CoinShares Research

ASSET HIGHLIGHT: ETHER

In addition to its potential as a platform, Ethereum's native token, ether, has also emerged as an investable crypto-asset. To properly assess the investment potential of this emerging asset, we aim to provide readers with context surrounding the asset via: a quick overview of the Ethereum platform and its component parts; a discussion about current and future growth drivers and related metrics; an examination of price, volume and transaction trends; a look at ether as a portfolio tool; and finally a brief overview of some of the largest risks to the platform and corresponding token.

This Page is Intentionally Left Blank

TABLE OF CONTENTS

PLEASE REVIEW THE DISCLAIMER ON PAGE 17

Certification Concerning Research Analysts

The research analyst(s) denoted by an "AC" on the cover of this report certifies (or, where multiple research analysts are primarily responsible for this report, the research analyst denoted by an "AC" on the cover or within the document individually certifies, with respect to each security or issuer that the research analyst covers in this research) that:

(1) all of the views expressed in this report accurately reflect his or her personal views about any and all of the subject securities or issuers; and

(2) no part of any of the research analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the research analyst(s) in this report.

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 Ethereum and its 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 like ether.

ETHER BACKGROUND

Ethereum is the brainchild of informatics prodigy and Bitcoin Magazine cofounder Vitalik Buterin. Borne from a perceived lack of flexibility in the Bitcoin scripting language, Buterin developed the idea of a cryptocurrency whose scripting language could handle programs of arbitrary complexity. This, in turn, would enable smart contracts of any imaginable kind, to be run on a global virtual machine, itself comprised of a decentralised network of nodes.

In order to code up his specification, Buterin enlisted the input and assistance of Gavin Wood, Jeffrey Wilcke, Charles Hoskinson and several others. With their help and influence, two implementations of Ethereum began taking form, one written in C++ (Parity) and one in Go (Geth) [1].

Buterin then embarked on a worldwide fundraising journey under the legal umbrella of the newly created Ethereum Foundation, a Swiss non-profit "stiftung". Its mission as of October 2018 is to "to promote and support Ethereum platform and base layer research, development and education to bring decentralised protocols and tools to the world that empower developers to produce next generation decentralised applications (dapps), and together build a more globally accessible, more free and more trustworthy Internet".

The Ethereum Foundation was able to bootstrap protocol development with investor funds before taking the network live by offering early investors access to pre-mined ether tokens via an Initial Coin Offering (ICO),

At the time, this was the largest and most successful ICO ever executed. Buterin and his team sold a total of 60 million ether (~59% of total supply in October 2018), netting more than 31,500 BTC, worth around $18 at the time [2]. Additionally, on top of the coins sold to investors, 12 million pre-mined coins were also distributed to developers and various other internal stakeholders.

With development funding secured, work on implementations rapidly progressed through a series of Proof-of-Concepts culminating in the creation of a functioning testnet, Olympic. After a lengthy security audit and multiple months running on Olympic, Ethereum finally went live with the creation of the genesis block on 30 July 2015, at 3:26 PM UTC.

The first release, or Ethereum era, was fittingly named Frontier. It was followed in turn by the Homestead release marking the dawn of the second era. We are now in the third era of Ethereum after last year's Metropolis (Byzantium) release. The fourth and final era, Serenity is expected sometime in the 2020's.

TECHNOLOGY & ARCHITECTURE

As suggested by the title of its whitepaper, the intent of Ethereum is to act as a protocol allowing developers to build and run decentralised consensus-based applications and smart contracts. These applications are executed on a public blockchain and allow for the distribution of computational tasks across a network of nodes in exchange for market driven fees. The idea is to leverage the censorship resistance of a blockchain to make a platform for "unstoppable applications" [3].

DEEP DIVE: SMART CONTRACTS

The term smart contract was first described in a publication of the same name posted by Nick Szabo in 1994 [4]. In this short essay, Szabo described a smart contract as "a computerised transaction protocol that executes the terms of a contract".

In other terms, a smart contract is a piece of code which automates the execution of an agreement between two parties based on the inputs it is given.

Some examples employed to illustrate potential uses of smart contracts include: automated liens which transfer control of loan-financed assets based on payment histories; trustless escrow; and trustless bets or lotteries.

Consider the following possible smart contract bet (in pseudocode) on the outcome of A which has two possibilities, X and Y:

1. Alice pays 10 ETH to the smart contract
2. Bob pays 10 ETH to the smart contract
3. The outcome of A can be X or Y
4. The source of the outcome of A is B
5. If B says the outcome of A is X, Alice receives 20 ETH
6. If B says the outcome of A is Y, Bob receives 20 ETH

Committing the execution of the above contract to a decentralised system like Ethereum ensures that no third party influence over its execution is possible.

TECHNOLOGY & ARCHITECTURE

To achieve this the Ethereum protocol comes with a Turing-Complete programming language named Solidity. This approach stands in stark contrast to the design of Bitcoin, whose built in programming language, Script, is explicitly not Turing-Complete.

In short, this means the protocol can be programmed to perform any calculation possible by any other programmable computer, allowing for the execution of arbitrarily complex computations [5]. A smart contract is then a piece of cryptographic code that will perform a subset of computations, as set out by the developer.

Bitcoin is theoretically also a smart contract platform, but one that is restricted to value transfer transactions of limited complexity. Ethereum smart contracts on the other hand, can perform whatever task developers wish to assign to them. Smart contracts are read and executed by every single node in the Ethereum Network, through a protocol feature called the Ethereum Virtual Machine (EVM).

ETHER

A central underpinning concept of the Ethereum blockchain is the value token called 'ether' (ETH). Ether is used as the denomination of all value-transfer functions on the network and is the currency in which the 'gas function' is valued. Gas is, not unlike combustion engines, what makes applications run on the Ethereum network. It acts as remuneration for offering computational power to the network for use by decentralised applications (dapps) and is claimed by miners as a fee for providing computational power to the network.

This fee paid to execute an operation on the EVM is calculated by multiplying *gas cost* by the *gas price*. *Gas price* refers to the exchange ratio between gas and ether. *Gas cost* refers to how many units of gas must be paid *per operation*.

The *gas cost* is fixed and determined by the protocol. An overview of gas costs can be found in Appendix G of the Ethereum Yellow Paper. As an example, a single transaction, such as sending Ether between two wallets, costs 21,000 gas, whereas complex operations such as executing a smart contract, which may contain numerous transactions, will cost a larger amount of gas.

The *gas price* is set by market forces as users can individually determine the price that they are willing to pay per gas. However, the higher the gas price a user sets, the faster the transaction is likely to be processed by the network. This is because each block in the Ethereum blockchain can only process a limited amount of transactions, measured in gas.

