H12018: CRYPTO REPORT

Behind the hype, speculation, and public imagination that has gripped this emerging asset class there are market fundamentals. Indicators which offer essential insights to the market dynamics, investment patterns and overall development of these exciting new technologies.

At CoinShares Research, we strive to distill this information for our readers; to separate the signal from the noise, and to provide the sort of clear, intelligible, and relevant insights that are required to keep pace with one of the fastest moving industries of our time.

The Crypto Report aims to educate, inform and stimulate the creation of new ideas in our readers, as we cover four of the largest, most rapid-growing and technologically interesting crypto-assets in the industry.





	TABLE OF CONTENTS	
Industry Summary		3
Market Overview		3
Regulatory Developments		3
ICOs		3
Market Entrants		3
Industry Developments		4
Asset Summaries		4
Bitcoin		4
Litecoin		5
Ethereum		5
Ripple / XRP		5
Numbers Dashboards		6
Figure Explainer		6
Bitcoin		7
Litecoin		8
Ether		9
XRP		10
Important Disclaimer		11

None of the commentary or analysis contained herein is meant to constitute financial advice. This document is meant to be used as a foundational guide to cryptoassets and their potential. All analysis is meant to provide emerging trends and observations that may offer value in developing your own investment thesis, though past performance is not indicative of future performance. Please consider all risks carefully prior to making any investment, especially in an evolving asset class like cryptoassets.

Attachments:

- 1. https://www.mtgox.com/img/pdf20180307_report.pdf
- 2. https://www.sec.gov/news/speech/speech-hinman-061418
- 3. https://www.nomuraholdings.com/news/nr/holdings/20180515/20180515.pdf
- 4. https://www.bloomberg.com/news/articles/2017-12-21/goldman-is-said-to-be-building-a-cryptocurrency-trading-desk
- 5. https://www.fnlondon.com/articles/jpmorgan-crypto-strategy-20180517
- 6. https://bitcoin.org/en/version-history
- 7. https://github.com/TheBlueMatt/bips/blob/betterhash/bip-XXXX.mediawiki

- 8. https://bitcointechtalk.com/what-is-a-bitcoin-merklized-abstract-syntax-tree-mast-33fdf2da5e2f
- 9. https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/
- 10. https://eprint.iacr.org/2017/1066.pdf
- 11. https://bitcointalk.org/index.php?topic=305791.0
- 12. https://medium.com/@ianedws/roadmap-to-bitcoin-developments-f7af59b6d122
- 13. https://medium.com/@icebearhww/ethereum-sharding-and-finality-65248951f649
- 14. <a href="https://medium.com/l4-media/making-sense-of-ethereums-layer-2-scaling-solutions-state-channels-ethereums-layer-2-scaling-state-channels-ethereums-layer-2-scaling-state-channels-ethereums-layer-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ethereum-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-state-channels-ether-2-scaling-stae-channels-ether-2-scaling-state-channels-ether-2-scaling-state-

CoinShares Research

Lead Analyst (AC): Christopher Bendiksen - Carlota Ochoa - Samuel Gibbons

research@coinshares.co.uk



Yet another eventful half-year in the cryptoasset space lies behind us. Aggregated market cap peaked in early January at around \$830 billion and has since retraced to around \$250 billion at the end of June (Source: CoinMarketCap). During this time the bitcoin price has retraced approximately 62% from the 2018 highs as we have entered the young asset's third bear market lasting more than 6 months. That being said, at the end of June 2018, bitcoin is still up 154% year-over-year. The reversal in prices was arguably led by a combination of regulatory uncertainty and sizeable profit-taking by long-time hodlers, including a famous, yet oft-forgotten one: A report [1] published by the bankruptcy trustee of the infamous Mt. Gox exchange revealed that between December 2017 and February 2018, the trustee liquidated 35.841 BTC and 34.008 BCH for a total of approximately \$400 million. Most notably, 18,000 BTC were liquidated on 5 February, coinciding with the lows of the year (retested at the end of June 2018) and a subsequent 63% relief rally shortly thereafter.

