates for very significant additional crypto investment. If there is e.g. an ETF tracking a number of crypto assets, any such fund will need to either buy such assets in the same proportion as described in the product rules, or build synthetic positions in such assets using derivatives (derivatives exist only for a very limited number of major cryptocurrencies, which would limit investment into them in such cases so far). Even the major institutional players such as the global investment bank Goldman Sachs are exploring the idea of entering the market for crypto derivatives.[15]

Room for smaller, trading-oriented crypto hedge funds – long-only funds failing

In 2018, the number of crypto-oriented hedge fund startups has also been higher than ever before, with soon 100 of having been created this year and more in the pipeline, accounting for and estimated of 20 percent of all types of hedge fund launches already[16], and while there has not been any possibility to succeed with any 'buy-and-hold' investment strategy so far in 2018 (only funds that started around mid-2017 at the latest may still be successful with such a strategy, but if the current bear market continues that may not be sustainable either), there have been plenty of very short-

[14] "*SEC Moves to Make Decision on VanEck-SolidX Bitcoin ETF Proposal*", Coindesk on 20 September 2018

[15] "*Goldman Sachs Exploring Crypto Derivatives, Says COO*" Cointelegraph on 20 June 2018

[16] "*Crypto Hedge Fund Launches Are Soaring to Record Levels This Year*" Coindesk on 10 October 2018

term trading opportunities, so it is possible to succeed with an opportunistic short-term trading strategy that may also be algorithmic, machine-driven. The challenge is, however, that the market is limited in size and may be shallow without any sufficient depth, especially concerning anything else than the most liquid cryptocurrencies like bitcoin and Ethereum, so no large-scale operation exclusively focusing on crypto trading is likely to be successful, but the fund sizes at this stage will need to be fairly small to "fit" into the market, given that the whole asset class is no more than USD 200 billion, with one asset, bitcoin, taking up more than half of it.

High-caliber institutional personalities joining the crypto world

Increasing institutional interest and acceptance is also demonstrated by personalities of the highest institutional caliber such as the former President & COO of Goldman Sachs and former Director of US National Economic Council Gary Cohn joining a blockchain startup as an adviser in October 2018[17], and Sheila Bair, the former chair of the Federal Deposit Insurance Corporation, also having joined a board of a blockchain startup focusing on a stablecoin[18], among a number of others, showing that the segments that have been the most critical towards crypto assets i.e. institutional investors and representatives of various government agencies or central banks are also going past that phase of rejection and entering the phase of acceptance (many grudgingly, such as Jamie Dimon of JP Morgan Chase[19]) as crypto assets are here to stay, and for a reason, with the most dynamic among them seeing the opportunity in the crypto sphere and accepting it. Who would have believed still in 2017 that such personalities, and more, join the cryptocurrency bandwagon – and choose, like Gary Cohn, a blockchain startup before any other more 'conventional' Fintech startup? Times are changing, and all this shows, with (a) institutions coming in, and (b) most senior bankers, financiers, regulators and other government officials giving favorable, supportive comments about the blockchain industry, and (c) even getting personally involved in such enterprises that the industry has reached a certain level of 'maturity' as it starts being accepted by such institutional figures. This means, at the same time that despite of the market slowdown, the efforts to build these businesses indeed must not slow down, because the faster the infrastructure is operational, the faster it can be filled with new business, economic activity and result in new digital wealth.

3. ICO boom loses steam but continues

One of the smartest and best financial innovations of recent times to fund projects

Initial Coin Offerings, or ICOs, are an excellent new way to fund technology startups perfectly in sync with the spirit of these modern times. The world of finance has in many ways got dusty and rigid, and new innovation is necessary to bring the toolbox up to the speed with today's needs. A project cannot by definition be realized before it is funded, and this innovation provided startup teams with the critical funding tool to make their projects happen. For most ICOs, to be exact, there are no 'coins' that would have their proprietary blockchains, but 'tokens' that have been issued on existing blockchains, for the simple reason that project normally needs to be funded before it can be realized and the blockchain delivered, as stated above, so projects are funded through issuance of tokens rather than coins directly. Therefore, the method should more appropriately be called 'ITO' i.e. Initial Token Offering.

[17] "*Ex-Donald Trump adviser Gary Cohn joins blockchain start-up*" Financial Times on 12 October 2018
[18] "*New York Regulator Greenlights Paxos Ethereum-Based Stablecoin*" Forbes on 10 September 2018
[19] "*Jamie Dimon says he regrets calling bitcoin a fraud and believes in the technology behind it*" CNBC on 9 January 2018

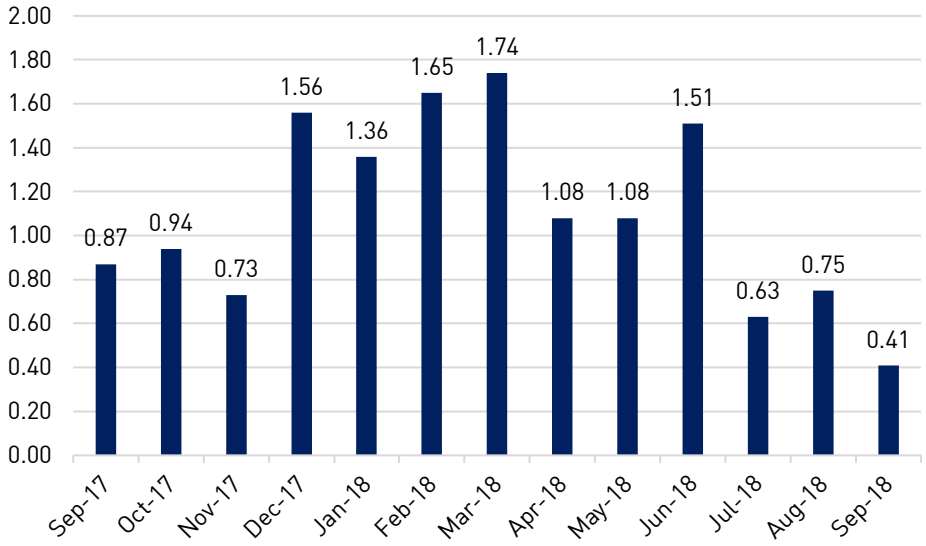

Chart 9: Total funds raised by ICOs in USD billion. Despite recent slowdown and the exceptional amounts raised during the first half of 2018, the monthly total funds raised are still at a high level, with August 2018 corresponding to November 2018, and only September 2018 having been at a clearly lower level. Data source: ICO Bench

In 2018, more funds have been raised than ever before

In 2018, already during the first 6 months of the year, ca. USD 8.4 billion was raised through ICOs, which was more than 2 times higher than ca. USD 4 billion raised during the entire year 2017. Between September 2017 and September 2018, USD 14 billion have been raised, so the year 2018 will by all means be a record year, with USD 10.1 billion already raised, despite the recent slowdown. To date, according to ICO Bench, USD 22 billion have been raised through the ICO method, which by far surpasses the 'traditional' crowdfunding mechanisms, and venture capital investment into blockchain projects as well (while a part of venture capital investment has also taken place in the form of tokens upon participation in ICOs).

Super-sized fundraisings of EOS and Telegram stand out

A handful of mega projects such as EOS that started their ICO in July 2017, raised an estimated total of USD 4.3 billion[20] over a 350-day Dutch action period, averaging about USD 11 million a day after the initial 5-day period with USD 172 million. EOS was successful, because it had a perfect timing at the peak of the bitcoin boom, and since the market value of the listed EOS token on the Ethereum platform kept increasing during the sales period, at times reaching almost USD 22, 22 times its starting price around USD 1, the intake of funds ended up being astronomic. This massive ICO alone was as much as everything raised during 2017, for which that ICO accounts a significant percentage too, as it started in July 2017 and lasted until June 2018. The only other one that reached ten-figure amount was the messaging app Telegram with its USD 1.7 billion pre-token and pre-ICO fundraising round (or two)[21] for its TON tokens that do not yet even exist (through SAFT agreements i.e. Simple Agreements for Future Tokens). At the same time, the Telegram messaging app already had 200 million users and counting, so it had an existing platform upon which to leverage the future TON token and its blockchain platform. Those two projects alone amount to USD

[20] "*Investors Bet $4 Billion on a Cryptocurrency Startup*" Wall Street Journal on 29 May 2018

[21] "*Telegram Raises $1.7 Billion in Coin Offering, May Seek More*" Bloomberg on 30 March 2018

6 billion, and the rest are of far smaller magnitudes and normally amount to less than USD 100 million, with the average being in the low teens or currently even in single digits (see Chart 10 below). ICOs far surpassed the traditional venture capital fundraising volume too. Now, when the ICO boom has lost its steam as the consequence of the general crypto bear market, the relative share of venture capital funding is on the rise again.

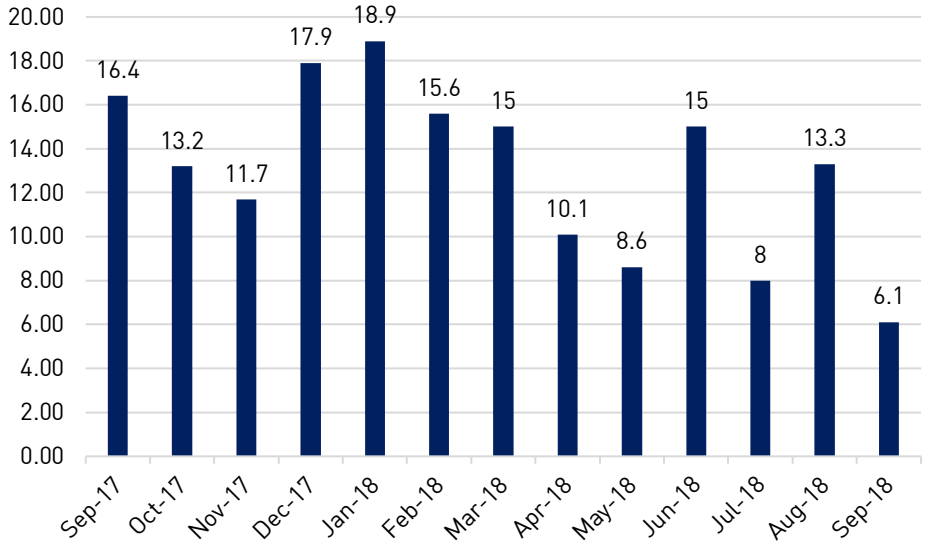

Chart 10: Average funds raised in an ICO in USD million. The average amounts raised through ICOs have clearly decreased lately Data source: ICO Bench

Ban on social media marketing strongly limited promotional tools

FB, Google, Twitter advertising that boosted the ICO market massively in 2017 was all eventually banned in spring 2018, citing too many scams as the excuse and the need to 'protect users from such scams', also taking the steam out of the boom, as no comparable marketing and advertising tools have been available ever since. Some of these bans have been partially lifted to allow legitimate crypto advertising, but no ICOs.[22] Thus ICO marketing remains also technically much more challenging that what it was at the peak of the boom.