Because every single Ethereum node executes every single operation of all smart contracts and applications committed to the Ethereum network, there is a gas limit imposed on each block in order to prevent overloading the nodes.

The gas limit is decided by committee vote among Ethereum developers and is currently set to 8 million gas. This roughly corresponds to 381 transactions per block.

Limiting the block size also creates a fee market as miners are incentivised to process the transactions with the highest paying fees.

ETHEREUM CONSENSUS MECHANISM

Nodes arrive at consensus through proof-of-work. We have previously described this style of consensus mechanism in our Bitcoin Asset Highlight and refer any interested readers there for a more thorough treatment of its principals.

Ethereum uses a composite consensus algorithm called Ethash in its Proof-of-work. Ethash is an amalgamation of Dagger—a calculation structure based on a directed acyclic graph (DAG)—and Hashimoto—a proof-of-work algorithm written by Thaddeus Dryja. The combined properties led to the dominant limiting factor in Ethash mining speed not being hashes per second, but megabytes per second of RAM access [1].

Although Ethereum currently utilises proof-of work, developers have expressed a long-stated intent to migrate Ethereum to a consensus protocol based on proof-of-stake. This intent manifests itself in the current protocol via the 'difficulty bomb', a piece of code causing an exponential increase in mining difficulty over time regardless of hashrate.

The intent is for this mechanism to avoid another Ethereum chain spilt upon activation of the proof-of-stake mechanism by rendering mining on the forked chain impossible. While originally aimed at taking full effect in 2017 the timing of the difficulty bomb has been reset multiple times in order to allow more research to be conducted on proof-of-stake.

No final specification of Ethereum's proof-of-stake protocol—lovingly nicknamed Casper—has been released at the time of writing. Some of its probable attributes have been discussed in public however, giving some limited insight into its proposed structure.

A complete discussion of the merits of proof-of-stake as they compare to proof-of-work is well outside of the scope of this paper, but for interested readers we

TECHNOLOGY & ARCHITECTURE

recommend the corresponding proof-of-stake Deep Dive further down on this page, the Risks section at the end of this document, as well as the following sources [6, 7, 8, 9, 10, 11, 12, 13, 14, 15].

DEEP DIVE: PROOF-OF-STAKE

Proof-of-stake is a consensus model whereby the 'voting power' of miners with respect to the creation of new blocks is proportional to their token holdings, not their cumulative computing power.

Comparing by contrast, under proof-of-work, the more common and proven consensus model pioneered by Bitcoin and currently employed in Ethereum, miners freely compete to find solutions to a cryptographic computer 'puzzle'. The respective 'voting power' of miners with regards to block creation is therefore proportional to how much real-world computer hardware each miner supplies.

This causes block creation to have externalised costs against which internal token rewards are given as incentives. Miners are therefore incentivised to act in the best interest of the system lest they risk devaluing their only means of recovering their hardware investment, that is selling their reward tokens on the open market.

Furthermore it safeguards the openness of the system by ensuring that entering the pool of validators is possible for anyone willing and able to make the required investment in hardware regardless of the desires of current protocol stakeholders.

Proof-of-stake is an attempt at a completely different approach to consensus formation. Here, network participants can only become block validators by acquiring protocol tokens and prove holdings above certain minimum levels.

Validation privileges are then afforded proportionally based on the size of the holdings of prospective validators. Tokens would be locked up in staking accounts and would earn nominal returns proportional to the size of the stake.

If successful the model would virtually eliminate the expensive creation paradigm of the proof-of-work model. Block creation under proof-of-stake would carry no expenditure beyond that of block validation, which is comparatively negligible and in any case unavoidable.

Continued --->

PROOF-OF-STAKE CONTINUED...

The required expenditure to reach consensus would thus be nearly zero. A transfer of wealth from e.g. US dollars to ether does not expend any meaningful amount of any scarce resource and is a capital transformation, not an expenditure. Any cost of staking would therefore have to refer to the opportunity cost of keeping staked ether immobilised.

A system like proof-of-stake would also serve to protect active stakers from Ethereum's perpetual inflation by distributing all newly created coins among them, equalising its effects on the holdings of stakers.

The way we see it, the fundamental difference between the two systems can be expressed as a trade-off between 'trustlessness' and consensus cost:

In proof-of-work, *trust* is minimised by relying on externalised cost as a sufficient factor for the system to arrive at distributed consensus.

In proof-of-stake, *cost* is minimised by relying on internalised trust as a necessary factor for the system to arrive at distributed consensus.

Ethereum developers are of the opinion that the additional trust required by a proof-of-stake system is a small and reasonable addition to the existing trust requirements already placed on protocol developers and source code hosts [14].

THE ETHEREUM VIRTUAL MACHINE

All transactions and smart contracts submitted to the Ethereum system are executed by the Ethereum Virtual Machine (EVM). This virtual machine is a runtime environment which operates much like any other virtual machine—such as running Windows on your Mac—by executing code on host machines according to its own internal specifications.

The EVM is a 256-bit register stack, sandboxed and fully isolated from the host system. All Ethereum nodes run an implementation of the EVM and therefore executes all of the same instructions as the rest of the network.

Instructions (smart contracts) can be written in several languages including the native Solidity, LLL, Mutan and Serpent.

SECOND LAYER APPLICATIONS

As previously discussed in both our Bitcoin and Litecoin Asset Highlights, blockchains cannot scale at the base layer while simultaneously retaining its decentralised

TECHNOLOGY & ARCHITECTURE

properties. A short version of this issue can be constructed as such: For any node to verify in a trustless manner that the current state of Ethereum is the true state, they need to keep a copy of the entire blockchain, that is, the complete history of all transactions ever made. However, if the system is to act as a 'world computer' the size of this dataset would be enormous and clearly outside the ability of most users to keep on their computers.

The increasingly acknowledged solution to this fundamental property is by scaling via layered architecture such as Bitcoin's Lightning Network. This solution moves smaller, less valuable transactions (or smart contracts) requiring less trust and more speed to higher protocol levels, leaving the base layer as a final consensus authority.

There are a couple active proposals for second layer scaling of Ethereum. One called Raiden and another called Plasma. Both propose the use of state channels as conduits for increasing the execution capacity of the EVM [16, 17] .

Instead of running the computations directly on the EVM, users would buy computational capacity directly from other users using another second layer protocol protected by codified checks and balances.

Upon finishing the execution of the code, the computation provider would present the output along with a bonded amount of ether used as 'security' for the truthfulness of the solution. Any other network member could then check the solution to see if it is indeed correct. If not, it could then be deferred to the base layer which will act as a final judge on the dispute.