The regulatory landscape has seen some positive developments in the last six months. Earlier in the year, South Korea highlighted that it was planning to regulate cryptocurrencies and bring them into the open, as opposed to outright banning them. In May, Japan announced that the country is working on cryptocurrency regulation and building a template for ICO and digital currency exchange regulation. Most recently, an SEC official announced [2] that bitcoin and ether are not securities due to the decentralised nature of their networks. Decentralisation, they argue. materially reduces information asymmetries that might otherwise arise when a central third party is a key determining factor in the enterprise. It also reduces the value that the application of the disclosure regime of the federal securities law would add. The SEC also provided more guidance on the criteria that are taken into account during its determination of whether a token primarily functions as a consumer item with utility or as an investment that would be bound by securities law. These criteria include: whether the token was created to meet the needs of users or whether it was created to feed speculation, whether independent actors are setting the price, whether it is clear that the primary motivation of purchasing the token is for personal use, whether tokens are distributed in a fashion that meets users' needs and incentivises users to promptly use the network, whether the asset is marketed and distributed to potential users or to the general public and whether the application is fully functioning or still in early stages of development. This guidance on ICOs and the determination that decentralisation is a measure of security status should give the community at least some long-awaited clarity.

2018 is also proving to be a record breaking year for ICO funding, with total funding raised in the last 6 months already surpassing the total of 2017 (Sources: CoinShares Research, Smith+Crown). Most notably, Telegram concluded the biggest ICO to-date, raising \$1.7 billion through two rounds of private sales, according to SEC filings. This reveals an interesting trend that we have also observed; new projects are increasingly opting to raise funds privately from the professional investment community and are avoiding public sales. We could see this trend continue if crowd liquidity dries up and founders increasingly see benefits from conducting private sales. From a regulatory standpoint, private sales limit exposure to KYC/AML risks due to the lower number of participants. Furthermore, the professional investment community can lend additional support to young projects such as office space, legal opinions, administrative support etc. If funding continues to move to the private domain, we suspect that more projects will instead attempt to derive network effects from airdrops internally in the existing communities of their parent platforms.

Another event worth mention is the long-awaited launch of the EOS mainnet. EOS is a blockchain platform for the development of decentralised apps and has been marketed as the first viable alternative to Ethereum. EOS was designed with the idea of bringing together the best features from existing blockchains by making it simple to use while enabling features such as intuitive developer functions, on-chain scalability, private key recovery and theft protection dictated by a unique governance structure. EOS raised an estimated \$4bn in a one-vear token sale that concluded this lune. Like many others, EOS opted to use Ethereum ERC20 tokens that effectively represent IOUs for future tokens on the EOS blockchain. This represented the first large scale "hard spoon" (full state data transfer) of a blockchain. whereby a new chain inherits the account balances held on another chain. In the case of EOS, all ERC20 balances



were frozen at the time of the hard spoon and thereby became non-transferable. The transfer process did not run entirely smoothly, and neither did the novel governance structure which lacked clarity and an enforceable constitution, resulting in block validators holding conference calls to arbitrarily decide whether or not certain accounts that were flagged as fraudulent should be frozen. The launch has been a clear example of the general vulnerability of many new platforms and specifically ill-defined governance structures.

Finally, it has been encouraging to see continued interest from the institutional investor community throughout 2018. In order to service this interest, numerous projects have been rolled out that are continuously professionalising the crypto industry. The lack of custody solutions has long been a barrier to entry for capital, one that is being addressed through projects such as the <u>partnership</u> [3] between CoinShares' parent company Global Advisors, Nomura and Ledger.

CoinShares is also working on launching its treasury department to provide treasury management solutions for cryptocurrency companies. A number of additional services have launched across the industry with the intent to facilitate the tokenisation of traditional assets via regulated security tokens. Polymath and tZero are interesting examples of exchanges and platforms aiming to facilitate the migration of traditional assets onto the blockchain. Banks are also making moves, with Goldman Sachs [4] and JP Morgan [5] announcing the creation of crypto trading desks or strategies.

In summary, while the crypto industry has seen a rough first half of the year in terms of price drawbacks, development is continuing at a strong pace. There are substantial steps currently being taken towards professionalisation of the industry with increased regulatory clarity and institutional participation. We eagerly await the developments of the next half-year and look forward to more exciting times in crypto.