Difficult market conditions help weed out the scam

The over-hyped state of the ICO market in 2017 attracted all kinds of actors to participate the market, also the bad ones. There have been some projects that have very bad if any substance, with no likelihood of any viability, and some that were outright scams, with no intention of realizing their proposed plans at all. Now that the market has become again more difficult and that the investor expertise and level scrutiny of projects has also increased, with some crowd and more professional analysis also helping to spot the scams, the difficult market in itself is perhaps the best tool to weed out the scams, as they will have much harder time to attract any interest.

Weeding out the scam will not be limited to those attempting to raise funds through ICOs, but also cover the the service providers, or purported service providers that demand pre-payment in ETH but then deliver nothing as agreed, or steal the identity of

[22] " *Facebook Relaxes Ban, Accepts Some Crypto Ads*" Coindesk on 26 June 2018

a known service provider but then turn out to be entirely other people – when the market gets more difficult, those attempting to defraud by falsely proposing services that they never intend to deliver in marketing, promotion or other support functions to an ICO, are likely to increasingly vanish from the market.

So the end result of the currently more difficult market is likely to be a market of higher quality, also covering its support functions, the small industry that has taken shape around the ICOs. Projects and service providers of quality are likely to rise to prominence, and the scam that could flourish in very easy and loose circumstances, will now be rooted out. Even if the adjustment may be painful, the end result will be better. This pattern is, however, typical to all new and "hot" areas, where visibly mediatized successes that sometimes have been achieved very fast attract also actors that have nothing to do with the actual innovative Fintech entrepreneurship driving the sector, but, as said, they are likely to be filtered out during this bear market.

Normal probabilities of venture success apply: most projects will fail

It is clear that not every project will be successful, and this is what venture capitalists and other experienced startup investors know well. If it is the rule of a thumb that 1 in 10 projects will be truly successful, the same will also apply to blockchain startups. Most of them will either fail or only reach modest or moderate level of success, but some of them will be spectacularly successful: the blockchain industry already features a number of its own 'unicorns' among the best cryptocurrencies and company startups i.e. those with a valuation or market capitalization in excess of USD 1 billion, as also discussed elsewhere in this report.

ICO was essentially a coincidental application on Ethereum platform

It was not in the cards of the creators of the world's currently second largest cryptocurrency by market capitalization[23], Ethereum, that practically the main use and application of the platform has been those ERC-20[24] token smart contracts enabling the functionality of an ICO to accept funds for a certain amount during a certain period in time in exchange for the project's newly issued token. However, to the frustration of Ethereum's creators[25] ICOs indeed have been the main application of the Ethereum platform, and not much anything else. The real "enterprise use" as a "world computer" that Ethereum aspires to be has been minimal, also due to the fact that Ethereum in its current form is slow, cumbersome and expensive, with its capacity being fully used already by these ICOs, demonstrating that the platform is already congested and definitely cannot take any significant supplementary economic activity for any other value-adding use. The success of Ethereum as ICO platform also became its curse in terms of its desired use as an enterprise platform for decentralized applications: it does not have much further capacity for them, as the ICO business sucked up all of that. At the same time, this enabled USD 22 billion worth of enterprise being funded, which was a tremendous boost for the development of the blockchain industry.

Ethereum must be rebuilt – the current flawed version will be redundant

Now, it has been realized that the whole Ethereum platform has to be rebuilt and restructured[26], or one could dump it altogether as redundant – if nothing is done, the network will basically paralyze itself. The question is, what will then happen to all these thousands of ERC-20 tokens, whether they will have any compatibility with the

[23] Current market capitalization of ETH outstanding is ca. USD 22 billion, according to Coinmarketcap

[24] https://en.wikipedia.org/wiki/ERC-20

[25] "*Ethereum's Vitalik Buterin on the bitcoin bubble and running a $125bn blockcha*in" FT on 19 April 2018

[26] "*Ethereum's Next Upgrade Could Be the $29 Billion Blockchain's Biggest Test Yet*" Coindesk on 30 August 2018

future Ethereum blockchain that will be entirely new, in which case it might be better to just launch the new thing separately and let the current Ethereum die as obsolete, because that is what is going to *de facto* happen anyway – for practical reasons, it will anyway be a fork, not an entirely new blockchain. Ethereum was a nice proof of a concept, but real-life demonstrated that it was never conceived to go that far, nor is it capable of going that far, so everything that has been built around it may collapse as well, when the core is taken out and rebuilt altogether. And if the core is not rebuilt soon enough, the internal "*difficulty bomb*" in the source code will be triggered, paralyzing the whole setup for good. So Ethereum has an inbuilt obligation to rebuild itself to stay modern – or die. This is a fact known by anyone into the coding part, but many in the public have no idea, and still, thousands of tokens depend on this platform, which in the worst case scenario will die altogether in an automatic, programmed manner. At the same time, there are so many vested interests that will ensure the new incarnation of Ethereum will indeed be built, so the concern for its continuity should not be exaggerated either.

Technically better ICO platforms than Ethereum exist but are not generally known

Contrary to what many think, Ethereum is not even the best platform for ICOs, unless certain very specific characteristics are needed that the Turing-complete, 'verbose', and very flexible Solidity programming language enables. There are lesser known but better alternatives that would be perfect for most ICOs, but only a smaller number of people are aware of such other options, also given Ethereum's rather dominant "market share" in the ICO market that is more than 90 per cent. One of such better platforms is Stellar, which is cheaper, faster and more secure than Ethereum, where a transaction costs a fraction of a cent (and all transactions cost the same, irrespective of network situation like with Ethereum, where congestion can multiply so-called gas fees), transactions are confirmed in a couple of seconds (against Ethereum's several minutes – hundred times faster), and given the less 'verbose' nature of Stellar's programming language compared to Ethereum's Turing-complete Solidity, there is must less room for any risks that with Ethereum can really be significant, as a number of cases have proven, such as the famous DAO case with USD 70 million theft.[27] So there are much better alternatives around, but since Ethereum gained ground and established its market share, its position as *the* ICO platform with the ERC-20 tokens got stuck to it, both in good and bad. Since the ICO market is now in a slower mode, no new platform for ICOs emerges either, and people practically don't get to know about any other option as more interesting alternatives.

Most democratic funding tool ever

ICOs have also probably been the most democratic funding tool ever, enabling a worldwide, real-time access to a project's funding, open to basically anyone with cryptocurrency at hand. It has overtaken the guarded system of venture capitalism, where an elite group of venture capitalists are offered the best projects on a silver plate, and the small retail investors can only maybe access an IPO years later at valuations that are dozens if not hundreds of times higher than during the initial rounds, but here, the ICO mechanism offers anyone a democratic and open access to venture funding, with the additional benefit of the liquidity of the token, which does not have to be held for long periods like shares that may have to be held for 5-10 years in a venture capital investment before any exit, but can be disposed of at any moment when the token is listed (many list them right away after the completion of the ICO), and as they are neither shares nor other securities of the startup, it is up to the crypto market

[27] "*The Ether Thief*" Bloomberg on 13 June 2017

to determine, how they perceive the token's value vis-à-vis the project that has issued them, as well as vis-à-vis the project's peer group, if any exists. The tradability of the tokens independently of the project is yet another feature democratizing the venture financing process, leaving it entirely up to the token holder, whether he or she wants to stay onboard and follow the development of the project and whether the progress achieved is in any way reflected in the token valuation, or see to an opportunistic moment to dispose of his/her tokens via the marketplace.

Regulators should understand that the ICO is the most retail investor friendly funding tool ever created: direct access to projects, no middlemen, no consulting fees, virtually immediate liquidity, enormous global choice of projects to diversify risk of purchases

The regulators should be happy about these advantages and not try to take them again away from the small people by falsely 'protecting' them – practically protecting them from any opportunity to gain on their investment. There is Darwinian evolution anyway, and if any token purchaser diversifies his or her bets well enough, some of them will yield good gains, some not, but that choice must be left with the token purchaser and not again regulated away, when such a wonderfully democratic and open funding mechanism has been conceived. When regulators and politicians have also tried to push business away from banks, this is exactly it: there is no need for any bank in a token sale, so any attempt to restrict this modern tool would lead to return to the perverse situation of putting the business again into the hands of traditional banks and similar actors, when technology has now taken out the middleman and the costs of the middleman: there is no one between the token purchaser and the actual project issuing them against contribution to the project. This is absolutely ideal in itself, the *state-of-the-art* of corporate finance.

Risks can be smartly managed by limited bets and diversification, not by stifling regulation

Given that the ICOs are to make technology projects possible by having them funded, and only a fraction of all projects will be successful, as is the case with any form of venture funding, they must not be oppressed by any heavy-handed regulation, because the market must be let to determine the winners from losers through the Darwinian evolution driving markets, and any investor must just diversify the bets between many enough projects and measure the bets according to own risk capacity and risk appetite – since one token tends to cost only a few cents or no more than a few dollars, depending on the number of tokens issued and sums raised, the amounts at stake per individual token purchaser can be very small indeed. That is the best means of risk management – the regulators, who obviouslu have no competence in assessing the underlying technological substance of cases any better than an average retail investor, cannot be the ones determining the success or fundability of a project, but the market – and the crowd – must be. Excessive regulation will only lead back to an elitist form of funding, because if the ICOs get banned, restricted or limited, and conditions imposed upon individual retail buyer participation, what that effectively does is to cut out the individual, discriminating them, and leading back to the old system, where access is only offered to professional and institutional investors, who can cherry pick the best projects, and cut out the individuals from all that upside. Then, the individual investors can only buy shares in such companies at their IPOs (not ICOs) years later at a much higher price (and be allocated very limited number of shares), when the venture capitalists, who cherry picked the deal, cash out. That will again lead to the undemocratic situation, from which the ICO was the smart way out: to make project financing finally democratic and globally accessible to all without any middleman, with a very smart liquidity mechanism and risk diversification as well. The smart contract took over from the middleman – this indeed is disintermediation at its best: technology cutting out the waste, and putting the focus on the matter at stake.