The underlying idea is that participants, knowing that they are liable to be punished for provably bad behaviour, would be incentivised to act in good faith, thereby securing the accuracy of the system and providing assurance to computation buyers.

SHARDING

Another proposed scaling solution involves splintering the base layer into multiple separate 'shards', each responsible for handling its own subset of computations [18].

Sharding is a relatively common technique employed in database scaling and can be thought of as reducing system redundancy by partitioning the total data set such that network participants only need to hold a smaller part, instead of the entire set.

zkSNARKs

A recently added feature in the Ethereum protocol are zero-knowledge Succinct Non-interactive ARguments of Knowledge or zkSNARKs for short. Introduced in the Byzantium hard-fork of late 2017.

Without going into too much detail—those interested in the nitty gritty can delve fairly deep down here [19]—among other improvements, zkSNARKs enable vastly increased levels of privacy for Ethereum transactions. This in turn adds to the fungibility of ether tokens and reduces the ability of miners to censor execution of specific code on the EVM.

UTILITY & GROWTH OPPORTUNITIES

SMART CONTRACT PLATFORM

Ethereum and its ether token is an embodiment of the desire for a fully programmable money. The boundless flexibility offered by Ethereum's Turing Completeness enables a near unlimited amount of monetary applications with built-in contract settlement.

Any attempt to enumerate all such applications is vain as the potential of the platform allows for the creation of applications not yet imagined. Among those already conceived of, we mention tokenised securities, derivatives and organisations (DAOs), prediction markets, trustless escrow and betting, attestation, multisignature and time-locked contracts as some of the most interesting and immediately promising potential applications.

SMART CONTRACT SETTLEMENT LAYER

As briefly discussed in the Technology and Architecture section, a future potential role of the Ethereum base layer is that of a settlement arbitrator for upper layers of high volume smart contract throughput.

In such a role, the base layer is envisioned to act as a sort of digital 'supreme court' where any potential disputes arising in the upper layers would be settled.

DISTRIBUTED WORLD COMPUTER

Regardless of whether the functionality at scale is achieved on the base layer or in upper layers, the overarching goal and ultimate potential of Ethereum is to act as a distributed world computer.

The hope is that a common underlying protocol standard for sharing of computational resources will cause all sellers and buyers to converge on a common platform where a global market for the purchase and delivery of such services will emerge.

If successful as envisioned, this would completely revolutionise the market for computational resources

UTILITY & GROWTH OPPORTUNITIES

and enable a new era of global standards, prices and accessibility. Any user, without regard for identity or location could access a global market for computation and execute any profitable code without the possibility of censorship* or arbitrary restriction.

ETHER AS DIGITAL OIL

Whereas bitcoins are often likened to digital gold, ether has more in common with digital oil. The analogy is quite fitting when considering the role of ether as 'gas' in the execution of code on the Ethereum Virtual Machine.

It remains to be seen if the analogy will hold also in terms of asset behaviour. Digital commodities with industrial utility as computational fuel are entirely novel and we are watching their development with interest.

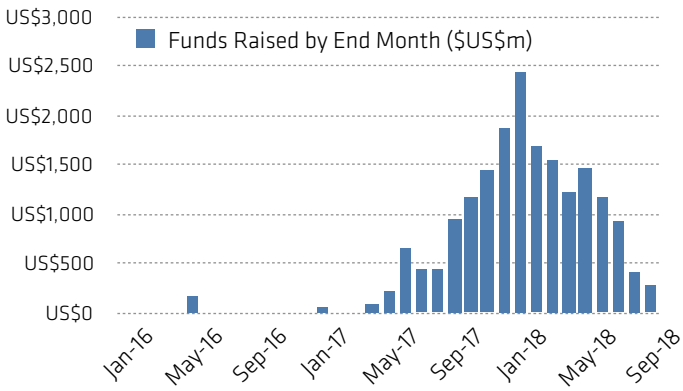
CAPITAL FORMATION PLATFORM

While ICOs predated Ethereum, the explosive growth in the issuance and sale of tokens which we have observed over the last couple of years owes much of its effect to Ethereum's ERC20 token standard.

There are a multitude of aggregators of ICO data all using different methodologies. All have their own individual merits and issues and it is unlikely that any single aggregator has been able to perfectly measure the total amount invested in ICOs.

In Figure 1 we show monthly cumulative funds raised by all ICOs as measured by Autonomous Next.

fig. 1 Monthly Cumulative Funds Raised by ICOs



Sources: Autonomous Next, CoinShares Research

Out of these figures, ICO Watch List estimates that Ethereum captured approximately 83% of total market share.

While the 'wild west' phase of capital formation using unregulated ICOs has cooled significantly, the potential for security token issuing is vastly larger than that of tokenised start-up funding and Ethereum is well placed to compete for market share in the fight for security token offerings.

* See Risks section for further discussion of the issue of censorship resistance on the Ethereum platform

SPECULATIVE VALUE & METRICS TO WATCH

In this section we have mapped some possible drivers of growth in the utility value of the underlying Ethereum network as well as a selection of metrics which may offer insight into protocol usage and development.

We caution however that all metrics are single components in an aggregate system and thus affects network value in a compound manner. The section bears close resemblance to its sister sections in our Bitcoin and Litecoin Highlights since many of the relationships highlighted are equally interesting for most cryptocurrencies.

Speculation plays a substantial role in driving the ether price and is influenced heavily by the performance of other cryptocurrencies and the market as a whole. There are many other decentralised tokens with which ether competes on both technical and speculative fronts and their relative performance over time has an impact on speculative belief. One trend to watch when evaluating performance is the overall dominance (share of the decentralised token market's outstanding value) of ether among competitors.

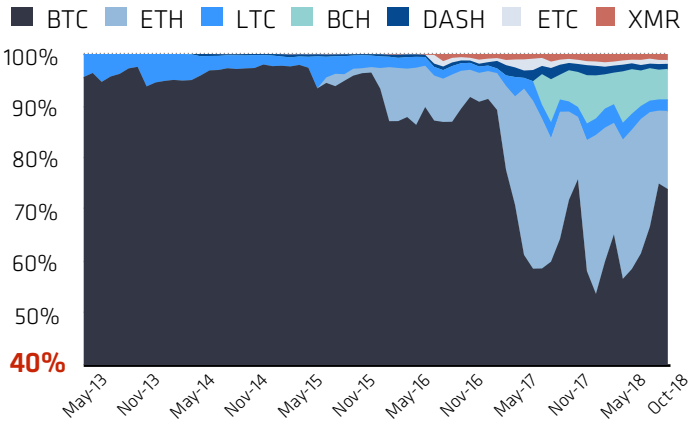
DOMINANCE

We measure dominance among crypto assets as the percentage of cumulative network value (modelled on conventional market capitalisation). Since its first publicly-priced trades, ether has seen its unit value rise from a few dollars to a peak of more than $1350. Even in the face of widespread new competition, ether has steadily remained the second largest mineable crypto asset since overtaking litecoin in 2016 (Figure 2, next page)

But more than merely measuring each currency's relative valuation/standing, the long-term dynamics of the dominance curve can illuminate trends in funding patterns between competing protocol technologies. As systems develop, each addition or reduction of value to the codebase should elicit organic responses in the volume and momentum of funding flows between coins as investors re-weight their holdings based on their belief in the viability of the technologies.

