TAURUS

DIGITAL ASSETS AND SUSTAINABLE DEVELOPMENT

Two irreconcilable worlds ?

TAURUS GROUP SA MARKET ANALYSIS

DECEMBER 2018

Taurus Group SA
11, rue d'Italie
1204 Geneva
Switzerland

FOREWORD

Global warming is increasingly worrying and the 2015 COP21 Paris agreement, which aims to contain global warming below 2°C by 2100, is the last of many multilateral initiatives tackling the topic. Most industries now put sustainable development at the heart of their investment and capital allocation decisions.

How does sustainable development relate with digital assets? The Financial Times[1] defines sustainable development as being "about maintaining an equilibrium between human activity and the natural environment over the long term. It involves a fine balance between the economic, social and environmental needs and expectations of various stakeholders ". Digital assets - especially Bitcoin - are however often been as not being environment friendly due to the energy cost of mining. Recent reports from venerable institutions have stated that Bitcoin mining accounts now for one percent of the world's energy consumption and even that it could push global warming above 2°C by itself[2]. Others threat these reports as "fake news"[3]. To what extent are the concerns about digital assets sustainability justified? Are all blockchains environments unfriendly? What is the current carbon footprint of digital assets and what are the possible evolutions?

This article provides a rapid overview of the emerging digital assets industry from an environmental point of view. First it classifies the different protocols according to their consensus algorithms. Second, it quantifies the energy consumption of digital assets. Last, it presents alternatives that are much less energy-hungry.

[1] http://lexicon.ft.com/Term?term=sustainable-development
[2] See Mora, Rollins and al., 2018, Nature, Bitcoin emissions alone could push global warming above 2°C
[3] https://medium.com/setocean/fake-news-bitcoin-energy-consumption-4312da7f12fa