...... ASSET SUMMARIES

Bitcoin

Compared to the somewhat tumultuous times of H2 2017, with the implementation of Segregated Witness, the Bitcoin Cash split and the victorious battle of Segwit2x, the first half of 2018 has been a relatively tame time for Bitcoin. Periods like these are cherished by developers as quiet times for actual work. As always, development of Bitcoin Core remains at pace with one major (0.16.0) and one minor version release (0.16.1) publicised on 26 February and 15 June, respectively. Both versions include new features, various bug fixes and performance improvements. For a full overview of changes, compatibility, and credits you can take a look at the full version history since release number 0.3.21 on bitcoin.org's version history sub-page [6].

Among the biggest developments in Bitcoin this year we surely find the successful launch and growth of the Lightning Network mainnet as a second layer on top of Bitcoin's on-chain base layer. Lightning offers network participants the ability of sending and receiving instant bitcoin payments of any size, at negligible fees while only using the on-chain Bitcoin base layer to fund and close accounts. Between 19 January (first data) and 30 June, the number of lightning nodes with channels has

grown from 54 to 1,482, the number of payment channels has grown from 105 to 5,666 and total network payment liquidity has grown from 1.24 BTC to 26.2 BTC (Source: bitcoinvisuals.com). While that is an impressive growth rate we would like to point out that the total liquidity pool of the network is still quite low, possibly reflecting caution on parts of experimental network participants while the technology matures.

One protocol development we believe to be particularly worthy of special mention is TheBlueMatt's (Matt Corallo) BetterHash protocol for communication between mining pool participants. We believe this new protocol can significantly reduce the centralising pressures of pooled mining and return power to small-scale miners. For a nice overview of BetterHash we refer you to TheBlueMatt's <u>GitHub</u> [7]:

While Bitcoin does not have an "official" roadmap (as the large number of contributing developers makes such a concept impossible to achieve) there are a number of interesting protocol improvements currently being worked on, including Merkelised Abstract Syntax Trees [8] (MAST), Schnorr Signatures, [9] Bulletproofs [10] and



------- ASSET SUMMARIES

<u>Confidential Transactions</u> [11]. The intent is to increase efficiency, on-chain transaction capacity and privacy. For a more comprehensive overview, we suggest this [12].

Litecoin

There is normally not much to add separately for Litecoin protocol development versus Bitcoin. Litecoin improvements are largely taken directly from the Bitcoin code repositories and minimally altered to be fully compatible with the small differences between Litecoin and Bitcoin.

Many if not all of the upcoming Bitcoin development proposals will probably make their way into the Litecoin Core project, but Litecoin's smaller development team means that changes are often easier and faster to implement. This has precedence in Litecoin's early implementation of e.g. Segregated Witness, and we would not be surprised if we see at least some of the proposed Bitcoin improvements implemented on Litecoin first.

Ethereum

Much has changed with respect to the planned upgrades and additions to the Ethereum network in the past six months. Most notably, the Constantinople hard fork that was planned for Q1 this year and was expected to include Casper (the addition of Ethereum's new Proof-of-Stake consensus mechanism), has been delayed until at least Q4 2018. This is primarily due to a shift in priorities following the launch of Cryptokitties, which made it clear that scaling solutions are of higher importance than other Ethereum Improvement Proposals (EIPs) such as Casper.

Casper is now expected to be split into two phases. The first phase is Casper Friendly Finality Gadget (FFG), a hybrid solution between Proof-of-Work and Proof-of-Stake. Casper FFG is expected to be deployed with the Constantinople hard fork in Q4 this year. The second phase is Casper Correct By Construction (CBC), which is intended to fully replace the current PoW consensus mechanism with PoS. Casper CBC is currently expected to be deployed in late 2019, with the Serenity release.

Scalability broadly refers to transaction throughput and cost. Currently, the network can process approximately

15 transactions per second but is vulnerable to significant slow-downs and increase in transaction costs (gas price) during periods of high activity. This is due to the fact that each full node on the ethereum network must validate each transaction, meaning that transaction throughput on the network is limited by the transaction throughput of each individual node.