Regulation can make or break it – but talent and innovation are mobile

Jurisdictions offering smart and supportive, light touch regulation – or keeping the ICO industry free of any regulation at all – will be the winners in this game of gaining competitive advantage between nations. They will help to create success stories in their respective countries, build new economic activity and generate new tech jobs and wealth through innovation, boosting general economic growth and wellbeing. The fools thinking that everything must be oppressed under regulatory control will once again be the losers, creating complete lose-lose situations, where talent, potential and opportunity will flee and seek more fertile grounds elsewhere to build this high-potential industry. It is indeed a choice that can lead to a lot of success and new wealth, or the loss thereof. The portability of the technology and the mobility of the new generation of talented and skilled people will, however, ensure that they will find new home, where innovation, advanced technology and entrepreneurial success are cherished.

4. Potential of privacy-oriented cryptocurrencies

Scandals of mass surveillance and unauthorized leaks of private data evoke concerns

Recently, the world has awaken to a grim reality with platform businesses and governments abusing their powers and position by amassing limitless quantities of data on individuals in gross breach of their privacy that is a fundamental human right. Sweeping collections of data cannot be justified by governments by giving the eternal excuse of fighting terrorism and other forms of crime; combatting the wrongdoings of a small minority does not justify the reckless abuse of the rights of the majority. Instead, other, more specific means must be developed and applied to focus on known areas of crime (e.g. any groups promoting attacks on innocent people "justified" by a twisted ideology, and anybody participating or sympathizing with such groups), instead depriving everyone of their fundamental rights of privacy by surveilling everyone without any grounds that can be in any way linked to such majority of people. Depriving the rights of privacy is not in any way equal to the promotion of a common good – it is only a form of abuse that must not be tolerated; crime must be rooted out, but that task does not justify the abuse of fundamental rights of everyone, especially, when technology has given better means for that task already long time ago. Equally, when the platform businesses collect data – and have numerous times got caught of collecting data in devious ways hidden from the users that definitely have not been authorized in any terms of use, such as what was revealed in the Facebook data scandal in 2018[28], on which grounds lawsuits have been brought against such platform businesses – the purpose of such data collection is not for any common good but for the purpose of maximizing the profits of such platform businesses, often to enable as targeted marketing as possible, even if it intrudes into the privacy of the individual user in no way acceptable. Both the public and business-driven intrusion into individuals' privacy has gone way overboard and caused a deep indignation: the tide is turning back to a world, where individuals demand their rights to privacy be respected, as indeed should be the case.

Increasing calls to get money back to where it always was: private

Money and the use thereof were much more private in the past than what is the situation today. Was there somehow more crime in the past, when money was cash rather than cards and other online payments? Not likely. The financing of all kinds of

[28] "*Zuckerberg failed to fix Facebook users' privacy concerns*" Financial Times on 17 April 2018

illicit activity has been used as an excuse to spy into everyone's finances and private transactions, but people are not taking that anymore. Everyone cannot be abused on the grounds of what a very small minority does. Today's technology enables highly targeted surveillance, and, in fact, the more advanced the technology is, the less there is any kind of justification for any mass surveillance and intrusion to privacy, because such technology enables more and more surgical surveillance on the suspects on grounds that do have merit, opposite to the sweeping mass surveillance that does not have any justification. Therefore, there should be much greater privacy of the transactions of the vast majority, but there isn't. This has caused a growing demand to put the privacy of money and payments right back to where it should be: to be absolutely private.

Privacy-oriented cryptocurrencies bring back the lost benefits of cash

To tackle this challenge, a number of privacy-oriented cryptocurrencies have been created, and there is a constant development of new cryptographic techniques to guarantee the privacy and confidentiality of transactions. As most of the cryptocurrency accounts (or "public keys") are only pseudonymous rather than completely anonymous, and the transactions in public blockchains are all visible for anyone to examine, blockchain transactions rather diminish than increase privacy, when they are all publicly exposed, so such transactions are by no means acceptable in terms of protecting privacy. An increasing number of new projects is being funded for tackling such challenges.[29]

Required qualities for successful privacy networks

Probably the most well-known among the current cryptocurrencies offering particular privacy features is Monero (XMR), which enable private addresses and private transactions. Another quite well-known privacy-oriented cryptocurrency is zcash. To be successful[30], such networks must be highly decentralized so that any censorship can be attacked through concentrated attacks on any 'central' entity, and there must be active code development to keep it ahead of any risks, good liquidity, large and growing user base, and real ecosystem around it, so that the currency can be widely used. Low liquidity, small user base, lack of ecosystem and lack of active development will cause any such currency lose its edge and usability in protecting privacy.

Privacy-oriented crypto is not for illicit use; the illicit use of fiat is serious indeed

Obviously, the opponents to privacy and promoters of limitless intrusion into privacy would claim that privacy-oriented cryptocurrencies are only used for illicit purposes, but that is nonsense. That is only an excuse to try to break such projects and get users out of them, so that anyone can be spied on. The fraction of fiat money used for illicit activities is always greater, and those attacking cryptocurrencies should clean up any criminality in the use of fiat money before attacking cryptocurrencies that in fact should be ideal for public authorities, contrary to baseless claims made against them, given their very public record of transactions. If there are cases such as the USD 200 billion Danske Bank money laundering scandal[31], corresponding to the current value of all cryptocurrencies together(!), there is a lot to clean up first at the home base of those attacking cryptocurrencies. And, to underline, the Danske Bank case is just one prominent example of illicit use of fiat money among many.

---

[29] "*Paradigm Leads $30 Million Funding for Crypto Privacy Startup StarkWare*" Coindesk on 29 October 2018

[30] "*Cryptoasset Market Coverage Initiation: Valuation*" by Satis Group p. 9, 30 August 2018

[31] "*Inside Danske's €200bn 'dirty money' scandal*" Financial Times on 3 October 2018

The problem is not the illicit use of crypto: the problem is the illicit use of fiat

The total market capitalization of Monero is currently USD 1.8 billion[32], that whole value would only amount less than one percent of the Danske Bank USD 200 billion case i.e. and if it is speculated that if a small fraction of Monero's value were to be used in any illicit transactions that be only a small fraction of one percent compared to the Danske Bank case. That helps to put things into the right perspective: those hysterically attacking the privacy-protecting cryptocurrencies as some kind of nests of illegal activity should perhaps look at the fiat money scandals first and clean those up.

More privacy-oriented cryptocurrencies are likely to emerge in response to demand

It is clear that more privacy-oriented cryptocurrencies will emerge, because people demand to have the fundamental right to privacy restored, and with such cryptocurrencies, it is possible to get closer to the levels of privacy offered by cash – the privacy that crumbled via the proliferation of card and online bank payments.

Since something like Monero can only cater for a very small number of people, given its USD 1.8 billion total value, there must be more and more of such privacy-oriented cryptocurrencies, and the best ones among existing privacy networks will also need to expand their money supply to cater for such growing need.

5. Competition for world's payments

The most obvious use cases of cryptocurrencies relate to payments. That is the core function of any cryptocurrencies, where payments are essentially nothing more than entries recorded in the underlying distributed ledger, the blockchain. And given the globally distributed nature of the ledger among innumerable network nodes, any payment is by definition global and indifferent to any geographical borders there may be between the sender and the recipient of the transaction. The payment, depending on the cryptocurrency used, may be almost free and take place virtually in real time.

Some key characteristics required for a global cryptocurrency / payment network

Anyway, any cryptocurrency aspiring to become the world's currency and the world's payment network should have its transactions to be (i) global (condition easily fulfilled for practically all of them), (ii) virtually free (when e.g. the prices of bitcoin and Ethereum got expensive, also the network mining fees to confirm transactions got every expensive, also reflecting network congestion, so they did not fulfill this condition, but some others do, e.g. Stellar charging a fixed fee that is a small fraction of a cent), (iii) take place in real time (for bitcoin, Ethereum and most 'mined' cryptocurrencies, the transaction confirmation time is not sufficient, being 10 minutes for bitcoin (see Chart 11 below - or 60 minutes for 6 block confirmations generally considered to be 100% safe), and 15 minutes for Ethereum, whereas e.g. Stellar and Ripple have transactions confirmed in 3-5 seconds), and (iv) have a global scale i.e. transaction throughput (where bitcoin and Ethereum cannot handle more than a few transactions per second, and e.g. Ripple and Stellar at least 3,000 and in theory more), with traditional card networks such as Visa processing ca. 60,000 transactions per second globally, meaning that to be a truly global payment network, the scale should be a million transactions per second or more. Nobody has yet achieved that, so the challenge remains to have both a sub-second transaction confirmation time (low latency) and a million transactions per second for a global scale (high scalability).