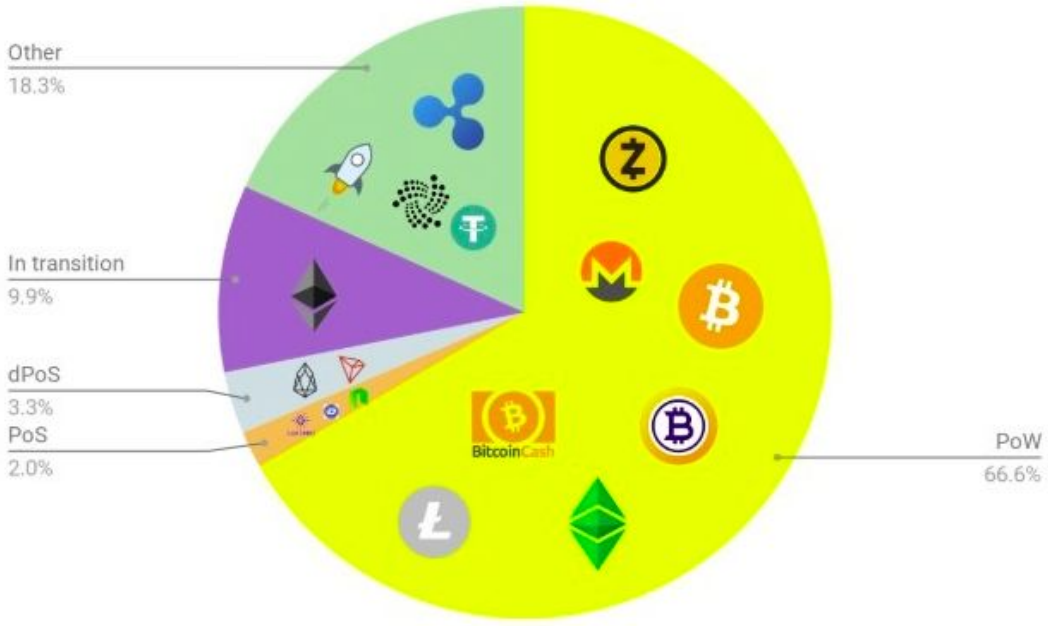
I. ENERGY CONSUMPTION OF DIGITAL ASSETS

a. Consensus algorithms

Digital assets are registered and maintained on a distributed ledger infrastructure. Miners collectively maintain a ledger of all the transactions, known as "blockchain". A fundamental feature of such a distributed network is the algorithm by which its network participants (also called "nodes") validate transactions and ensure the consistency of the ledger across all nodes. This is the so-called "consensus" algorithm which can be divided in two main categories - Proof of Work (PoW) and Proof of Stake (PoS), with a few variants thereof.

Not all consensus algorithms are energy-hungry. PoW algorithms have been - rightfully - the most widely criticized due to two main factors i) their high energy consumption ii) their powering the largest blockchains, in particular that of Bitcoin (which represents more than half of the total digital assets market cap at the time of writing). Other, much more efficient, consensus algorithms are being developed and/or already put in production. For example, Ethereum, the third largest blockchain by market cap, is shifting its consensus algorithm from PoW to PoS[4]. In addition, EOS, which raised the largest ICO ever, has built and put in production a Delegated PoS algorithm (dPoS)[5]. Figure 1 below shows, for the Top 20 cryptocurrencies, which consensus algorithms are used.

Figure n°1: Top 20 cryptocurrencies consensus algorithms repartition (by market capitalization)



[4] See Taurus article "Ethereum: a broken engine?" https://www.taurusgroup.ch/ethereum-a-broken-engine/
[5] See Taurus article "EOS, the next Ethereum?" https://www.taurusgroup.ch/eos-the-next-ethereum/

b. The Proof-of-Work (PoW) consensus algorithms

The Proof-of-Work (PoW) name comes from the fact that miners have to compete in order to find a solution to a cryptographic problem (based on a hash function[6]). This competition takes place every 10 minutes for Bitcoin - as blocks have to be validated every 10 minutes. Practically, for each new Bitcoin block, miners invest their computational power in order to find the right answer to the problem and thereby record the block into the blockchain. The fastest miner to find a solution is awarded newly-minted bitcoins[7].

The high energy consumption coming from mining activity is linked to the nature of the PoW. By design, PoW involves a "brute force" approach to validate each block, namely, the repetition of hash function evaluations. Therefore, the higher the computational power of a miner, the more hash function evaluations are computer, and so the higher the chance to find a solution to the PoW and mine the block.

Professional miners have invested in huge mining farms (data centers dedicated to mining) that run 24x7x365. Since June 2018, the total number of hash function evaluations per second for Bitcoin has fluctuated between 30 and 60 quintillion per second. Unsurprisingly, these giant mining farms use massive amounts of electricity to run countless processors. In addition, cooling down the infrastructure furthers adds to the electricity bill, which amounts to 60-90% of total mining cost-base. In order to reduce this electricity bill while at the same time boosting processing power, several major processor improvements took place: over the years, the transition from CPUs to GPUs and then to ASICs[8] has multiplied the mining efficiency by a factor of 10,000 (see the blue curve on the figure 4 below). Alas, total energy consumption *has kept increasing*. The Digiconomist news site estimates the latter to 50+ TWh per year (see Figure 3 and section c. below).

[6] A hash function is a function mapping data of arbitrary size to data of a fixed size. The values returned by a hash function are called hash values, fingerprints, or simply hashes.
[7] 12.5 bitcoins per block at the time of writing this article
[8] An ASIC (application-specific integrated circuit) is a microchip designed for a special application, such as a particular kind of transmission protocol or a hand-held computer. You might contrast it with general integrated circuits, such as the microprocessor and the random access memory chips in your PC

Figure n°2: Bitcoin hashrate[9]