The proposed scaling solutions can broadly be split into two groups. Layer 1 solutions are implemented at the base-level protocol of Ethereum and therefore require a hard fork. Sharding [13] is the most prominent Layer 1 solution on which the Ethereum Research Group is working. Layer 2 solutions, such as State Channels, Plasma and Truebit, are built "on-top" of the existing blockchain as smart contracts and do not require a hard fork. We recommend this article [14] for an explanation of the different Layer 2 scaling solutions. Dapp specific state channels have already been built (e.g. FunFair, Spankchain), whilst the Raiden Network (equivalent to Bitcoin's Lightning Network) is expected to launch its MVP for general payment channels on Ethereum later this year. Plasma is the brain-child of Vitalik Buterin and scales by enabling the creation of child-chains with independent consensus mechanisms to interact with the main-chain via smart contracts. OmiseGo have already built an MVP with plasma for their decentralised exchange and expect initial implementation in Q3 this year.

Ripple / XRP

The Ripple team continues to deliver as RippleNet surpasses 100 members. Most notably, Ripple is building out its emerging market presence as remittance providers and banks across LatAm, China and India join the network.

They have concluded the pilot programme for xRapid, the service targeting payment providers facing liquidity challenges in emerging markets. Ripple announced that the average participant in the pilot saw cost reductions between 40% and 70% and that the average xRapid payment took just over 2 minutes. Industry heavyweights such as MoneyGram and Fleetcor participated in the pilot. This is a significant development, as xRapid is currently the only institutional service that *requires* participants to transact in XRP.

Ripple have also taken the xCurrent and xVia products to market. In part of this effort they have partnered with the Saudi Arabian central bank to provide a pilot program to support Saudi banks to use xCurrent. xCurrent enables banks to settle cross-border payments instantly with end-to-end tracking.

H1 2018 CRYPTO REPORT / / FIGURE EXPLAINERS

These are the Figure Templates for the Next 4 Asset Summaries

...... fiq.1 fiq.2 fiq.2

Figure 1 is a simple price chart with a trade volume overlay. Price and volume are indicators of investor confidence and market liquidity, respectively. This chart type is referred to as a candlestick chart due to the characteristic shape of the figure segments. The body of the candlesticks represent the price movement between open and close and the "wicks" represent the intraperiod highs and lows. Market prices are read on the Left Hand Axis. Single candles can represent any period length, in this report however, they represent one week. Because cryptomarkets never close, the open and close times are set to midnight UTC. The lower bar represents total market trade volumes and reads on the Right Hand Axis.

Figure 2 shows annual returns running from the first reliable price signal of an asset until publishing date. This aims to give readers an idea of the long-term performance of the asset.

fig.3 fig.

In Figure 3 we look at the top 5 geographical markets by US\$ denominated trade volume*. This chart can give insight to the relative popularity of certain crypto-assets in different regions across the globe. It can also be interpreted as an indicator of exposure to legal, regulatory or other government-imposed risks in jurisdictions with high volumes.

Figure 4 shows monthly cumulative trade volumes* broken down by the largest fiat trading pairs. While there are additional fiat currencies trading in the market, the vast majority of trading is done via the top 7 (including Tether) fiats, with all remaining pairs only representing a small fraction of total global trade volumes. Readers can here observe periodic changes in overall trade volumes as well as which fiat pairs dominate trade in the crypto-markets. Overall trade volumes are indicative of market liquidity.

fig.5 fig.6

Figure 5 shows percentages of total monthly trade volumes* by exchange jurisdiction. Similarly to Figure three, this chart aims to lend insight into the relative geographical location of asset trading as well as an indicator of trade exposure to legal, regulatory or other government-imposed risks in jurisdictions.