SPECULATIVE VALUE & METRICS TO WATCH

fig. 2 Cryptocurrency Dominance as Percentage of Combined Market Cap Since Bitcoin Launch

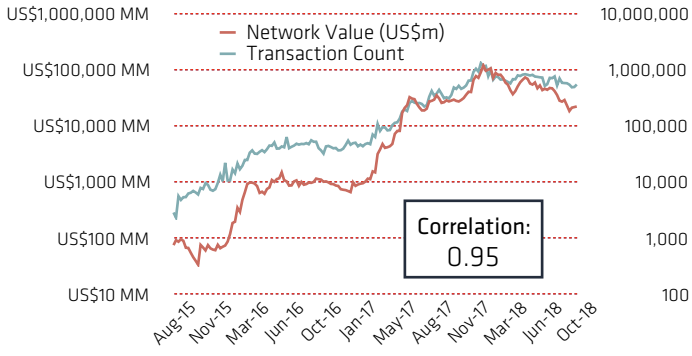


Sources: coinmetrics.io, CoinShares Research

TRANSACTION VOLUME

Speculative value in ether is part-driven by future expectation of utility, tuned by current level of hype. One indicator many digital asset speculators watch as a relational indicator of both price and network value is the development of daily on-chain transaction volume as a proxy for adoption and growth in usage. We observe a very strong correlation between daily on-chain ether transaction volume and network value (Figure 3). We do also caution that as blocks reach their max capacity and casual transactions increasingly move to second layer applications, this metric is likely to lose relevance.

fig. 3 Network Value vs. Daily Ethereum On-Chain Transaction Volume (# of Transactions)



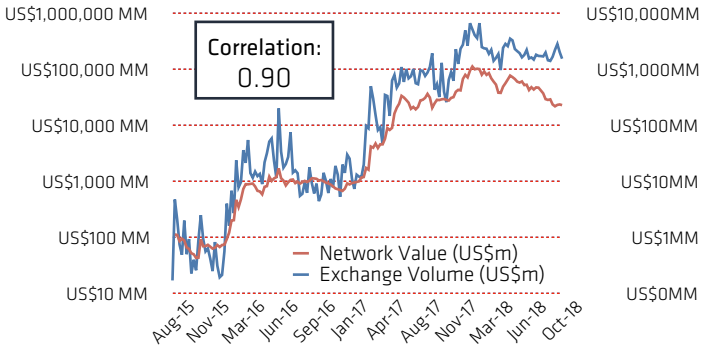
Sources: coinmetrics.io, CoinShares Research

EXCHANGE VOLUME

We also observe a strong correlation between exchange traded volume (US$) and Ethereum network value (Figure 4). However, because exchange volume (US$) and network value (US$) both contain the ether price as components of their calculation, this may create an inflated sense of covariance.

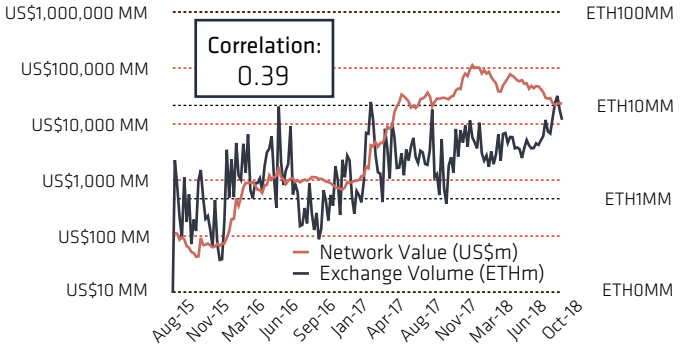
To standardise the relationship, one can look at ether-denominated exchange traded volumes. These have grown since inception, an impressive statistic given the meteoric rise of the ether price. This relationship does, however, correlate much less strongly than dollar denominated volumes versus network value (Figure 5).

fig. 4 Network Value vs. Exchange Volume



Sources: coinmetrics.io, CoinShares Research

fig. 5 Network Value vs. ETH Exchange Volume



Sources: coinmetrics.io, CoinShares Research

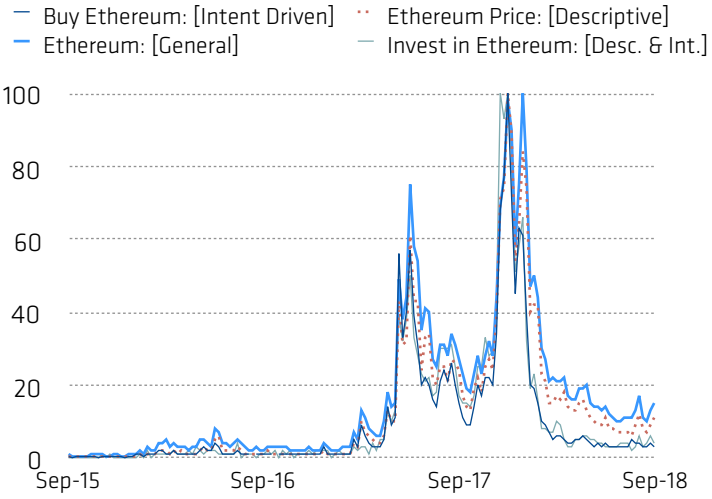
SEARCH TRENDS

Three-year Ethereum search trends reveal strongly hype-driven cyclical interest spikes of increasing magnitude (Figure 8). The peaks correlate closely with historical spikes in ether price and the corresponding media coverage. Overall this suggests a market that has thus far been reactive to cyclical speculation on future utility value.

In our searches we have assumed that the majority of people looking for for information regarding Ethereum are unaware that the monetary unit is called ether and that they instead are searching for 'ethereum' terms even when looking for price information.