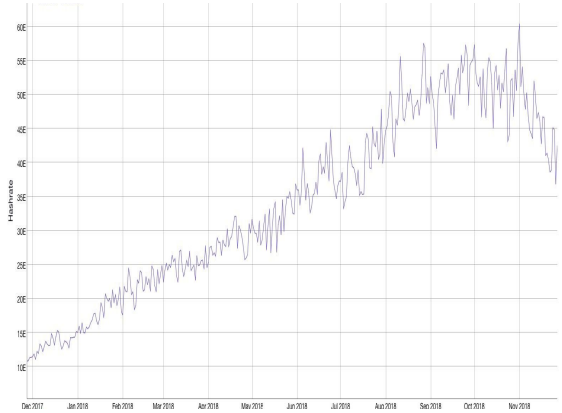
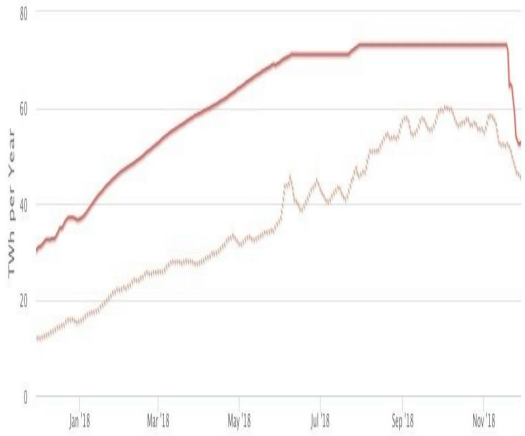
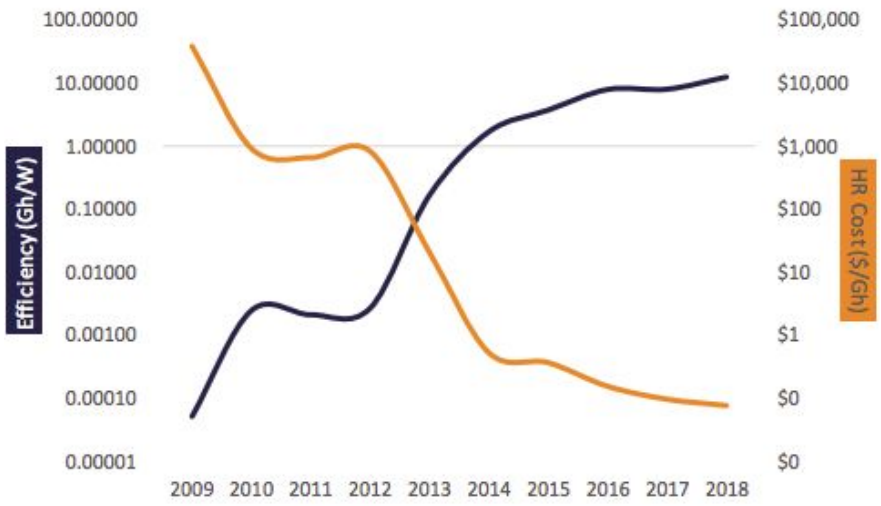


Figure n°3: Bitcoin est. energy consumption[10]