Figure 6 shows average daily annualised volatility per year, running from the first reliable price signal of an asset until publishing date. Observing volatility over time can help readers get a sense of changes in the risk-profile of their crypto-assets.

fig.7 fig.8 fig.9

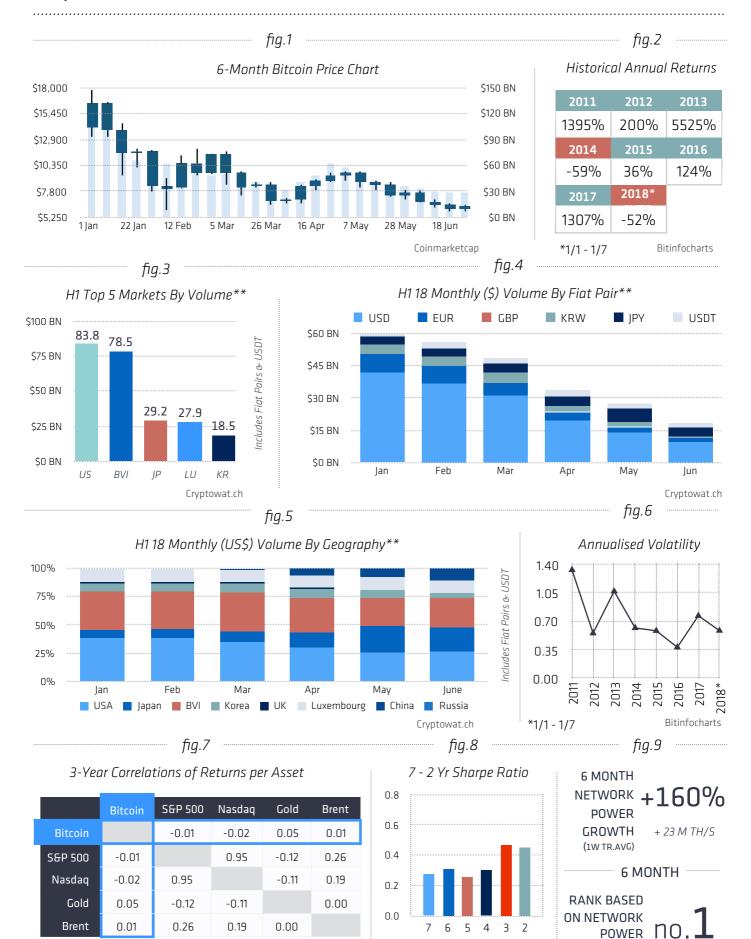
In Figure 7 we look at the correlation of cryptoassets against a basket of commonly investable assets using Pearsons Correlation Coefficient. Basic portfolio theory teaches that portfolios containing a diverse and uncorellated basket of assets are less vulnerable to volatility. A score of 1 indicates that two assets move completely in unison, a score of 0 indicates that they move entirely independently of each other and a score of -1 means they move completely opposite. Figure 8 shows various multi-year Sharpe Ratios. Sharpe Ratios are risk-weighted measures of return. The higher the score the better investors are compensated for the level of risk added by the asset.

Figure 9 shows the network power growth measured by change in hash rate. As a simplified rule of thumb, networks with higher hashrates are costlier to attack at the consensus level.



H1 2018 CRYPTO REPORT / / BITCOIN





^{**} Measured on Top 15 Exchanges by Volume (Spot Only, No Token-Fee-Model Volume Counted)