[32] Coinmarketcap on 11 November 2018

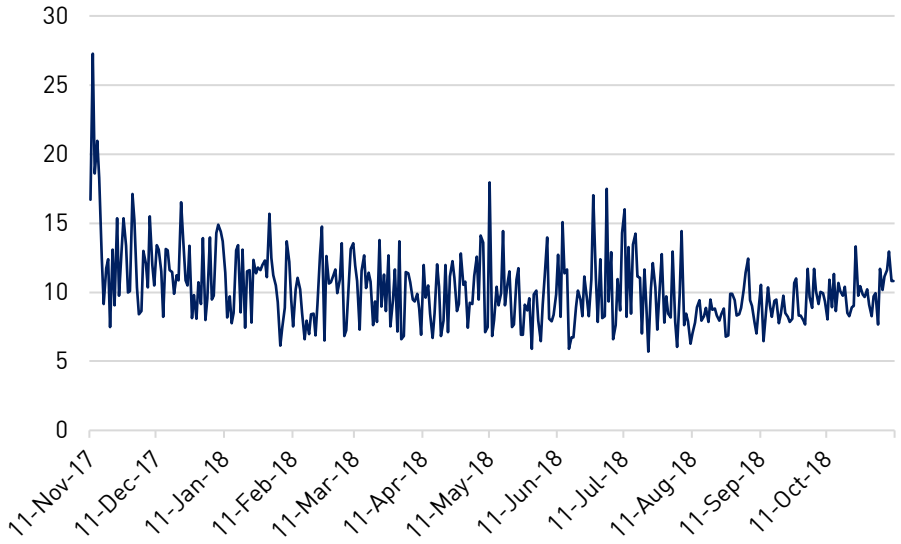

Chart 11: Bitcoin median transaction time in minutes 11 November 2017 – 10 November 2018. Bitcoin transaction confirmation times make it impossible for bitcoin as such to function as the medium of exchange for everyday payments at POS on and offline. Data source: Blockchain

	Bitcoin	Ethereum	Stellar	Ripple
Average transaction confirmation time	60 minutes (6 blocks)	15 minutes	3-5 seconds	3-5 seconds
Average transaction fees	USD 0.6 per transaction	SUD 0.02 per transaction	USD 0.01 for 300,000 transactions	USD 0.01 for 3 transactions
Transactions per second	3 transactions per second	7 transactions per second	3,000 transactions per second	3,000 transactions per second
Consensus mechanism validating transactions	Proof of Work (PoW) - mining	Proof of Work (PoW) - mining	Stellar Consensus Protocol – not mining	Ripple Consensus Protocol – not mining

Chart 12: Protocol comparison. Some key characteristics of Bitcoin, Ethereum, Stellar and Ripple to illustrate the suitability of these different protocols and approaches to the issue of global payments. It clearly demonstrates the speed and scalability advantage of non-mining protocols vs. mining protocols.

Serious structural flaws in major cryptocurrencies; comprehensive revamp needed

While distributed ledger technologies will definitely provide with the solution to the problem of global payments, making the old and outdated global financial 'plumbing' such as the SWIFT payment messaging network, payment card schemes (Visa, MC, Amex and so on), correspondent banking and payment clearing and settlement systems tied to such old architecture redundant, it will need to be taken further to achieve the required global speed and scale. This is one of the very keys in next generation blockchain development, to be able to create such blockchains that are able to function as the world's payment network. Some other projects such as Ripple and Stellar are closer to what is required than bitcoin and Ethereum, as demonstrated in the Chart 12 above, but they have focused their efforts on serving the wholesale operators, the incumbent banks, and one does not cause revolution by subjecting itself to the incumbent actors, whose interest is to suffocate the rise of anything that could in any way weaken their power. They should instead build a direct end user base, but they are afraid of alienating their wholesale clients, which creates a twisted setting that in fact prevents them from achieving the global potential they might otherwise

have. Of course there are further issues such as the fact that Ripple's source code is seriously flawed and even replacing it with two new protocols on top of each other will not remove the problem but only patch it up and transfer it from one part to another – these problems are described in the two academic white papers published on the protocols intended to replace the current Ripple protocol (the new one called Cobalt)[33]; the spat between Ripple and Stellar, which was founded by a co-founder of Ripple and which in turn was initially set up as a fork of Ripple, also signal such issues[34], which Ripple has also tried to deny in the past. It is even scary to see how flawed the three of the world's currently biggest blockchains by market value are: Bitcoin, Ethereum and Ripple, all of which would basically need to be rebuilt from the ground up to make them sustainable. Some work is being done within each of them, because they have recognized the gravity of the situation, respectively, even if they try to keep the problems at a low profile vis-à-vis the larger audiences. Because of the flaws of the biggest blockchains, the opportunity to create a solution for the world's payments is even greater: the more analysis is made and the deeper understanding is gained, the more there are opportunities that present themselves for those who do enough study.

Sending money globally (and other items of value in digital form) will indeed become as fast and cheap as sending emails, but nobody has done that yet. That is, however, entirely achievable with existing technological bases that just need to be taken a bit further.

Bitcoin and Ethereum lack the scale and speed needed for global payments

In this race for the world's payments, as shown by Chart 10 above, both bitcoin and Ethereum are out of question, because their protocols and the underpinning blockchains are not able to handle such speed and volume, nor enable virtually free transactions, and those coming after them, Ripple and Stellar, have their own problems that also require significant revamp, if not a complete rebuilding of their code base, which may also lead to compatibility issues vis-à-vis any application currently existing on top of such platforms.

No proof of the commercial viability and security of the lightning solution yet

Even if solutions such as the so-called "lightning network" as a second layer on top of the bitcoin blockchain to enable "lightning fast" payment transactions to circumvent the structural capacity and speed problem in bitcoin have been proposed[35], it is still a long way to establish, whether such ideas can really solve the problem, because it is not so simple, when 'payment channels' need to be separately opened and closed between every sender and recipient, and then eventually settled within the underlying bitcoin blockchain, with the second layer also creating another security risk[36]. Second layer solutions tend to be 'patch-up' solutions that may not be sustainable, and there is no sufficient evidence of their practical use nor any mainstream commercial applications to prove the use case either. A true global payment network would require the intended functionality built into the core protocol directly, not creating a potentially unsustainable structure of several independent layers that need to communicate with each other.

[33] "*Continued Decentralization & the XRP Ledger Consensus Protocol*" Ripple on 21 February 2018

[34] "*Ripple/Stellar Consensus System May Have Serious Issues*" Brave New Coin on 6 December 2014

[35] "*Bitcoin's Open Secret: Lightning Is Making Better Online Payments Possible*" Coindesk on 10 August 2018

[36] "*Bitcoin developer warns Lightning Network is flawed and likely vulnerable to DoS attacks*" thenextweb on 27 February 2018

No proof of viability of sharding solutions either

Besides lightning, Ethereum has also proposed a "sharding" solution to carve out the network into smaller shards to be able to better scale up the volume and speed, but such solutions are still years away[37] from the testing and application phase.

No proof of the viability of any new entrant

Very recently, some new projects have been introduced, claiming to be able to tackle this challenge. However, no new project provides with any concrete proof of being able to solve the problem either. As an example, or a curiosity, in October-November 2018, the Israeli project labelled "Initiative Q" has captured global media attention due to its successful email referral campaign resembling a pyramid scheme, promising a very valuable amount of a cryptocurrency that does not yet exist, only based on a hypothetical calculation derived out of thin air. The project claims of having received 4 million signups by using the world's oldest marketing trick of promising "free money", subject to the realization of such project. The project, however, does not even provide with a technical white paper nor any other necessary detail either, but only with some very generic statements that can be adopted by anyone making similar claims. So far, the project has been only a pure marketing campaign with a signup website and nothing else. Normally, any serious project has at least presented with a well-thought of white paper on how it will approach the problem, but this "Initiative Q" has not done anything else than attracted people to sign up with remote indications of vast amounts of money "for free". It is not likely this Q project will be able to bring anything new to the table either.[38]

Vast blue oceans remain ahead in the field of global payments

If the whole spectrum of various propositions to solve the problem of the world's payments, and anything considered between one end, where bitcoin really exists, and the other end with projects with over-hyped promises such as that Initiative Q, and anything in between, like those that are a bit more serious propositions like Ripple and Stellar, and then the ERC-20 token projects, some of which claim to be able to process a million transactions per second, which claim is entirely baseless, when the underlying Ethereum blockchain can only handle a few per second, it can be seen that it is still vast blue oceans ahead in this area of global payments, because no one has yet delivered any concrete solution that would in a credible way be able to tick all the boxes required from a global payment network.

6. Bad public policies driving crypto deposits

Currently, it is estimated that 40-50% of crypto assets are held as "offshore deposits", and it is possible that this figure may exceed 90% over the next ten years[39], but, at the same time, many factors may evolve differently, causing a different outcome, if e.g. more and more other assets get tokenized such as securities, precious metals and other commodities, then accounting for a much larger part of such digital assets.

Bad government policies and economic mismanagement drive crypto deposits

It should be noted that the interest towards holding crypto assets as offshore deposits can emanate from various circumstances that logically lead to such growth, e.g. (i) devaluation of fiat currencies (many currencies e.g. in South America and Africa have

[37] "*Ethereum Sharding Slated for 2020: ETH Foundation Researcher Justin Drake*" CCN, 6 July 2018
[38] "*Initiative Q Won't Solve Bitcoin's Problem*" Forbes on 8 November 2018
[39] "*Cryptoasset Market Coverage Initiation: Valuation*" by Satis Group p. 5, 30 August 2018

lost practically all their value due to hyperinflation caused by economic mismanagement and rampant corruption), (ii) unfavorable domestic fiscal policies (or outright abuse in certain countries, where fiscal tools are *de facto* used to confiscate private income and assets – this does not only happen in countries like Russia and China, but also even in EU countries, like it happened e.g. in France a few years ago in the form of 75% tax, a *de facto* confiscation of private funds, during the failed regime of François Hollande), (iii) capital restraints by governing bodies (capital controls limiting transfers of money and assets abroad, even among EEA countries, in Iceland fairly recently, as well as in EU countries like Greece (2015) and Cyprus (2013), or controls imposing limits on maximum FX transfers out like what China has imposed on its citizens, USD 50,000 per year), or other economic mismanagement and instability (which may also cause excess inflation and currency devaluation like (i) above) such as excess budget deficits and national debts – national debt levels in excess of 100 percent are commonplace in the EU (at least in Greece, Italy, Portugal and Belgium[40]), where failed monetary policies of the ECB have killed growth and destroyed trillions of euros worth of wealth, leading to impossible situations, where the normal adjustment mechanisms available with sovereign currencies (such as having the currency gain or lose value in function of the relative competitiveness of the issuer's economy) have been eliminated by forcing everybody to accept the euro, perhaps the most disastrous technocratic currency experiment in the history of the humankind, which suits nobody, but destroys the wealth and growth of everybody (even the countries recently experiencing hyperinflation have not caused as much damage as euro, because such economies are much smaller, whereas the euro has destroyed trillions worth of wealth), and then politicians are too weak to acknowledge this reality and stop that horrendous experiment that has cost trillions of euros, only to concentrate monetary powers in the hands of a handful of technocrats that have never managed any real business in their lives, or held any real responsibility for anything whatsoever. Those technocrats destroying trillions have not been put up for the vote in front of the nations, whose wealth they have destroyed (not difficult to calculate, when it is seen, how much economic growth and return on funds and assets have been lost because of this), and those current and former politicians being the decisionmakers in such matters in many cases do not have any understanding or competence whatsoever on the matters they decide upon, leading to a very dangerous cocktail of arrogance and incompetence. The complete failure of the euro is the dirty open secret, a hot potato that people are aware but too weak to deal with: the medicine definitely is not more economic integration, but much less: the diverse economies of Europe are so different that it is absolutely imbecile to try to force them into a common straightjacket that suits no one. Europe's economies will never be unified, and it is a horrible error to even try to force them to be similar. Economic success is never reached by any forcing but through free enterprise, and the nations must have their sovereign rights respected and take the monetary powers into their proper hands, so that the sovereign currency again reflects the particular characteristics of the underlying economy, be it weak or strong, but that is up to the free and sovereign nation to decide.