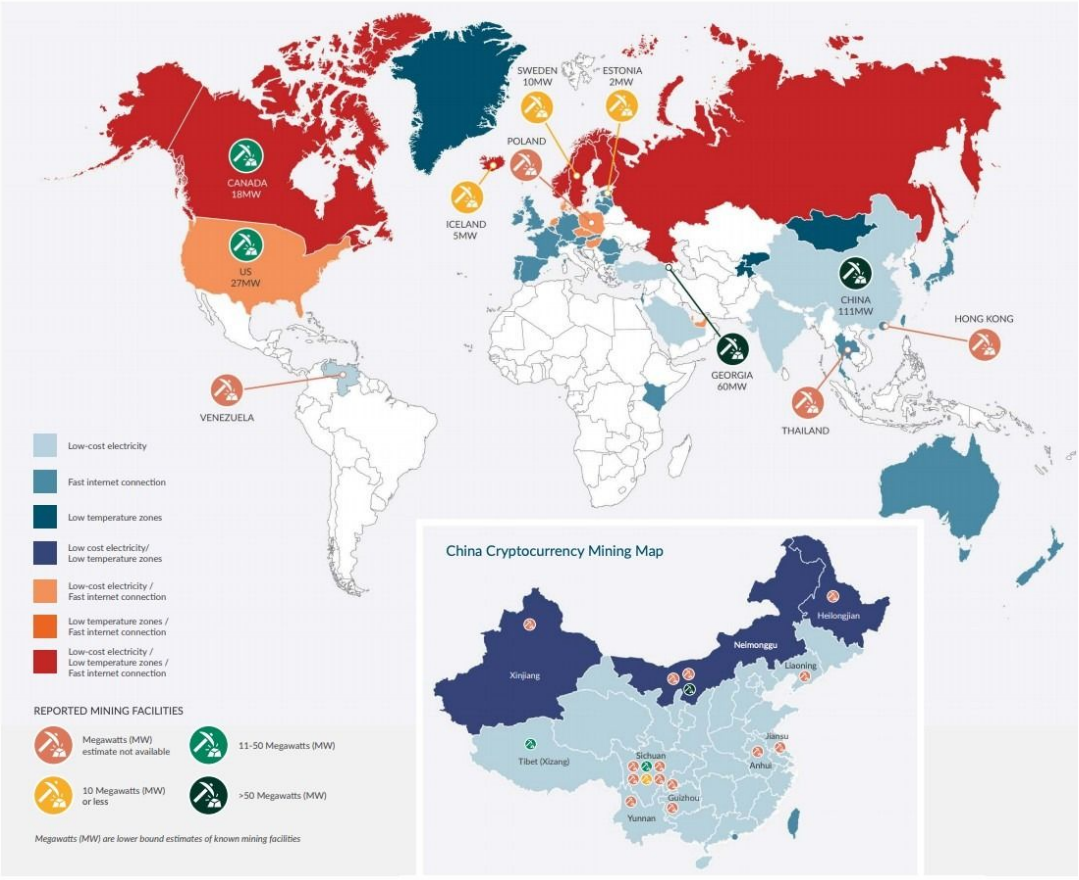
N.B.:Both figures display the past twelve months

Figure n°4: Mining efficiency evolution[11]



[9] Bitinfocharts.com, as of 28/11/2018
[10] https://digiconomist.net/bitcoin-energy-consumption
[11] https://research.bloomberg.com/pub/res/d3bgbon7nESTWTzC1U9PNCxDVfQ

Figure n°5: Global cryptocurrency mining map[12]



c. Current attempts to estimate energy consumption

The energy consumption debate surrounding cryptocurrencies, and especially Bitcoin, has emerged last year, notably with the publication of the so-called *Bitcoin Energy Consumption Index* on the Digiconomist website[13]. According to this index, if Bitcoin were a country, it would be ranked 39th in the world in terms of energy consumption, while Ethereum would be ranked 79th.

While these indices are only approximations, we believe that the big picture and order of magnitude are correct. Figure 6 shows several sources estimating the Bitcoin annual electricity bill and Figure 7 shows Taurus energy consumption estimates for both Bitcoin and Ethereum. Annual Bitcoin electricity consumption is thus estimated to be around 14-65 TWh. For comparison, US Christmas lights burned 6.6 TWh in 2008[14] and residential cooling consumed 212 TWh in 2017[15]. Last, according to a recent study[16], at least 77.6% of the electricity used to mine Bitcoin comes from renewables sources of energy.