SPECULATIVE VALUE & METRICS TO WATCH

fig. 6 GOOGLE SEARCH TRENDS FOR ETHEREUM TERMS



Source: Google Search Trends, CoinShares Research

Even though the baseline search volumes are somewhat drowned out by the sheer magnitude of the spikes, they do reveal a slow but steady increase in long-term search interest. Current general Ethereum interest is roughly half that of the same time last year, but more than eight times that of two years ago.

Table No.1	2015	2016	2017	2018 (YTD)
Returns	24%	773%	8825%	-70%
Volatility	224%	131%	136%	93%

Sources: coinmetrics.io, bitinfocharts.com CoinShares Research

INVESTMENT CASE OF US$ 10,000

As a relative comparison it can be helpful to index a potential set of portfolio components to see how they perform in relation to each other. In this case, the index would start each asset with a US$ 10,000 investment exactly 3 years prior to the date of writing (9 October 2018). For comparison - we've chosen a basket of commonly invested assets (S&P 500, Nasdaq Composite, Gold and Brent), versus the performance of ether.

The development is remarkable. After briefly dipping below $10,000 for a few weeks, the ether began a series of spectacular bull runs. Before 6 months had passed, ether had already broke the 10x mark before languishing through most of 2016 at a relatively moderate pace.

At the end of 2016 it briefly touched the 10x mark again before climbing rapidly past 100x. It then tempered its growth through most of the summer of 2017 before embarking on yet another bull run.

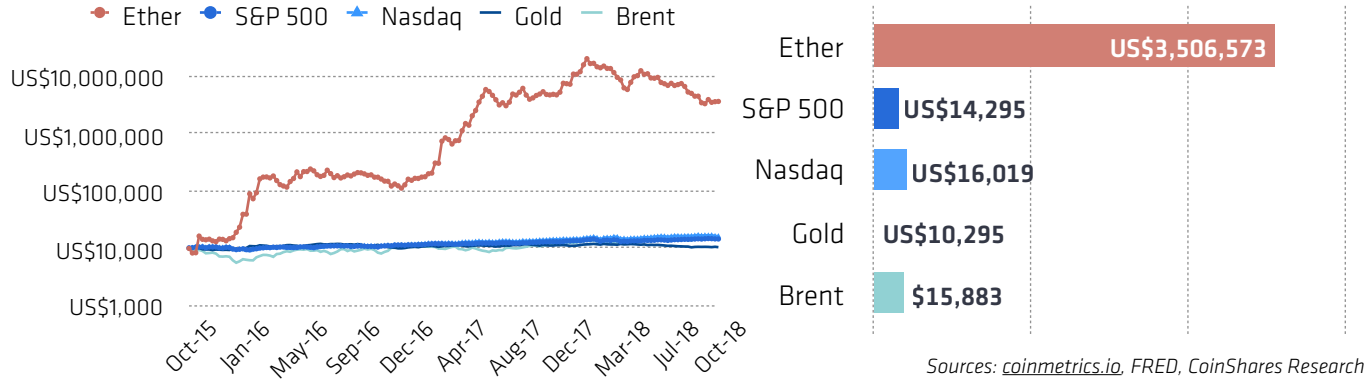
The late 2017 run-up saw it break the 1000x mark around the end of the year, topping out at almost $20,000,000. This peak marked the beginning of the longest and deepest bear market in the history of ether, shaving more than $16,000,000 off its peak values to the current value of $3,500,000.

While prices have come far off their tops, the initial investment would have returned 350x.

ASSET PERFORMANCE & CORRELATIONS

As is the case with many crypto assets, measuring pure asset returns over the entire lifetime of ether will return figures that verge on the absurd. Table one gives an overview of the annual returns and volatility of ether since 2015.

fig. 7 3-YEAR DEVELOPMENT OF US$ 10,000 INVESTED IN COMMON INVESTABLE ASSETS



Sources: coinmetrics.io, FRED, CoinShares Research

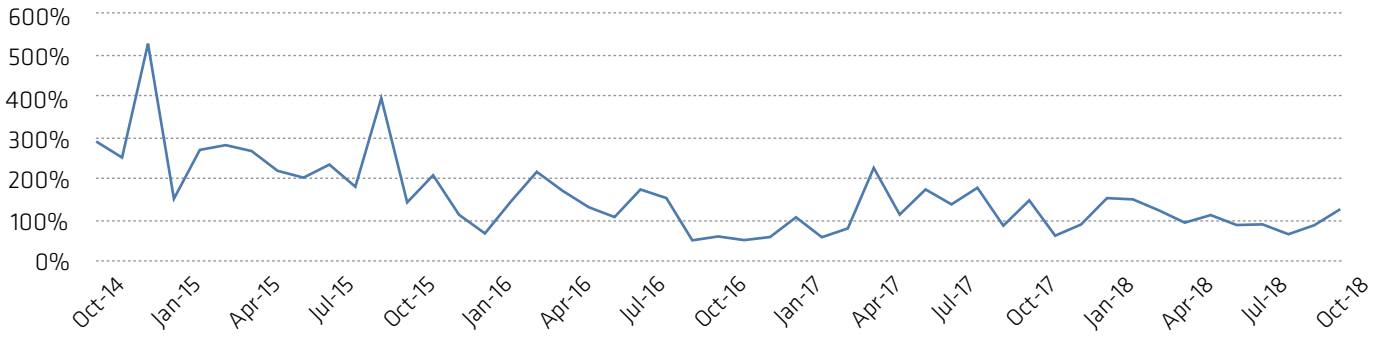
ASSET PERFORMANCE & CORRELATIONS

fig. 8

ETHER VOLATILITY OCTOBER 2014 - OCTOBER 2018
(30-DAY ROLLING ANNUALISED STANDARD DEVIATION OF DAILY RETURNS)

VOLATILITY

However, in order to access returns on these levels, ether investors must withstand severe volatility. Looking at historical annualised figures for ether, we observe that the multi-year trend of falling volatility was broken in 2017 as hefty price action yet again caused large increases in volatility (Figure 8). While we suspect volatility might dampen over time as the price reaches maturity, ether still behaves like a growth asset requiring substantial risk tolerance on the part of investors.