When so many countries, 19 in Europe, have given up their sovereign currencies (which should be one of the basic qualities of sovereign nations, to have their own currency) and got in return "a suit that does not suit them", the euro, they might as well move directly to cryptocurrencies that are independent of states and governments and not subject to failed economic policies and mismanagement. Perhaps this untenable

[40] "*Government debt slightly up to 86.8% of GDP in euro area*" Eurostat on 20 July 2018

situation will on its part drive the development of a new breed of cryptocurrencies that will deal with that problem.

Free movement of capital and the portable technology help accumulate and manage digital assets as a new store of value

So it is obvious that the imbalances and instability caused by bad policies and economic mismanagement push increasing amounts of funds into cryptocurrencies that are not dependent on such policies, thus putting the "store of value" function as their primary function so far. In the world that should be knowing less and less borders, it is natural to move and allocate capital between assets, and when there is simultaneous negative impact of holding capital in traditional assets and currencies, and the new opportunity to hold such assets in an extremely portable form that can be managed from anywhere on the planet, it is obvious that such cryptocurrency deposits or holdings will increase.

Increasing amounts of traditional assets will be converted into digital form

More and more of wealth will be created and stored in digital form. Crypto assets will only increase and be expanded to cover many traditional asset classes through tokenization and similar mechanisms.

Growing need to offer crypto banking services to manage increasing digital wealth

When the volume of crypto assets grows, and the holdings of such assets in the form of crypto deposits seeking safe havens from government abuse grow (and also generally growing due to the crypto economic activity taking shape), there is also a growing need for the management of digital wealth and legitimate crypto assets, which is a vast opportunity to create and offer crypto banking services on a global basis. There are always some clueless, embittered people, who would try to attack this and claim that such services would be only to cater for tax evasion or illegitimate funds, but such people should watch out and think first: this is the future – the separation of money and assets from governments and government control is inevitable due to the proliferation of such globally accessible technology that brings in vast value added and efficiencies gained in terms of cost and time. There must be services to manage this increasing digital wealth so that both digital and traditional assets can be smoothly accessed.

It was technocrats who pushed for non-cash payments and separation of money from sovereign powers: cryptocurrencies are just an evolutionary result thereof

In fact, it was the technocrats who initiated such evolutionary path by creating supranational (but failed) currencies like the euro, which is nobody's currency. Cryptocurrencies are equally detached from any government, but they are also decentralized and censorship resistant, and cannot be affected by failed policies. The valuations of major cryptocurrencies will stabilize, when they get more and more commonplace in the everyday life, and when the underlying crypto economic activity grows, eventually absorbing the traditional, physical economy. What would be a more suitable type of currency for the future world than cryptocurrency? It was the central authorities themselves that started this evolution away from physical money, and this is the continuity of that, to make money entirely virtual, but also in ways that does not give powers to anybody not meriting them such as central authorities abusing their powers, but being decentralized, democratic, censorship-resistant and globally distributed for resilience and resistance against any attacks. Decentralized cryptocurrencies cannot be used as tools for political purposes in contrast to central banks that are nothing but political in everything they do: the so-called 'central bank independence' is nothing but a smokescreen to create an illusion that has nothing to do with the reality. Only decentralized cryptocurrencies can guarantee independence from any political interference.

New generation of better cryptocurrencies coming

It is clear that there will be an entirely new breed of cryptocurrencies around: what has been seen was only the first round.

Crypto banking as bridge between digital and physical realms

Even if banking as a closed-entry system may be in conflict with the decentralized philosophy of the crypto world, such crypto banking activities offering high quality services for transacting, holding, storing and managing digital assets form an important connection between traditional and digital finance in ways that benefit both.

Smart politicians and regulators building crypto nations will be the winners

Such entities will need to be subject to the regulation in their domiciles, which requires jurisdictions with smarter and more enlightened regulators that are forward-looking and not backward-looking, understanding the value of this business for their jurisdictions. It is a positive sign of a successful and smart stance, when serious financial centers have already labelled themselves as "crypto nations". Those will be the winners, and those who do the opposite, will lose: the crypto clientele is modern, sophisticated and represents the future, and the future is the one that needs to be accommodated, not the past, if the objective is to reach any success at all.

7. Only smart, supportive regulation makes sense

Bill Clinton: Don't kill the goose that lays the golden eggs

In connection with the discussion and debate concerning cryptocurrencies and blockchain-based finance, some smarter US regulators and other prominent public figures[41] pointed out that it would be idiotic to kill the goose that lays the golden eggs i.e. the stifle the nascent blockchain industry with excess regulation, but work out with the industry a smart basis for a regulatory regime that supports the growth of the industry, not limiting or stifling it. Regulatory uncertainty, and the market's fears for overregulation have also had an impact on the crypto market, being a reason among a number of others for the market stagnation.[42]

Choice for nations and regions: to be a winner supporting crypto, or a loser attacking it

In general, the best way to kill innovation is regulation. Europe has been very successful in that, and that is why it always trails in innovation and innovative technology enterprise. Attacks against FAANG or other technology companies do not help or improve its position – it is only a demonstration of mismanagement of public resources in allocating them in attacks instead of trying to finance the buildup of something constructive. There is no visibly successful cryptocurrency startup in the EU – in Europe, there are only places outside of the EU, such as Switzerland and a few small nations outside of the EU that have adopted a smarter, more constructive approach, and despite of some regulatory hassles, as usual North America remains a cradle of innovation: the most successful cryptocurrency startups are de facto all American, and some Asian, but there are none in the EU. Why? Because the EU approach always is, very unfortunately, to regulate and tax everything that moves to death, and they are probably the most successful in the world in killing any incentive for innovation. In other words, that is called shooting to your own feet. So it is for sure that EU, unless it radically changes its approach vis-à-vis its obsession to overregulate

[41] "*Bill Clinton: Over-Regulation Could Kill Blockchain's 'Golden Goose'*" Coindesk on 1 October 2018
[42] "*Regulation News Still Moves Bitcoin Prices, BIS Report Says*" Coindesk on 24 September 2018

and overtax everything, can be excluded from the list of domiciles for a successful blockchain industry – or anything successful in innovative business for that matter. It could be otherwise, if there were smart and competent people deciding on the matters: some other countries have understood this better, the fact that one must not kill the goose that lays golden eggs, but Europe never learns this, so it always comes last in innovation, and without innovation, there is no growth, as the pitiful statistics show. If EU wants to reach any other success than being the world champion in overregulation and overtaxation that are the worst possible areas of focus, it will need to entirely turn its approach upside down from the current one that is a sure recipe for a continued disaster and loss in the international competition for technological innovation and successful enterprises in that area – or any area, for that matter.

Europe at crossroads: repeat past mistakes and lose again, trail in innovation further, or change approach completely and win

This really is a choice for Europe and in particular for the EU: whether to repeat the past stupidities and over-regulate and over-tax everything, or adopt a wholly different approach that is light-touch, supportive and industry, innovation-driven, not regulation-driven. If bureaucrats focus on the fear of losing their power by everything new and then trying to control such "threat" by attacking it with regulation, then they are focusing on an entirely wrong thing. Unfortunately, the bill is always in the end of the day paid by the taxpayers of the member nations, when over-regulation and over-taxation has yet again taken one more opportunity for economic growth and success from them – indeed, the "protection of consumers" means protecting them from ever gaining any economic success and profit that goes to the old-world incumbents that they defend because of vested interests. Many people know this all, but action must be taken to prevent such disasters from happening again.

Innovation must be given priority, and everything else comes after that: it is innovation that creates wealth, whereas regulation kills that

Regulation indeed cannot determine – and cannot be let to determine either – what are the winners and the losers in this game: the markets must be let to decide that on the merits of the projects. It is not the stifling regulation that "protects" the investors, which is only propaganda by some using it as an excuse to submit everything to their unmerited powers, but the principle of risk diversification to diversify the bets into small, manageable portions, and not take any disproportionate risks per single investment – most people do have reason to know that, what kind of risks they are able to take, be something regulated or not.

Success can come from anywhere, so the seeds sown must not be suffocated

In this nascent industry, a project created by "nobody" may be far more successful than one created by "big names", so who is behind a project is no guarantee of its success or quality, because some fresh new brains may have come up with extraordinary things, and to support young talent, any stifling regulation must be banned from everywhere, and innovation let to flow freely. Market never rewards bad projects in the end of the day, and their judgement is thousand times more competent than that of regulators, because it represents a group of people actually looking into these things and having understanding to assess them on their merits. In any new, nascent industry, the only option is a very 'light-touch' regulation if any at all, because otherwise the talent will flee and find a better place, leaving those that get too excited about regulating only losses in their hands, eliminating any upside potential at all, and, once again losing in the economic competition. Unfortunately, many people deciding on such matters are not intelligent enough to understand this, and then, entire nations will suffer, when the talent and the potential that might otherwise remain there, if there is free space to innovate and get the innovation funded and off the ground, will flee and seek a better place, where they can focus on their substance instead of excessive red tape that they cannot handle, and should not handle either, because their focus must be on realizing the vast potential this new technology enables in

disrupting so many industries and generating enormous new value – like the FAANG did in their respective industries. If e.g. EU wants to have any startups at all that can become the future FAANG, it would better be light tough and resist its over-regulatory instincts that indeed are horribly bad instincts: look at where EU is in innovation, where it is in growth – at the very bottom. The EU Parliament's report on cryptocurrencies in summer 2018 (footnote 5) was quite reasonable given that it is an EU institution, but it must be ensured that reasonable approach is maintained and that the other EU institutions do not again wreck that unique economic opportunity for growth and to bolster EU's meager credentials in innovativeness by applying their horrible erratic judgement in stifling that emerging possibility through overregulation. That tendency must be resisted and reversed, or EU will once again be the big loser in innovation and technology.