[12] Global cryptocurrency benchmarking study, 2017, G. Hileman, M. Rauchs, Cambridge Centre for Alternative Finance
[13] https://digiconomist.net/bitcoin-energy-consumption
[14] https://www.energy.gov/sites/prod/files/maprod/documents/Energy_Savings_Light_Emitting_Diodes_Niche_Lighting_Apps.pdf
[15] see U.S. Energy Information Administration (EIA) website: https://www.eia.gov/tools/faqs/faq.php?id=1174&t=3
[16] https://coinshares.co.uk/bitcoin-mining-cost/

Figure n°6: main Bitcoin annual electricity consumption estimates

Study	*Year of estimate*	*TWh per year*	*Country equivalent**	*World rank**
Digiconomist	2018	65	Iraq	42
Leopold & Englesson	2017	26	Bahrain	67
Malone & O'Dwyer	2014	25	Slovakia	68

* The equivalence in terms of country electricity consumption is based on the CIA World electricity consumption[17]

Figure n°7: Bitcoin and Ethereum minimum electricity consumption estimate

	Bitcoin	*Ethereum*
Market capitalization ranking	1	3
Avg. Network Hashrate*	36 E/s	152.88 M/s
Best mining hardware efficiency**	44 Th/s	485 Mh/s
Estimated number of hardwares in circulation	*820,682*	*315,217*
Mining hardware electricity consumption (W) per hour	2000	850
Network minimum annual electricity consumption (TWh)	14.2	2.3

*YTD average
**BTC: EBIT E11++, ETH: Innosilicon A10 ETHMaster (GPU)

d. Comparison vs. alternatives

Some critics argue that digital assets network are unsustainable by comparing Bitcoin and VISA, quoting that the VISA network only consumes 0.5 TWh, significantly lower than Bitcoin's 14-65 TWh estimate. We can however draw several objections to this comparison:

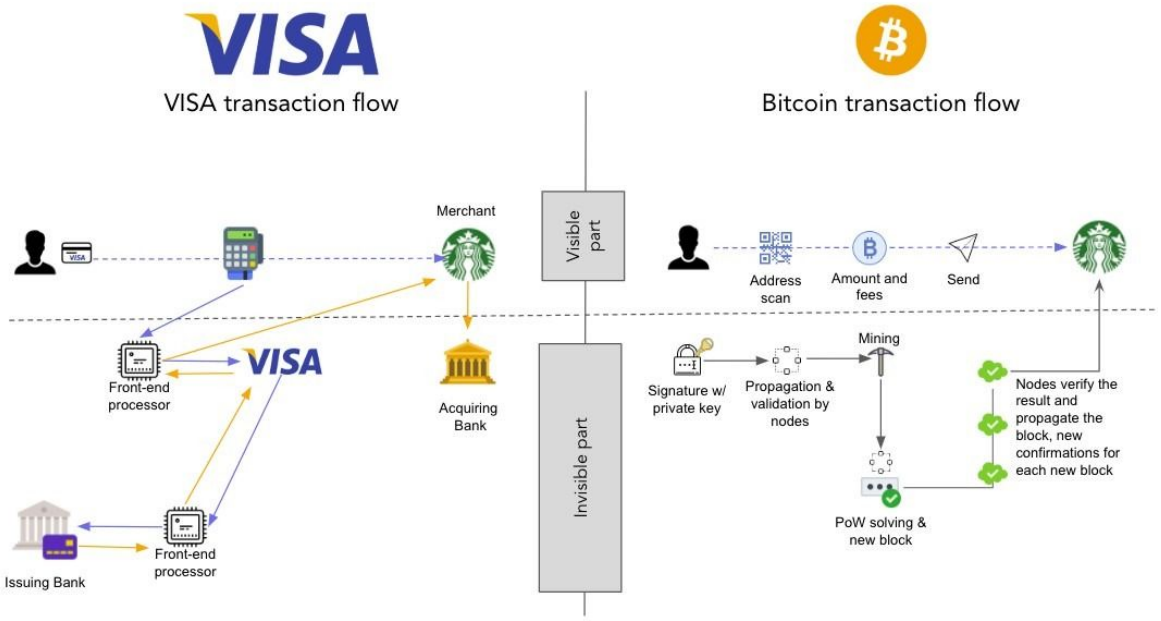
- This comparison is flawed because VISA is only one piece of a payment network, while Bitcoin is a full payment network. A fair comparison would require to add part of the banking system electricity consumption to VISA's as payment network typically includes the issuing bank, front-end processors and the acquiring bank.