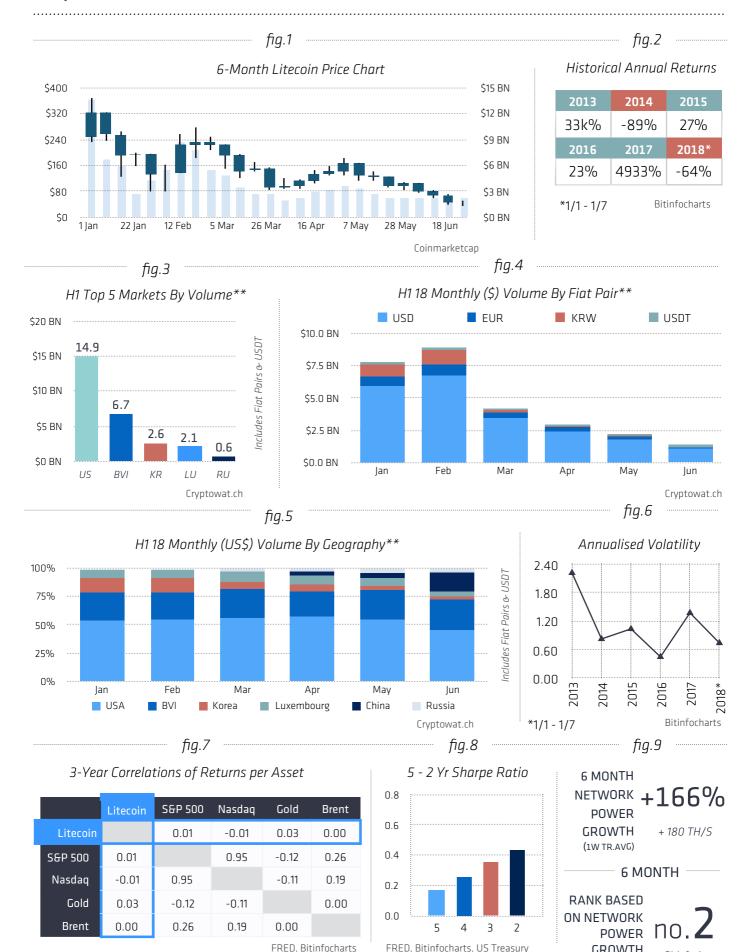
FRED. Bitinfocharts

FRED, Bitinfocharts, US Treasury



H1 2018 CRYPTO REPORT / / LITECOIN

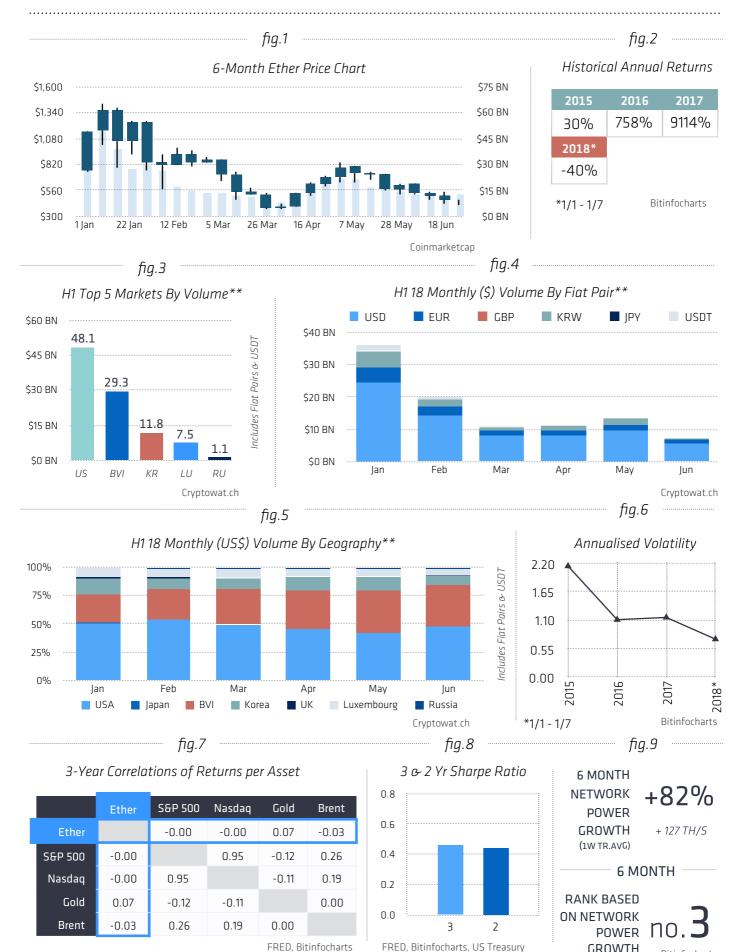




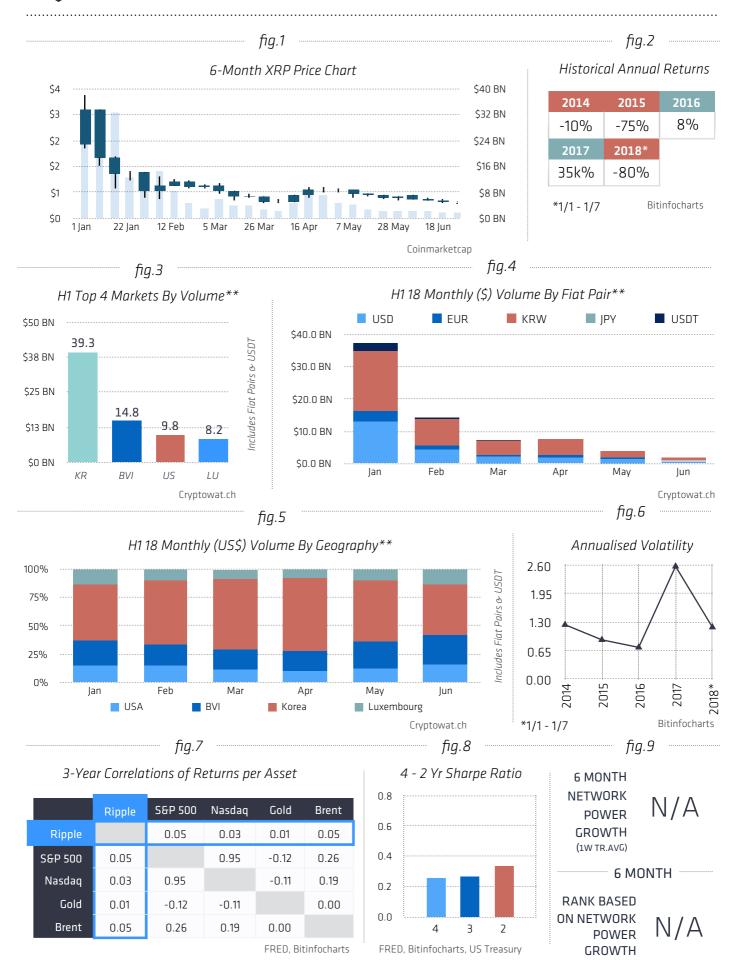
^{**} Measured on Top 15 Exchanges by Volume (Spot Only, No Token-Fee-Model Volume Counted)



H1 2018 CRYPTO REPORT / / ETHER



^{**} Measured on Top 15 Exchanges by Volume (Spot Only, No Token-Fee-Model Volume Counted)





IMPORTANT DISCLAIMER

Please note that this document is provided on the basis that the recipient accepts the following conditions relating to provision of the same (including on behalf of their respective organisation). Should the following conditions not be acceptable, please destroy this document without retaining any copies.

This document does not contain, or purport to be, financial promotion(s) of any kind. This document does not contain reference to any of the investment products or services offered by members of the CoinShares Group.

Digital assets and related technologies can be extremely complicated. Crypto-currencies can be extremely volatile and subject to rapid fluctuations in price, positively or negatively. Crypto-currencies are loosely regulated and there is no central marketplace for currency exchange. Supply is determined by a computer code, not by a central bank, and prices can be extremely volatile. The digital sector has spawned concepts and nomenclature much of which is novel and can be difficult for even technically savvy individuals to thoroughly comprehend. The sector also evolves rapidly.