Regulate the regulators to prevent horribly costly errors – real checks and balances must be instituted and enforced, or otherwise the taxpayers will again pay the bill

Regulators are not smarter than the businesses pioneering in innovation, and cannot and must not hold any decisive roles in "deciding the fate" of cryptocurrencies and other blockchain applications – in fact, they are often the contrary. There are sometimes rather worrisome situations, where officials that do not comprehend and grasp the cryptocurrency and blockchain thing at all think that they however know better, stamp everything they don't like or understand as "high risk" and "money laundering" or other illicit use, and then try to ban and demolish it. Such people are not only risks to the process of innovation and generating new employment and success through entrepreneurship, but they represent one of the gravest risks to common good, a fact that many don't understand. Regulators should be regulated themselves, to prevent any abuse of their powers – no public power can be without a comprehensive set of real checks and balances, and the regulators have been the ones having the least of them, even if they generally belong to the executive branch of government that must be under real control and accountability without any excuse. As it has been seen, some public comments made by regulators in different countries vis-à-vis cryptocurrencies are not only lacking intelligence but they also demonstrate complete lack of understanding of the underlying substance.

Smart pro-crypto regulators can facilitate a lot of economic value-added and new job and wealth creation

At the same time, there have been a few smart regulators who see the big picture and the utility of distributed ledger technologies and cryptocurrencies in generating new economic activity, wealth, lowered barriers and improved access to finance, inclusion and empowerment – not some dark monster created only to enable illicit activity. It is not terribly smart of a central banker to cry that "stop creating money from nothing" to blockchain entrepreneurs, when the central banks do exactly that by themselves – it is decades ago since e.g. USD was backed by any tangible asset, gold. Some smarter current and former officials[43] have acknowledged the fact that almost no fiat currency is these days based on anything else than the illusion that because it is issued by governments or government-backed bodies, one can trust it, but there are so many cases around the world, where government-issued money has been anything but trustworthy, leading to situations, where anything else than such government-issued 'legal tenders' are considered safer and more trustworthy as monies, including cryptocurrencies.

[43] "*Sheila Bair says bitcoin has no intrinsic value — but neither does the dollar*" Marketwatch on 2 March 2018

8. Tokenomics vs. monetary economics

Suitability of the discounted cash flow method

The methods to value cryptocurrencies have been subject to intense debate. It has been seen that cryptocurrencies cannot be correctly valued by using the same discounted cash flow method that is commonly used in valuing securities that essentially are the sums of their discounted cash flows such as dividends, coupons and any residual values. Cryptocurrencies essentially do not produce any cash flows, even if there are some that generate an annual "inflation" amount that is paid to either all holders of that currency or those that participate in tasks such as mining, if the currency in question is produced through mining, or otherwise validate transactions recorded in the blockchain as network nodes. Even if there is "inflation", which is not for the purpose of inflating the money supply, but for paying for various tasks, as mentioned, so that there is incentive to perform such tasks, which can be paid for as per transaction mining or confirmation fees or as annual "inflation" fees, that kind of inflation fee cannot be properly discounted to derive the "value" of such cryptocurrency, because such "inflation" or fees do not account for the entire economic activity enabled or related to such cryptocurrency.

Network effect approach

There are also tokens issued on existing blockchains such as Ethereum and Stellar, and some of those tokens have a mechanism to reward for a certain activity by their users, or generate network use fees or other fees based on activities on the network like rewarding apps and their users based on transactions created in the case of such tokens like KIN, which may then be distributed among the token holders evenly or based on their network activities. Such approach may enable a network valuation based on its "network effects" in creation and distribution of value that can be attributed to such tokens. This is also analogous to the traditional monetary valuation based on the level of economic activity within the economic unit using the currency, often the national economy of a country, or its "strength" relative to other economies.

Monetary economics

Rather than the discounted cash flow method, approaches closer to those of monetary economics should be applied, as cryptocurrencies indeed are the new and appropriate form of money for the Internet era.

In normal circumstances, the equation of exchange, as developed by the famous monetary economist Irving Fisher more than 100 years ago (1911), could be used, which, in its simplified form is

$$M * V = P * Q$$

where, for a given period,

M is the total nominal amount of money supply in circulation on average in an economy

V is the velocity of money, that is the average frequency with which a unit of money is spent

P is the price level, and

Q is a quantity of real expenditures (goods and services).

The money supply M, in this context, the market capitalization of a cryptocurrency, would be the value of all transactions Q (goods and services bought or sold) times 1 (price level P assumed to be 1, with no inflation), divided by the velocity V of money i.e. how many times the money supply circulates in the "economy".

The challenge in applying the equation of exchange

The challenge of applying such formulas in valuing cryptocurrencies so far is the lack of the underlying economic activity, while most of the transactions relate to speculative trading so far, and the number of transactions that relate to commercial activities to pay for products or services are so far minor in nature. The value of any cryptocurrency could not yet be reliably established by using such formulas, and if any were used, the velocity of the supply would be disproportionally large due to active trading e.g. in the case of bitcoin, but at the same time the value of the actual goods and services transacted would be very small, leading to distorted figures that do not correspond to the market capitalization determined by the crypto market.

Efficient market theory

At the same time, according to the efficient market theory applied to pricing by securities markets, assuming that the market is efficient with sufficient trading volume giving the necessary depth for efficient price formation, and that all relevant information is accessible to participants for the same purpose, then, the current valuation level for the cryptocurrencies that are traded should be the correct valuation level for them, which, at the same time, would not correspond to the value of the money supply estimated with the equation of exchange due to the lack of real and efficient economic activity in the role of money as medium of exchange. The valuation as suggested by efficient market theory may apply to the top 3-10 cryptocurrencies, where trading is significant, but for lesser cryptocurrencies the market may be so thin that there is no efficient price formation. The lack of market depth may also lead to disproportionally low valuations.

Applicability of models

It is expected that in the long run, when more and more economic activity takes place in the crypto economic sphere, valuation using monetary formulas will give an increasingly correct picture; so far, it is more determined by the speculative trading markets on the basis of the law of supply and demand in the marketplace. Cash flow based models will not work, because cryptocurrencies are not securities generating cash flows such as dividends or coupons, but rather resemble the characteristics of money, of which they are the new digital form.

Tokenomics vs. monetary economics

In fact, the approach of the recently coined term "tokenomics" is very similar to that of monetary economics. Tokenomics looks at the economic activity taking place within the space, where the token exists, and the more there is economic activity and transactions, the higher the value of the token, or coin. That thinking is parallel to the ideas behind the equation of exchange, where the variables relate to the money supply, velocity of money, the aggregate transaction value and the price level. The problem is, however, as stated, the lack of underlying economic activity so far, given the very early phase of such cryptocurrencies and tokens.

9. Ecosystem projects will be winners

Current lack of real economic activity within the blockchain platforms

As it has been seen, the volume of real economic activity within blockchain platforms is so far modest. It is normal, because this nascent industry is in its early phases, where the technology is emerging, not mature.

The (unintended) emergence of the ICO industry around Ethereum

Interestingly, the only area that has clearly formed its own ecosystem of active operators is the ICO industry largely around the Ethereum platform and its ERC-20

tokens (there are ca. 140,000 ERC-20 token smart contracts existing[44], and around 2,100 tokens listed[45]), the main use of which has been the fundraising through ICOs (see the Chart 13 below for the development of Ethereum transactions including smart contracts), Initial Coin Offerings. Around the ICO, there has been a whole new industry emerging that has provided various services to token issuers: platforms to create tokens, online directories to list token offerings (ICO platforms), smart contract coding and code audit firms, ICO marketing firms covering social media and traditional media marketing, PR firms, ICO conference and investor meeting organizers, community, airdrop and bounty campaign managers, specialized law, audit and consulting firms, ICO project incubators, and you name it. The ICO industry has indeed been the only real 'ecosystem' generated in the crypto space, with real business activity in it, even if the whole thing was never in the plans for Ethereum, but it just happened, when the suitability of the ERC-20 smart contract for crowd fundraising via token sales was discovered and started gaining pace. Now, when the ICO market has lost some of its steam due to the general stagnation of the crypto market, it is likely that many of such service providers are suffering as well, and many of them, having been very light weight online setups in the first place, will close down and disappear. As there were many scammers among the purported service providers, this market downturn will help to weed out the scam and what will remain, will be much more solid and of better quality, benefiting the next round of evolution.

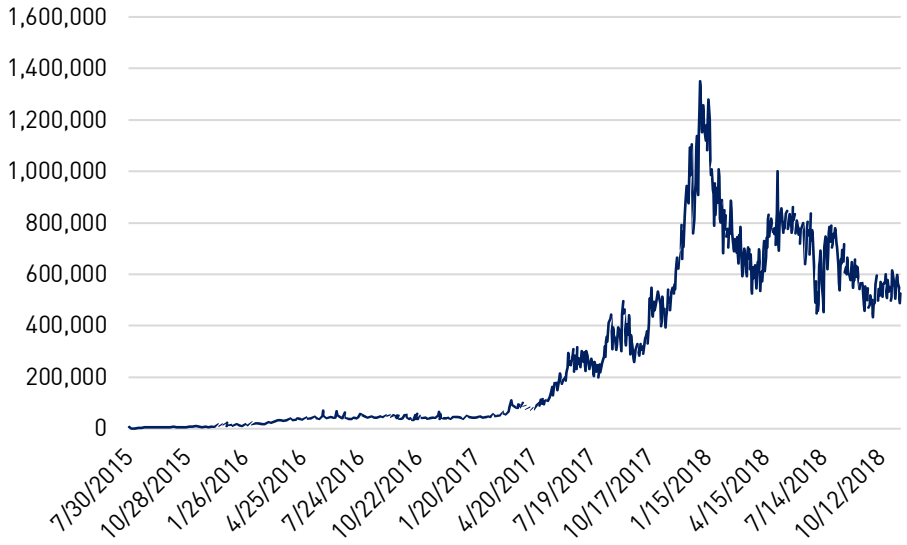

Chart 13: Ethereum transactions per day. The Ethereum transaction chart also reflects the trend of of the volume of smart contracts growing in the ICO boom and then the growth leveling off. Data source: Etherscan

No serious blockchain-based ecosystems yet

However, if serious projects and ecosystems are considered, there aren't any real ones up and running yet. When the volumes are very small, with the most notable applications being the likes of Crypto Kitties and the Augur prediction platform, where the amounts exchanged are also minimal, just around 300 users for both per day and decreasing, for Augur having been only 66 users per day, and this was a top Ethereum

[44] https://etherscan.io/tokens
[45] https://coinmarketcap.com/

application[46], it is clear that no real blockchain economic ecosystems have yet been created – the ICO industry has been only created to take money from those that are the entrepreneurs trying to build such applications and ecosystems, but it is not creating such real blockchain-based ecosystems on its own through its operation.