- This comparison is only partial. While Bitcoin is the leading digital asset and is indeed power hungry, there already exist more suitable payment networks in the space. For example, Ripple (XRP), the 2nd largest by market cap, is better designed to compete with SWIFT or VISA. Another study[18] compares USD (via

[17] https://www.cia.gov/library/publications/the-world-factbook/rankorder/2233rank.html
[18] http://papers.netrogenic.com/sid/eco-friendly-money.pdf

Visa network), BTC, ETH and XRP and it shows that Ripple is significantly less costly than Visa network to proceed a transaction: 0.00649 KWh for VISA and 0.0000113 KWh for Ripple.

Figure n°8: VISA and Bitcoin transaction flows



II. TECHNOLOGICAL IMPROVEMENTS: BEYOND PoW

Despite more efficient processors, PoW will continue to consume vast amounts of energy. Fortunately, technological advances are paving the way to more energy-efficient consensus algorithms, and we believe they will power the next generation(s) of blockchain protocols. This section will review in particular Proof-of-Stake consensus algorithm(s), ligthning networks, and directed acyclic graphs technologies.

a. Proof-of-Stake (PoS) and its relatives

The Proof-of-Stake class of consensus algorithms represents a solution to the energy consumption problem, by getting rid of the PoW competition described in section I.b above.

With PoS, the validator of a block is selected through a combination of probability and token holders' stake. The higher the "stake" of a node (how much tokens the node owns), the higher its probability to be selected as the validator of a block. The selection process typically involves some randomized processes. The transition from PoW to PoS for Ethereum is something to monitor closely, because if it does succeed, this will constitute a potential blueprint for the other PoW protocols currently used.

Other consensus methods based on PoS have emerged such as:

- The Delegated Proof of Stake (dPoS) used by the EOS network. Instead of choosing validators among digital asset holders like in classical PoS, a subset of users, called block producers are elected by the digital assets holders. Such a protocol increases the throughput of the network by limiting the number of actual validators, while achieving a decent degree of decentralization thanks to the voting process.
- The Proof of Authority (PoA) consensus method which is similar to PoS or DPoS with the exception that the validators are pre-determined. Unlike PoS, however, the amount of tokens held by a party does not increase their chance of earning more tokens. PoA therefore differs from PoW and PoS in that it doesn't create a the-rich-get-richer" dynamic.
- The consensus Delegated Byzantine Fault Tolerant (DBFT) used by NEO is another one based on token holders vote. They vote for Delegates, among which one Speaker is randomly elected. He proposes laws and if the delegates are unhappy about this new law they can simply say no and the Speaker can be substituted. Like PoA, DBFT and other BFT variants decorrelate the power of a node—in tokens or hardware—from its chance of validating transactions.

PoS and its variants do not involve cryptographic "brute force" computations as PoW does, and therefore is considerably more energy efficient. Besides improvements on the method of consensus,

others blockchains improvements and the use of innovative distributed ledger technologies could further lower the energy consumption.

b. Lightning network, side-chains

The lightning network mechanism enables participants to transact off-chain, that is, without directly interacting with the network A bidirectional payment channel is built between Party A and Party B through the creation of a ledger entry on the blockchain. The two participants can then do multiple buy and sell transactions among themselves without the need to broadcast any transaction to the network, hence saving energy. Once one of the two participants wants to terminate this relationship, it simply broadcasts the last version of the ledger to the blockchain.

