Education

Proof-of-Stake: A crypto path to lower energy consumption and yield

January 2022

IN PARTNERSHIP WITH

Summary

- As investors consider digital asset adoption, they are also concerned about the impact of energy consumption.
- Bitcoin's consensus mechanism, Proof-of-Work (PoW), consumes a large amount of electricity, with the Bitcoin network using as much energy as some small nations.
- Proof-of-Stake (PoS), an alternate consensus mechanism that eliminates the need for high computational power, is considered a popular solution for addressing crypto energy concerns.
- Ethereum, the second largest digital asset by market capitalization, is transitioning to a Proof-of-Stake consensus mechanism.
- Proof-of-Stake offers yield opportunities and its adoption may increase as the broader digital asset industry sees the effectiveness of yield as an incentive.

Overview

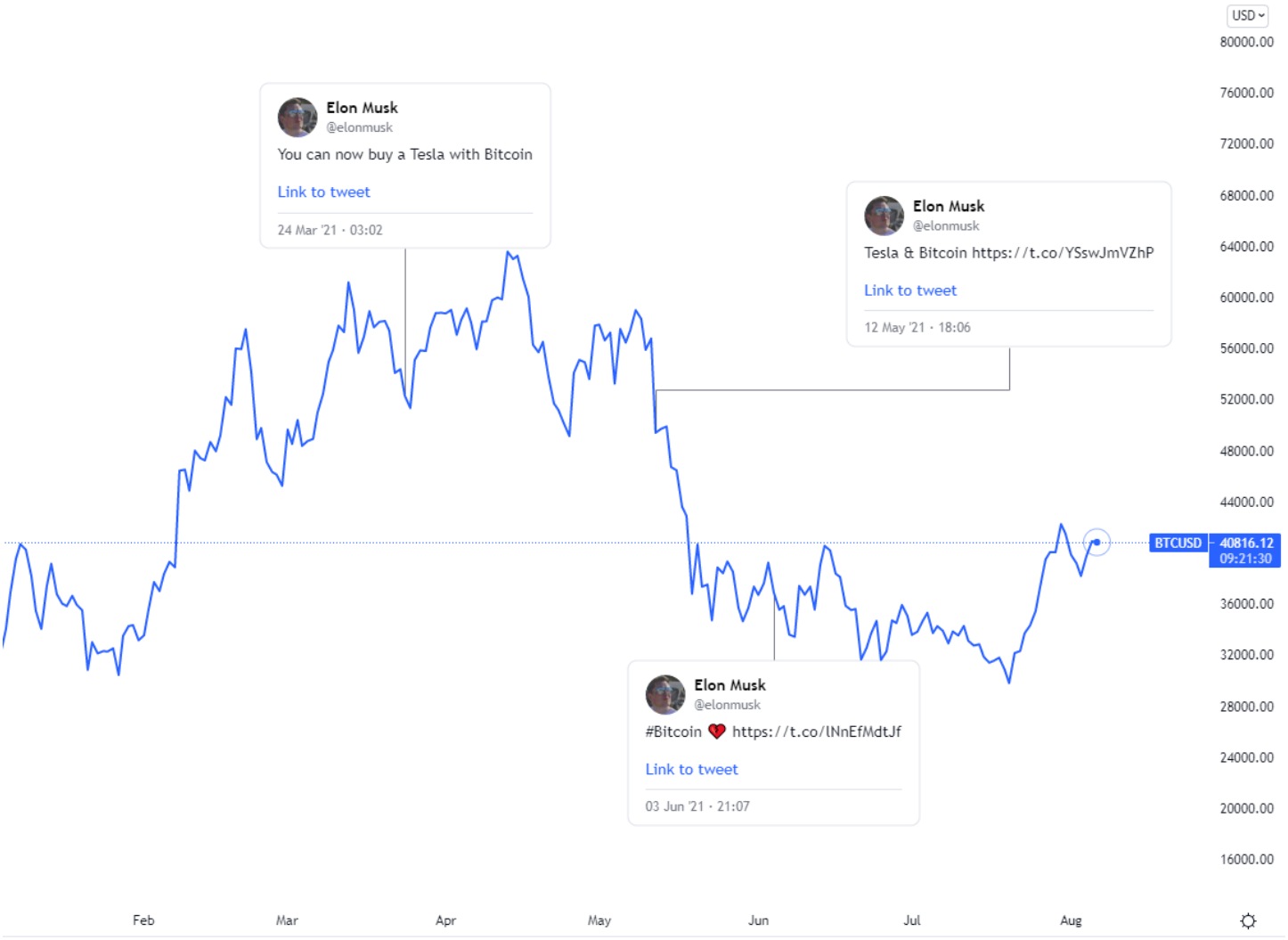
This report highlights conversations and developments related to energy usage concerns around digital assets, blockchains, and distributed ledger technologies (DLT), as well as initiatives by industry participants that are intended to address environmental concerns. As a popular solution, Proof-of-Stake and its role in providing yield opportunities is discussed. Our report is compiled from Digital Asset Research's (DAR's) data sources, public sources, media reports, and press releases, and, while wide-ranging, covers only representative initiatives related to environmental concerns in the digital asset space.

Digital asset energy usage concerns

Over the last several months, BTC has faced criticism due to the amount of energy that is consumed by mining activity on its network as it reaches agreement on a new block using a Proof-of-Work consensus mechanism. However, this is not a new narrative; concerns surrounding the energy used by the Bitcoin network to enforce its security and immutability have been brought up before, but are receiving additional attention now as BTC sees increases in institutional adoption and its asset price.