Think of Tesla with its purpose-build infrastructure with charging stations

Ecosystems will, however, be essential for the growth of the crypto economy at large: nothing can evolve in a vacuum, but there must be interaction and interconnections between the crypto economy and the traditional economy to help economic activity move between such realms, and have entirely new crypto economic activity to be created. A good parallel example from another context is the Tesla case: it was not enough to create a revolutionary electric car, but Tesla had to create a proprietary network of showrooms, service units and charging stations to be able to promote, sell, deliver, service and have the car charged so that it is usable in real everyday life, not only a curiosity. Crypto industry needs the same: there must be ecosystems taking shape to provide for an end-to-end experience also including a bridge between the physical and digital realms, so that funds and transactions can flow freely and smoothly between them and boost the creation and growth of a serious crypto economy that will in turn generate a lot of value added and synergies to its participants, and savings in cost and time.

An example of ecosystem: global payment network with its network bridges and dapps

A good example of this is a cryptocurrency and its blockchain functioning as a global payment network, gradually building up its dapp economy taking over from traditional financial service providers. The network cannot, however, operate in a vacuum, before such cryptocurrency becomes a widely recognized means of exchange, because otherwise, if there is no smooth way to (i) convert it to and from any other currency or asset, and (ii) use it as the means to effect transfers of any item of value including monetary payments, it will not reach any position as a widely used, global payments network and currency, or the process will at least be slower – nothing, however, stopped bitcoin from reaching global prominence, even if access to it has often been very cumbersome and limited, if operations to exchange fiat money have been required in that process. For this purpose, there needs to be 'bridge entities' or similar units holding balances of other crypto and traditional assets, such as banks offering both crypto and traditional banking services, but in a modern manner. Ironically, as long as there are those kinds of banks, they would be (i) closed-ledger and (ii) regulated, which would be two no-no's for the bitcoin purists, issues against which the whole thing is: a fight against control, abuse and censorship of central authorities that are the biggest risks and hazards of the current times. However, sensible, value-adding solutions can be created in environments where the regulators are smart and constructive, and see the wood for the trees.

Boosting both physical and digital realms

Such bridge entities provide the link between physical and digital economies and help the funds and assets move between such realms, and when more funds move into the blockchain ecosystems, more economic activity is created. That in turn will help to generate more and more activity within decentralized applications and other types of applications developed on the blockchain, which will then take over from traditional service providers like such bridge banks and other similar entities. The more crypto economies grow, the more self-contained they become, and, eventually, traditional

[46] "*Where Have All the Augur Users Gone?*" Coindesk on 8 August 2018

actors will merge into them. This is also what needs to be understood: the whole economy will become a 'crypto economy' i.e. in the end of the day there will be no difference, so it is useless to try to put them against each other, since the interest is shared, not opposite.

Impossible to accurately predict evolution, what is the significance of bridges

It is, however, not possible to predict the evolutionary phases of this nascent industry that may take entirely unforeseen turns, when new innovations emerge: it may be possible that the role of bridge entities and similar will be eventually much smaller, and more and more activity will be directly created within the crypto sphere in a self-contained manner, when certain critical mass is reached after having passed a certain tipping point of development. When crowds get excited about a new thing and it gets a viral momentum going, anything can happen – to the benefit of all, as this indeed will promote global financial inclusion, access to financial services, lowered barriers to entry and entirely new types of economic activity, business opportunities and wealth creation.

Most successful projects likely to be those with their ecosystems

It is likely, however, that the most successful blockchain projects will be those that build ecosystems around their core innovation from early on, because the internal synergies within such ecosystems will multiple the value for all participants, with any marginal transaction significantly adding the network value. Thus it is important to consider many elements of the ecosystem right from the beginning and work on to build an expansive community / user base for the platform.

An example of an intended ecosystem: the EOS cloud computing project

Some projects have understood this, and e.g. the largest project by funds raised, EOS, has already allocated around a billion dollars[47] out of the 4.3 billion raised for its ecosystem-related venture capital investments, attempting to generate a whole dapp-driven ecosystem around its core cloud computing platform. It will be seen, whether they are successful, because it is a long way to reach even the core promises made for the EOS blockchain in terms of speed, scalability, operating cost and so on – so far it is rather expensive to use[48], with a very small chunk of network capacity costing significant amounts, and the promised multi-thread scalability missing altogether[49] – so EOS must first use the billions it raised to make the core blockchain into what they promised it to be, before being able to build any dapp ecosystem around it at all.

New ecosystem-centered projects expected to transform their industries

However, the rise of the solid ecosystem-centered projects can be expected, with particularly significant opportunities in the world of payments, banking and other financial services that can indeed be revolutionized via the application of this nascent technology, creating a wholly unforeseen architecture and operating structures that reflect the future of global financial services that finally enables purely global operations.

---

[47] "*Former Jefferies Asia CEO to Lead $1 Billion EOS VC Arm*" Cointelegraph on 5 July 2018

[48] "*RAM It All: Rising Costs Are Turning EOS Into a Crypto Coder's Nightmare*" Coindesk on 4 September 2018

[49] "*EOS Multi threaded parallel processing execution*" Steemit February 2018

10. Will bitcoin remain?

Bitcoin at 10

Bitcoin just turned 10, with its white paper having curiously been published at Halloween 2008, at the end of October, by the person under the mysterious pseudonym "Satoshi Nakamoto". Thus, it is appropriate to finish this report with the 10th and last topic reflecting on the position and outlook of bitcoin, the world's currently largest cryptocurrency that originated the rise of the whole blockchain industry we are now experiencing. As the Chart 14 below demonstrates, bitcoin is by far the dominant cryptocurrency in the world as of today.

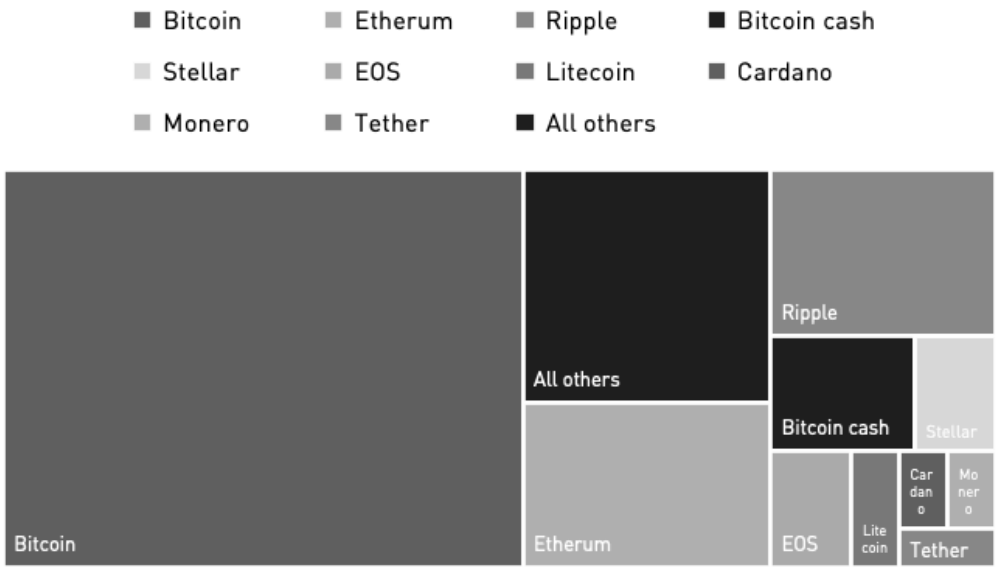

Chart 14: Relative shares of cryptocurrencies of the total market capitalization. Bitcoin is still dominant, holding more than 50% of the total market value, and the top 10 cryptocurrencies hold together 85%, with the remaining almost 2,100 tokens and cryptocurrencies only 15% of the total. Data source: Coinmarketcap

Unique achievement: digital currency recognized globally, created and maintained without any input from any government or central authority, censorship-resistant

What is perhaps bitcoin's most remarkable achievement is the fact that Bitcoin proved a currency with real value and universal recognition can be created and maintained without the involvement of any central authority, any central bank or other governmental body, and be completely censorship resistant. Bitcoin proved that it is possible to create 'private money' that is recognized globally but not controlled by anyone. The end of bitcoin has been so many times predicted by its adversaries and critics, but it is still going strong and dominating the cryptocurrency market, as the chart above shows, despite of all attacks it has had to endure. Its "*first mover advantage*" has been very strong indeed – but there are not, however, any guarantees that the same will remain.

Bitcoin is Chinese

Bitcoin also has certain significant risks related to the mining pools that generate most of new bitcoins: "*Cryptocurrency miners have banded to such an extent that "over 80 percent of Bitcoin mining is performed by six mining pools," with five of those*

managed directly by individuals or companies based in China."[50] Chinese mining pools control more than 50 percent of the hashing power[51] of the bitcoin network, so there is a risk that bitcoin may ultimately fall under Chinese government control, because, in that country, the totalitarian government ultimately controls everything, as e.g. many globally distributed news about the government suddenly confiscating prominent businessmen's assets without any due process or any legal merit tell. This indeed is a highly worrisome fact that many people do not know about: *bitcoin has already for a long period been 'Chinese*'. In this process, mining equipment manufacturers like the Chinese firm Bitmain have not played a small role, because they have helped create such powerful local mining pools in China by supplying their equipment. To take control of the majority of the hashrate, or the hash power of the network is one of the very few means to control and possibly break the network.