An alternative to the Lightning network is also the use of side-chains. A side-chain ("child") is a blockchain that is coupled with the main one ("parent") via a two-way peg. Thanks to this mechanism, side-chains can issue their own digital asset which price is pegged to the main-chain asset. For example, there already exists two side-chains linked to the bitcoin protocol: RSK and Liquid. The first one enables to build smart contracts and the second one is more of an institutional payment channel which can support high volumes and large transactions. Even if these side-chains provide obviously interoperability features and are needed for the current blockchains to scale, it does not solve the energy problem. Indeed they still need to have their own miners to verify and confirm transactions.

C. Other distributed ledger technologies

Other distributed ledger technologies like directed acyclic graph (DAG) are promising in terms of energy consumption. IOTA or Hashgraph use this technology for their networks. DAG represent distributed ledger networks which are not comprised of a chain blocks, but instead of a graph. In order for a new transaction to be taken into account on the network, it has to validate two former ones. In others words, there are no miners as the new transactions "mine" the previous ones. NANO uses a technology called "block lattice" which is a hybrid between blockchain and DAG. Each NANO account has its own blockchain. The users tracks only their account balance rather than the transaction amounts. Therefore there is less storage space needed.Thanks to their blockless nature, the network protocols based on DAG are a way less energy consumers than POW or even than POS ones. It could represent the future of distributed ledger networks but it lacks real world implementations as IOTA, NANO, etc. are for now considered as newbies that must gain trust.

PoW consumes necessarily a lot of energy as the quest of the "puzzle solution" implies a computational power hash rates race among miners. Methods of consensus like PoS are more efficient and are gaining traction. The use of off-chain solutions or side-chains will help the blockchains to scale but should not have a significant impact in terms of energy consumption. Other distributed ledger technologies which are even less energy consuming (i.e. DAG) are still in their infancy.

SUMMARY

The Proof-of-Work class of consensus algorithms, which is the most widely used and powers >50% of the market[19] today, is at the heart of the crypto electricity consumption issue. Proof-of-work is, by nature, energy-hungry and not sustainable.

Many technological improvements and other consensus mechanisms have emerged. Proof-of-Stake is one of the most adopted. Ethereum's transition from PoW to PoS could pave the way for other digital assets to follow and dPOS is currently used by EOS. Eventually, as for every new technology over time, energy consumption will be reduced drastically and the growth rates of current established cryptos will wind down.

To us, this question is being solved and scalability - not energy consumption - will be at the heart of the next generation of blockchain protocols.

[19] By market capitalization

Important disclosure

The information and opinions in this article were prepared by Taurus Group SA ("Taurus"). Taurus Group SA or the writer of this article has a significant financial interest in some digital assets such as Ether, Bitcoin, Litecoin, Bitcoin Cash or EOS. Taurus does not provide individually tailored investment advices. This article has been prepared without regard to the circumstances and objectives of those who receive it. Taurus recommends that investors independently evaluate particular investments and strategies, and encourages investors to seek the advice of a financial adviser. The appropriateness of an investment or strategy will depend on an investor's circumstances and objectives. The securities, instruments, or strategies discussed in this article may not be suitable for all investors, and certain investors may not be eligible to purchase or participate in some or all of them. This paper is not an offer to buy or sell or the solicitation of an offer to buy or sell any digital assets or to participate in any particular trading strategy. The value of digital assets may vary a lot because of changes in interest rates, foreign exchange rates, default rates, prepayment rates, securities/instruments prices, market indexes, operational or financial conditions of companies or other factors. Past performance is not necessarily a guide to future performance. Estimates of future performance are based on assumptions that may not be realized. If provided, and unless otherwise stated, the closing price on the cover page is that of the primary exchange for the subject company's securities/instruments. This article is based on public information. Taurus makes every effort to use reliable, comprehensive information, but we make no representation that it is accurate or complete. We have no obligation to tell you when opinions or information in our research change apart from when we intend to discontinue equity research coverage of a subject company. Taurus may make investment decisions that are inconsistent with the recommendations or views in this report.