With increasing media attention on digital assets and related technologies, many of the concepts associated therewith (and the terms used to encapsulate them) are more likely to be encountered outside of the digital space. Although a term may become relatively well-known and in a relatively short timeframe, there is a danger that misunderstandings and misconceptions can take root relating to precisely what the concept behind the given term is.

The purpose of this document is to provide objective, educational and interesting commentary and analysis in connection with the cryptocurrency market. This document is not directed at any particular person or group of persons. This material is solely for informational purposes and shall not constitute an offer to sell or the solicitation to buy securities. Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of CoinShares (UK) Limited ("CSUKL"), which is the issuer of this document, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and/or obtained from sources believed to be reliable; however, the CoinShares Group (which includes CSUKL) does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the date indicated. Any forward-looking statements speak only as of the date they are made, and the CoinShares Group assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time.

Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

CSUKL is an Authorised Representative of Sapia Partners LLP, which is authorised and regulated by the Financial Conduct Authority (FRN: 550103). The address of CSUKL is Octagon Point, 5 Cheapside, St. Paul's, London, EC2V 6AA.

This document is subject to copyright with all rights reserved. Use and reproduction of this document or any parts thereof may be done without permission, however, the following citation should accompany any reference to or other use of the information contained in this document: CoinShares Research H1 2018 Crypto Report.