A response is required – a new fork or an entirely new Bitcoin 2.0

When bitcoin has lost its independence to the Chinese mining pools that may be ultimately controlled by the Chinese government and thus may no longer be safe and censorship-resistant, the bitcoin community will face very fundamental decisions to make: will a new fork need to be executed to wrestle the control out of the Chinese mining pools, or will a "Bitcoin 2.0" need to be created (in addition to those 2,100 altcoins and tokens that claim to have presented the next bicoin, while none hasn't so far). It is clear that the current situation is not sustainable, when the majority of hashrate has been fallen under the control of mining pools ultimately controlled by a totalitarian government, which was exactly one of the worst nightmares of bitcoin's creator Satoshi Nakamoto.

Digital gold maybe, but no 'gold standard' for payments – question of revamp

While bitcoin represents 'digital gold' to many, it definitely is not the 'gold standard' in payments. As it has been discussed under topic 5 Payments, the characteristics of bitcoin are not sufficient at all for the function of a global payments network, and bitcoin will not become any world currency for payments, unless it is rebuilt from the ground up (which may also be needed for other reasons as demonstrated). If a comprehensive rebuild is done, a new hard fork of the codebase, there is also a risk that many other features would be changed, and the end result may then be very different from what bitcoin was intended to be, so there are massive risks in any effort to dramatically alter the characteristics of bitcoin that may create serious compatibility issues. Perhaps it should remain as it is, a 'store of value' (even if it is too volatile for that function too, even if the volatility has recently fallen substantially), because it cannot be a global 'medium of exchange' or 'unit of account' given its deficient qualities for such functions that a world currency should fulfil. But if it remains as it is, it may eventually lose in the competition, when technically more advanced and better next generation cryptocurrencies enter the market, and they will: for example, one of the major deficiencies of bitcoin, massive electricity consumption, will immediately put it into a very disadvantageous position compared to any new project achieving a better performance with much less energy.

Valuation

Indeed, if we consider the fact that the current market capitalization of the outstanding bitcoins in circulation is only USD 111 billion, even if this is the world's #1 cryptocurrency for the time being, it is a very low amount indeed, compared to the

[50] "*Research: China has the power to destroy Bitcoin*", The Next Web on 8 October 2018

[51] data.bitcoinity.org/bitcoin/hashrate/

money supply of major international currencies, only a fraction of a percent of such amounts, like USD 14 trillion for M2.[52] If the global gold stock is valued at USD 7-8 trillion (footnote 4), bitcoin is far away from having the levels justified for 'digital gold' as a store of value as well. Even when the market capitalization of bitcoin exceeded USD 327 billion at its peak on 17 December 2017[53], it is still a very small amount for a globally leading cryptocurrency, when the figure is put into perspective. Currently, the market is bearish and contains many elements burdening the valuation such as regulatory uncertainty, but even at its peak the valuation could be much larger in proportion to major fiat currencies. It is evident that either bitcoin, if rebuilt and the Chinese control issue dealt with, or some entirely new cryptocurrencies that may not even exist yet, will achieve total market capitalizations into trillions of dollars, because the world's money will be in such a digital form. It is only a question of time, and a question of which ones will be the winners in this space (including those that do not yet exist), not a question of whether it happens.

Hidden flaws

Recently, a serious flaw was discovered in the bitcoin codebase, the exploitation of which would have enabled a skilled hacker to cause the network to crash entirely[54]. Luckily, such flaw was discovered and fixed in a new version so that wrong people did not get to know about it before the update was implemented, but there might always be a risk that further errors in the codebase are found and exploited before they can be stopped. This shows that even the biggest blockchains in the world, with bitcoin holding more than USD 111 billion in digital wealth, may have flaws, on top of the thing that the architecture is already a decade old, even if a part of it has already been revamped. This all puts bitcoin into a vulnerable position – even if it has an active developer community, there is no strong guidance for the direction (one of the weaknesses of the decentralization, as after the initial creator no one controls it), and unless certain features like the huge energy consumption and low processing capability are improved, the risk to become obsolete upon introduction and proliferation of better, more modern and more capable cryptocurrencies can become great indeed.

The future

It will be seen, whether bitcoin becomes the new "Sony Betamax", or whether it remains the "VHS", the winning solution dominating the market. If the codebase is not revamped and dramatic changes made, the Betamax path may indeed have a great probability. If the necessary changes are executed well, bitcoin may maintain a very strong position in the future, but new entrants may also be able to eclipse it in totally unforeseen ways.

Conclusions

The purpose of this report was not so much to provide market facts, but to present views, opinions and outlook in order to incite debate and discussion around these important topics so that such matters can be taken further in this shared effort of building the crypto economy and the wonderful technology that underpins it. In brief, concerning the topics raised:

[52] https://tradingeconomics.com/united-states/money-supply-m0

[53] Coinmarketcap

[54] "*Bitcoin on brink of collapse after 'very scary bug' discovered in code*" the Independent on 20 September 2018

1. **Crypto market stagnates, waiting for use cases to launch, new products, regulatory certainty** Crypto market lost ¾ of its value during the first half of 2018 and has stagnated at that level ever since with exceptionally low volatility; bitcoin regained its dominance from the lows of less than 1/3 to more than ½ of the total crypto market capitalization; the initial bubble burst in a very similar manner compared to the Internet bubble almost 20 years ago, and the reasons are also similar: real-life use cases in action, real economic activity is still missing, and it will take time to achieve that; market waiting for new fund products to see new money in, and some regulatory certainty
2. **Retail investors out, institutions in** When the crypto bubble burst during the first half of 2018, retail investors, who first entered the market at the peak, nursed significant losses and left the market, with trading volumes down by 80%, and now they are being taken over by institutional investors interested in this new high-potential asset class to diversify their portfolios and benefit from the growth of the industry; institution-grade products and services being developed, and wider availability thereof likely to attract significant volume of new funds into the market and put upward pressure on prices
3. **ICO boom lost some steam but 2018 will be a record year** In line with the market downfall, the ICO boom seems to have lost some but not all of its steam, given the less active investor participation in the market, more difficult marketing circumstances (FB, Google, Twitter marketing that boosted in 2017 was banned in 2018, making marketing much more challenging); at the same time, difficult market conditions are weeding out the scam i.e. increasing the average quality of ICOs to come – the ICO is not dead, but it has clearly slowed down due to the market circumstances: fundraising continues despite of difficult market but with raised amounts being smaller, still being a record year by far
4. **Growing demand for privacy-oriented crypto** The global scandals in abuse of individual user data and revelations of government intrusion into privacy beyond previous beliefs have triggered the quest for privacy that is a basic human right, boosting demand for privacy-oriented cryptocurrencies – there will be more to come in that area
5. **Distributed ledger technologies will revolutionize global payments but technology needs to be taken further** Blockchain technologies enable a real revolution in payments, with the distributed ledger making possible payments that are truly global, virtually free and real time – the technology needs to be scaled up to increase the processing volume per second and the transaction confirmation speed to sub-second, but when this is achieved, SWIFT, payment card schemes such as Visa, MC, Amex, correspondent banking and traditional clearinghouses will all be history
6. **Bad public policies and economic mismanagement drive crypto deposits; crypto banking services needed to satisfy demand for services** Incumbent banks have rejected the modern and sophisticated crypto clientele that will require services to manage their traditional and digital wealth and transactions – 40% of crypto deposits are offshore, and various challenges in many countries will only lead to the increase in such volume over time up to 90%, creating a vast opportunity for on- and offshore crypto banking services
7. **Regulation: be smart and don't kill the goose that lays the golden eggs** Some countries have adopted a smart and constructive regulatory approach that supports the buildup of their blockchain industries that will give them a big boost in the global competition for innovation and wealth creation; some countries and regulations put taxation and regulation first, and they will once again lose the game: never kill the goose that lays the golden eggs, but adopt a 'light-touch' approach to keep it live and producing – the message must be

either smart or then no regulation, but bad regulation is a sure thing to lose in this global opportunity

8. **Valuation of cryptocurrencies: market values better than formulas at this stage** Since cryptocurrencies and tokens do not produce any dividend or coupons or any other cash flows or ownership rights, they are not securities, and since they do not have such cash flows, they cannot be valued with the discounted cash flow model as securities can be; since there is no sufficient underlying economic activity linked to particular cryptocurrencies, the monetary formulas to value a crypto money supply cannot be applied either so far; at this stage, the most accurate valuation is given by the crypto market itself, but this concerns the major cryptocurrencies such as bitcoin and Ethereum that are actively traded, whereas the shallow and thin trading on minor ones does not give any reliable valuation
9. **The winning blockchain startups are those that build the infrastructure for their ecosystem from the ground up** Think of how Tesla made its cars work in everyday life: it built an infrastructure of charging stations and service units – the same applies in the crypto sphere: crypto economic activity is not generated in a vacuum but it is boosted by bridge entities such as banks interfacing between real and digital economies, boosting both, and then further leveraged by a gradually evolving dapp ecosystem on top of the underlying blockchain and cryptocurrency; the winners in this game are the projects that develop and build from ground up a complete ecosystem, not only one component such as a new blockchain protocol, or just a token – success will come through the hard work to build up the whole architecture and infrastructure for its platform, and the most potential area is the domain of global payments and banking and financial services to be disrupted, revolutionized and replaced by advanced blockchain technologies
10. **Bitcoin may remain strong but needs a complete revamp rid itself of its flaws – otherwise it may become the Betamax of cryptocurrencies** Bitcoin, celebrating its 10th anniversary as the world's leading cryptocurrency, is at crossroads: to remain strong, its codebase would need to be dramatically revamped, as its high electricity consumption, very low transaction throughput and slow confirmation speed make it unable to become any serious player in global payments or much in anything else than a store of value, for which it also has been far too volatile. It is to say that it has to do the same as what Ethereum is planning, basically rebuild itself entirely, or gradually wither away and die. If bitcoin does not adapt itself the changing circumstances, it is likely to become another Sony Betamax that may have been in certain respects superior to VHS, but VHS became the standard for videotapes, while VHS also died later on, when new and better technologies were introduced. Bitcoin had a fantastic idea, and it proved that money can be digitally created outside of any government in a way that is credible and universally recognized, really creating a global digital currency, but to be able to remain so, it will either have to be rebuilt, or it perish. It may also fade away, when entirely new and better cryptocurrencies will be introduced and proliferated, and new ones will emerge anyway. So it will be interesting to see, will bitcoin's 20 years be celebrated in 2028, or has it been abandoned into the dustbin of history upon emergence of newer and better cryptocurrencies. Will bitcoin become *the* world currency? We don't think so – in its current form it cannot by any means get even close.