Sources: coinmetrics.io, CoinShares Research

RISK-ADJUSTED RETURNS

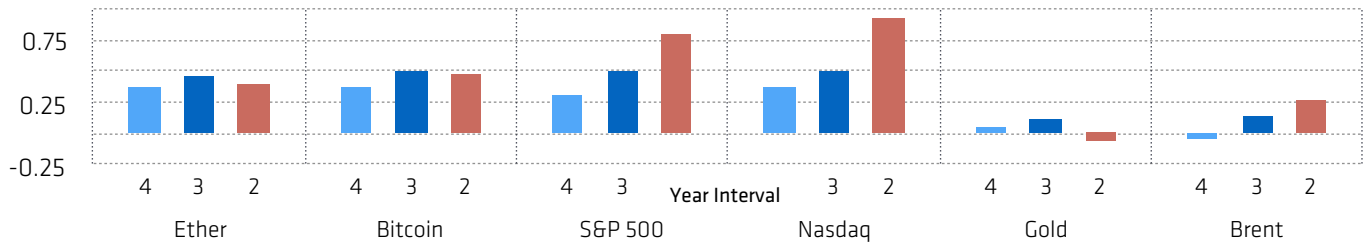
Neither pure returns nor volatility alone suffice as metrics for prudent portfolio allocation. Because assets are inherently different and incorporate unique risks, returns and volatilities, one must also look to risk-adjusted measures in order to achieve a valuable comparison.

Sharpe Ratios offer one method of comparing returns on the basis of standardised volatility measures. First, pure returns are discounted by a risk-free investment rate, represented by 3-month U.S. Treasury bills. Average excess returns above the risk-free rate are then divided by the price volatility of the asset, represented by the standard deviation of the excess returns. Assets with the highest Sharpe Ratio offer the best compensation to investors for the level of risk they are taking.

Ether is an extremely volatile investment asset. Even so, when applying the Sharpe Ratio to ether and a basket of commonly investable assets, ether scores moderately well against stock indexes like the Nasdaq and S&P 500 while consistently beating commodities like gold and oil (Figure 9).

fig. 9

(4-2YR) SHARPE RATIOS - MONTHLY RETURNS (VS. 3-M US TREASURY BILL) OF COMMON ASSETS



Sources: coinmetrics.io, FRED, US Treasury, CoinShares Research

RETURNS COMPARED TO COMMON ASSETS

One of the most exciting attributes of the cryptocurrency space is highlighted in Table No. 1 (Page 9): Whereas assets with similar returns (and risks) have largely been unavailable to anyone outside the venture capital industry, the open nature of crypto-markets has made high-risk/ high-return assets accessible to a much wider public. The 3-month returns in Table No. 2 (next page) makes the risk/reward relationship of the crypto-space compared with more 'traditional' assets abundantly clear.

ASSET PERFORMANCE & CORRELATIONS

Table No.2	Ether	Bitcoin	S&P 500	Nasdaq	Gold	Brent
Q4 2016	-40%	58%	3%	1%	-13%	14%
Q1 2017	527%	11%	6%	10%	9%	-5%
Q2 2017	486%	133%	3%	4%	0%	-10%
Q3 2017	3%	74%	4%	6%	3%	21%
Q4 2017	151%	225%	6%	6%	1%	17%
Q1 2018	-47%	-50%	-1%	2%	3%	3%
Q2 2018	15%	-8%	3%	6%	-6%	12%
Q3 2018	-49%	1%	8%	7%	-5%	7%

Sources: coinmetrics.io, FRED, CoinShares Research

CORRELATIONS OF RETURNS PER ASSET

Extending the discussion on comparative returns, Table No. 3 (below) shows the 2-year correlations between the daily returns of ether since October 2016 against the same set of assets as in Table No. 2 above, using Pearson's Correlation Coefficient.

The inclusion of uncorrelated assets into a diversified asset portfolio generally serves to lower its overall volatility. Thus, large movements in single assets only affect the overall portfolio value in a dampened manner as the probability of all assets moving together is low. Conversely, if all portfolio components move in unison there is an increased propensity for the entire portfolio value to follow the movement of single assets and greatly diminishing diversification benefits.

The daily returns correlation between ether and traditional investment metrics such as the S&P 500, Nasdaq, Brent Crude and Investment Gold indexes is nearly zero. This property makes ether uniquely interesting as a portfolio-balancing tool for investors

Table No.3		Ether	Bitcoin	S&P 500	Nasdaq	Gold	Brent
2-Year Correlations of Daily Returns	Ether		0.39	0.031	0.026	0.051	-0.027
	Bitcoin	0.39		0.015	-0.001	-0.006	-0.005
	S&P 500	0.031	0.015		0.94	-0.101	0.22
	Nasdaq	0.026	-0.001	0.94		-0.092	0.15
	Gold	0.051	-0.006	-0.10	-0.092		-0.005
	Brent	-0.028	-0.005	0.22	0.15	-0.005	

Sources: coinmetrics.io, FRED, CoinShares Research

RISKS

Major risks to Ethereum can be roughly classified into three general categories: Personnel Risk, Technological risk, and attack/regulatory vulnerability, with certain cases of overlap. Here we outline the most pressing risks, as we see them, with the express caveat that we cannot possibly cover every conceivable one.

KEY PERSONNEL RISK

Ethereum, unlike Bitcoin has a well-recognised leader and figurehead whose persona acts as the ultimate decision authority in matters relating to vision and development. Ethereum is therefore vulnerable to the wellbeing, continued motivation and productivity of its founder and leader, Vitalik Buterin. If any detrimental event or series of developments should befall Buterin, there are significant risks of disruption to both the development team and the Ethereum Foundation.

Such disruption can range from power vacuums and infighting as current stakeholders vie for power over the future of the protocol to simple disagreements on protocol changes going unresolved for extended periods of time, potentially even leading to political chain splits.

Furthermore, Mr. Buterin acts as a single pressure point onto which outside detractors can apply threats, bribes or other unsavoury means to impose their will on the protocol development.

ATTACK 'SURFACE AREA'

It is easy to envision that the more moving parts are present in a mechanical device, the higher the overall chance that somewhere in the mechanism, there will be a malfunction. The same exact relationship exists between the general size of software source code and its probability of suffering from bugs and other unintended software behaviour.

In a similar fashion, computer programs with a larger codebase will, generally speaking, have a larger surface area on which attackers may operate.

When recalling how the Ethereum protocol's Turing

RISKS

Complete programming language can run benevolent programs of arbitrary complexity, it is then also important to realise that similarly, such capabilities exposes the protocol to malevolent programs of equally arbitrary complexity.

A continuous increase in Ethereum complexity can therefore be viewed as an ever-increasing risk of either detrimental malfunction within the protocol or of the possibility of a successful external or internal attack.

As a concrete example of increasing complexity, the proof-of-stake consensus mechanism Casper, is significantly more complex than the current ethash proof-of-work system.

INFLATION

The ether inflation rate is basically dependent on four variables, block frequency, block reward, Uncles and Uncle reward. Although these metrics are semi-predictable in a steady state, it is not possible to forecast the inflation rate with a high degree of accuracy. Initially, in the Frontier implementation, each block had a block frequency of approximately 17 seconds and carried a block reward of 5 ether. This frequency was self-adjusting, lending some statistical predictability to the base inflation rate. Because the block reward is static (see announced changes to this metric in next section), the base inflation rate was nominally flat—though exponentially decreasing on a percentage basis as the total coins in circulation increased—but the nominal issuance amount (in ether) remained more or less the same.

With the release of the Homestead upgrade, block frequency was lowered to approximately 14 seconds, increasing the nominal ether inflation rate by a little more than 13%. Then, with the release of the Byzantium hard-fork, the Ethereum block reward was reduced via committee vote from 5 to 3 ether per block. The committee has since voted to decrease this number further, from 3 to 2 ether per block, in the Constantinople hard fork.

There is widespread criticism levied towards Ethereum in the crypto community for their repeated tendency to alter the Ethereum monetary policy via committee decision, a mechanism more commonly associated with central banks.

Underneath both block issuance rates there exists a mechanism called the Difficulty Bomb, which is meant to make mining progressively and irreversibly more demanding, eventually grinding the proof-of-work system to a complete halt. This disincentive scheme is a part of the long-term plan to migrate the Ethereum consensus mechanism from proof-of-work to proof-of-stake and avoiding a chain spilt by disgruntled miners. The difficulty increase is exponential with a slow onset, aiming to start taking full effect closer to the latest proposed Casper implementation date in late 2019 or early 2020. The difficulty bomb has been reset once before by hard fork and is set to be reset once more with the Constantinople hard fork planned on 30 October 2018.

While block frequency is both a fairly easy concept to grasp and a somewhat predictable metric, even when the Difficulty Bomb is accounted for, Uncles are slightly trickier to understand. Whenever a miner is working on top of what they believe to be the most current block, s/he is running the risk that another block has already been mined on top of the current block and transmitted to the rest of the network before s/he could get the message. If the miner then discovers a block and attempts to propagate it through the network, it will be rejected since the rest of the network is already one block ahead. Such a block is referred to as orphaned or stale, and the incidence of stale blocks increases with block frequency as there is less time for blocks to be propagated across the network before the next one is found. This means that a blockchain with short block intervals, like Ethereum (~14 seconds), will have a higher incidence of orphaned blocks than slower confirming blockchains like Bitcoin (~10 minutes). Uncles are stale blocks with shared parentage that goes a maximum of six blocks back from the present block.

Unlike other protocols like Bitcoin in which stale blocks represent wasted energy on the part of the miner, Ethereum rewards Uncles with seven eights of the normal block reward, or 2.625 ether, with a maximum of two Uncles per block. The reward exists in order to lower overall block propagation times and strengthen the security of the network, but comes at the expense of introducing an additional and variable quantity of inflation.

Due to the variable nature of its inflation drivers, the lack of clarity on its future issuance model, and frequent developer intervention, there is no reliable way of knowing the future inflation rate of ether.

This is one of the core differences between dynamic development networks like Ethereum where the protocol undergoes frequent changes in the face of its fluctuating environment, and more conservative protocols like Bitcoin where parameters such as coin issuance and inflation rates are fixed for the lifetime of the network. There is an essential tradeoff between predictability and flexibility with Ethereum receiving regular crypto criticism for its willingness to frequently change the rules of supposedly immutable systems.

RISKS

SCALING

Cryptocurrency scaling is a highly complex problem that cannot be sufficiently covered in the scope of this paper. We will endeavour to give a surface-level overview of the problems that has received the most publicity but would like to stress that the matter is much more complicated than it first appears.

Under the current protocol, Ether transactions are limited to approximately 15-20 per second, depending on the size and type of the transactions. Ethereum, like Bitcoin has a blocksize limit—manifested as the gas limit—as a measure to blockchain bloat.

As we keep repeating, there exists an essential trade-off between on-chain transaction capacity and decentralisation. There are two reasons for this, but both relate to the cost of operating Ethereum nodes, affecting the number of network participants who could afford running a full node.

The first reason is cost of storage and validation: All full Ethereum nodes must validate all transactions and keep a full copy of the blockchain in order to verify transaction history back to the genesis block.

If every single computation executed by a world computer were to be recorded in the blockchain, it would grow by terabytes every hour, making it unrealistically expensive for almost anyone to run a node.

The second reason is bandwidth limitations. If blocks were on the order of gigabytes and kept their current frequency of approximately 14 seconds, one can easily see how few people would have access to fast enough internet connections to keep up with the blockchain.

RUNNING A FULL NODE IS COSTLY AND TECHNICALLY CHALLENGING FOR MOST USERS

Unlike mining nodes, regular full nodes are not directly compensated for their services by the network. Running a full node is in the self-interest of ether holders as it is the only way users can be certain that none of the protocol rules have been broken by other participants without relying on someone else's trusted information.

However, operating a node comes with a very real cost and normally requires separately dedicated hardware on the part of the user. Although there is specialised lower-cost hardware coming to market it is still expensive enough that only a subset of all users can be reasonably expected to have a separate computer running Ethereum.

There has been significant anecdotal evidence that it is becoming increasingly untenable for regular users—that is, users with 'common' computer hardware and internet connections—to sync the Ethereum blockchain. At the same time we are observing a drastic drop-off of data services offering Ethereum network topography data, making it difficult for researchers to gauge the development of the Ethereum network health.

In the process of writing this paper we have contacted the Ethereum Foundation, posted in multiple Ethereum gitter chat rooms, and attempted getting in touch with developers of Ethereum data provision websites to try and get hold of hard data to assess these issues, but none have been successful. While this is not itself proof of any reduction of node count or increased difficulty in participating in the Ethereum network it is certainly worrisome.

HARMFUL LEGAL OR REGULATORY ACTION

Although Ethereum, like any other distributed network, cannot effectively be shut down without finding and disabling almost every single network participant, it is still vulnerable to damage dealt to it by powerful state actors. Damage of this kind cannot realistically kill the network, but it can certainly inflict severe monetary loss on network participants and deal powerful blows to adoption and use.

While, for example, outlawing the software is entirely unenforceable, it would almost certainly drive many participants off the network for fear of government repercussions, causing negative price pressures. Overly burdensome regulation can have much of the same effect.

With the notable exception of a handful of undemocratic countries, state-level responses to most cryptocurrencies have thus far been measured and reasonable. Most governments have chosen to observe its growth and development, more or less leaving it alone so as to not stifle innovation. This is a very reasonable response to an ecosystem, whose total network value has until recently been lower than most Fortune 500 companies, however, we cannot assume this cautious approach will continue as the total network value of cryptocurrencies begins to approach the M1 value of major world currencies.

Furthermore, because Ethereum is closely related to the issuance of other crypto tokens through ICOs, and was itself an ICO, there is a significant risk of it getting entangled in potential regulatory issues stemming from ICOs being deemed unregistered securities.

MUTABILITY

Blockchain immutability is a hotly debated topic in the cryptocurrency space. Many protocols posit blockchain

RISKS

immutability as a key value proposition and an enabler and safeguard of their store-of-value and censorship resistance properties.

The argument is that the public record, being fully transparent and verifiable, should be permanent and unalterable once consensus is reached (in practice this immutability is statistical, but the probability of being able to alter a block in a proof-of-work chain exponentially decays towards zero with each successive confirmation after the block one wishes to alter). In other words, no one should have the power to alter deposits, add money supply at will or edit valid transactional history.

On the other side of the table the opposing view is held that ledgers cannot be immutable, because that removes all possibility of ever correcting 'mistakes' entered into the public record. On its website, the Ethereum Foundation advertises its capability of enabling developers to "write unstoppable code", and the de facto motto of the now defunct Distributed Autonomous Organization (DAO) was "code is law". In fact, the DAO code explicitly stated that its contents were to be the only rules governing its entire existence.

Shortly after going live with more than $150m of ether invested into its contract structure, an unknown coder or group of coders (the attacker) took advantage of properties in the open source DAO code, which were unforeseen by its developers, and drained it of more than a third of its funds.

Although the actions of the attacker were entirely allowed by the contract code, and the code was available for all investors to review for their own due diligence, the Ethereum Foundation nevertheless chose to publicly endorse and execute a hard fork of the blockchain, resetting it to an earlier state, and effectively rewriting the ledger history from a point before the creation of the DAO. This was effectively a bailout of DAO investors and the only one of its kind ever executed at a remotely similar scale in the cryptocurrency space. But more importantly, it was a complete violation of both the mantras of "unstoppable code" and "code is law", and potential investors need to be aware of any past discrepancies between stated intent and actions taken.

Opinions of the event still dramatically differ within the cryptocurrency community. Detractors cite it as a broken promise on the part of the Ethereum Foundation, and an invitation to moral hazard on the part of developers. Supporters on the other hand tout it as a great success of justice over what were clearly malicious actions on the part of the attacker.

We also recommend that prospective investors perform their own investigation into the events surrounding the DAO failure, the subsequent split of Ethereum into Ethereum and Ethereum Classic, and the role played by the so-called 'white-hat hackers'.

PROOF-OF-STAKE IMPLEMENTATION

As we have covered in previous sections of this paper there is a stated intent among Ethereum developers to migrate Ethereum over to a proof-of-stake consensus mechanism.

Previous attempts at securing protocols using proof-of-stake by other cryptocurrencies have been generally functional, but no system with a market value or adoption level anywhere near that of Ethereum has ever attempted such a radical change in consensus mechanism via hard fork on an already operating network worth dozens of billions of dollars.

Furthermore, even with the existence of the Difficulty Bomb, we deem it unlikely that Ethereum miners will accept the implementation of Casper without a fight. This leads to a chain split risk—which is the exact outcome the Difficulty Bomb is intended to avoid—whereby miners continue mining on the proof-of-work fork of Ethereum.

While the Difficulty bomb will make mining increasingly difficult on the original chain, we see no reason why miners cannot themselves simply hard fork to remove the Difficulty Bomb. After all, hard forks are regular occurrences in the Ethereum community so another one should not be any more problematic than the others.

In terms of functionality it is entirely unclear whether or not proof-of-stake will be a stable long-term consensus mechanism. While both Vitalik Buterin and Casper lead researcher Vlad Zamfir seem entirely convinced it can work, other more experienced researchers of distributed consensus are of the opinion that it is fundamentally at odds with the principle of trustless consensus [11, 15].

Proponents and detractors do seem to agree that proof-of-stake requires certain concessions in the trust assumptions of the security model, and the main disagreement rests on whether these concessions are material or not.

We leave it up to our readers to make up their own mind on whether proof-of-stake offers a justifiable trade-off between reduced energy consumption and reduced trustlessness, or not.

CITATIONS

[1] V. Buterin, "Vitalik Buterin's Website," 14 September 2017. [Online]. Available: https:// vitalik.ca/general/2017/09/14/prehistory.html.

[2] V. Buterin, "Reddit," 5 Septermber 2014. [Online]. Available: https://www.reddit.com/r/ethereum/comments/2fhmzm/ethereum_was_second_largest_crowdsale_in_history/.

[3] E. Foundation, "Ethereum," 2018. [Online]. Available: https://www.ethereum.org.

[4] N. Szabo, "Smart Contracts," 1994. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[5] "Wikipedia," 2018. [Online]. Available: https://en.wikipedia.org/wiki/Turing_completeness.

[6] Bitfury, 13 September 2015. [Online]. Available: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf.

[7] B. Research, "Complete guide to Proof of Stake," 11 April 2018. [Online]. Available: https://blog.bitmex.com/complete-guide-to-proof-of-stake-ethereums-latest-proposal-vitalik-buterin-interview/.

[8] V. Buterin, "Ethereum Blog," 25 November 2014. [Online]. Available: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/.

[9] V. Zamfir, "The Histtory of Casper Part 1," 7 December 2016. [Online]. Available: https://medium.com/@Vlad_Zamfir/the-history-of-casper-part-1-59233819c9a9.

[10] V. Zamfir, "The History of Casper Part 2," 7 December 2016. [Online]. Available: https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-2-8e09b9d3b780.

[11] V. Zamfir, "The History of Casper Part 3," 11 December 2016. [Online]. Available: https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-3-70fefb1182fc.

[12] V. Zamfir, "The History of Casper Part 4," 12 December 2016. [Online]. Available: https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-4-3855638b5f0e.

[13] V. Zamfir, "The History of Casper Part 5," 30 December 2016. [Online]. Available: https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-5-8652959cef58.

[14] V. Buterin, "Twitter," 15 August 2018. [Online]. Available: https://twitter.com/vitalikbuterin/status/1029900695925706753?lang=en.

[15] A. Poelstra, 22 March 2015. [Online]. Available: https://download.wpsoftware.net/bitcoin/pos.pdf.

CITATIONS

[16] R. Network, 2018. [Online]. Available: https://raiden.network/101.html.

[17] J. P. &. V. Buterin, "Plasma," 11 August 2017. [Online]. Available: https://plasma.io/plasma.pdf.

[18] Wikipedia, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Shard_(database_architecture).

[19] C. Reitwiessner, "Ethereum Blog," 12 May 2016. [Online]. Available: https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/.

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 ether markets and Ethereum protocol developments. 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.


CS
HE RBX 02
HE RBX 01
HE RBX 18