This concern was voiced by Tesla CEO Elon Musk to his 50+ million Twitter followers on May 12, 2021, when he posted a statement saying that Tesla would no longer accept BTC as a payment method due to concerns about the "rapidly increasing use of fossil fuels for Bitcoin mining and transactions." Musk's decision came less than two months after he originally announced that customers could buy a Tesla vehicle with BTC and drew significant news coverage. In the days following his reversal, BTC's price fell and the energy impact merits of BTC and other digital assets were heavily discussed in the media and by institutional investors.

Figure A – Elon Musk's environmental concern tweets and BTC price



Source: TradingView, Digital Asset Research

The proof-of-work problem

In blockchains, a consensus mechanism allows network participants to validate transactions and agree on the state of the network in a decentralized manner. Since its inception, BTC has used a Proof-of-Work consensus mechanism to sustain its security and immutability. As the network now attempts to scale and BTC's price increases, Proof-of-Work's issues are becoming more apparent.

Proof-of-Work requires network validators to solve a mathematical problem in order to become the designated entity responsible for the validation of the latest block and subsequently receive the rewards associated with mining the block. This mathematical problem is a one-way cryptographic function that cannot be solved without using computational power to brute force and test every possible solution; you can think of the method by which validators attempt to solve the mathematical problem similar to a person who tries every possible combination of numbers to get the correct PIN when withdrawing money from their bank account at an ATM.

The Bitcoin network's Proof-of-Work algorithm also adjusts the difficulty of the mathematical problem that validators must solve based on the total power allocated to the network to ensure that each block always takes approximately 10 minutes to generate. The lucrative rewards offered by the Bitcoin network for mining a block caused many entities to enter the Bitcoin mining business, which in turn increased the computation power required to mine a block and drove up energy usage because of the aforementioned adjustment mechanism. The more miners there are competing with one another, the higher the computational power necessary to mine Bitcoin.

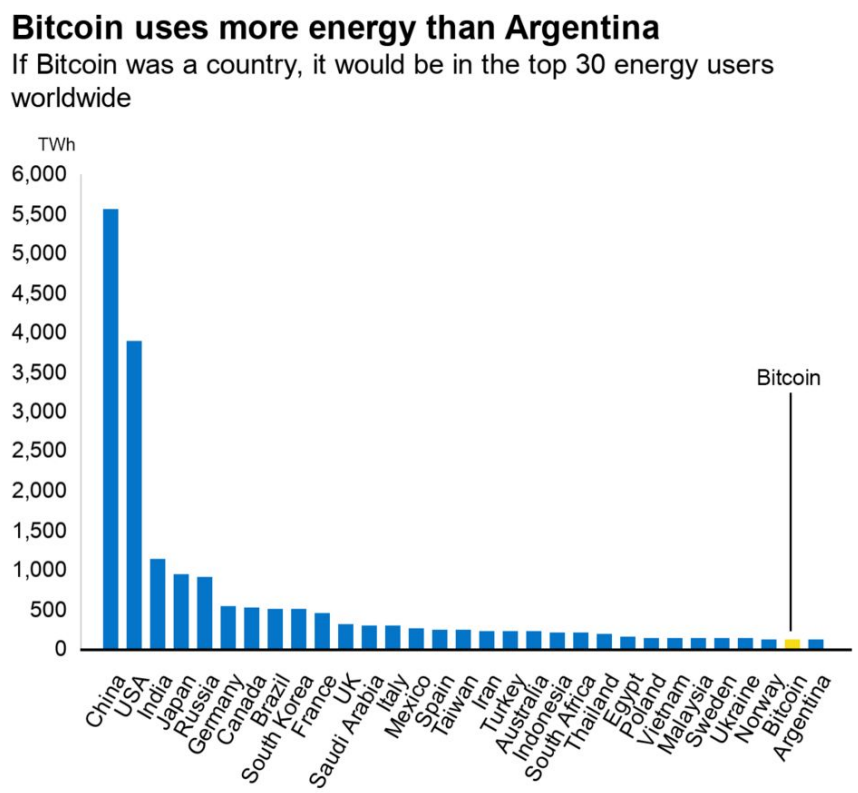
As BTC's price increases, miners are incentivized to allocate more computational power to the network, especially when the price increases significantly relative to the increase in the difficulty adjustment mechanism, which also can increase electricity consumption.

Figure B – Bitcoin historical network power demands

Source: Cambridge Bitcoin Electricity Consumption Index

To address concerns about energy consumption, some Bitcoin miners are shifting to green energy sources. Switching to green energy sources can help the perception of BTC as an environmentally friendly asset, but the Bitcoin network's Proof-of-Work consensus mechanism will continue to consume large amounts of energy, regardless of source. As a result, newer blockchain protocols are exploring other consensus mechanisms that consume less energy and promote decentralization.

Figure C – Bitcoin energy consumption against countries



Source: University of Cambridge Bitcoin Electricity Consumption Index, BBC

What is Proof-of-Stake?

Proof-of-Stake (PoS), a concept originally introduced by Sunny Kind and Scott Nadal in 2012, is a consensus mechanism design that allows network validators to participate in the transaction validation process that is used to maintain the network if they stake or lock the token associated with the network. By requiring validators to lock tokens, the incentives of the validators and the network are aligned; a validator wants the network to continue functioning and would not want to attack the network because the value of the validator's underlying locked capital would be reduced if an issue occurs.

Proof-of-Stake consumes less energy than Proof-of-Work because, rather than requiring computational power to solve a mathematical problem, it allocates the right to validate transactions across different validators based on the percentage of tokens locked by each validator.

To prevent validators from conducting malicious behaviors for their own benefit, most Proof-of-Stake systems also include mechanisms that discourage attacks. A penalty mechanism known as "slashing" that will reduce or eliminate the validator's locked capital is often implemented to handle scenarios where the validator misses transactions, double signs transactions, or performs other malicious activities.

Proof-of-Stake Nuances & Concerns

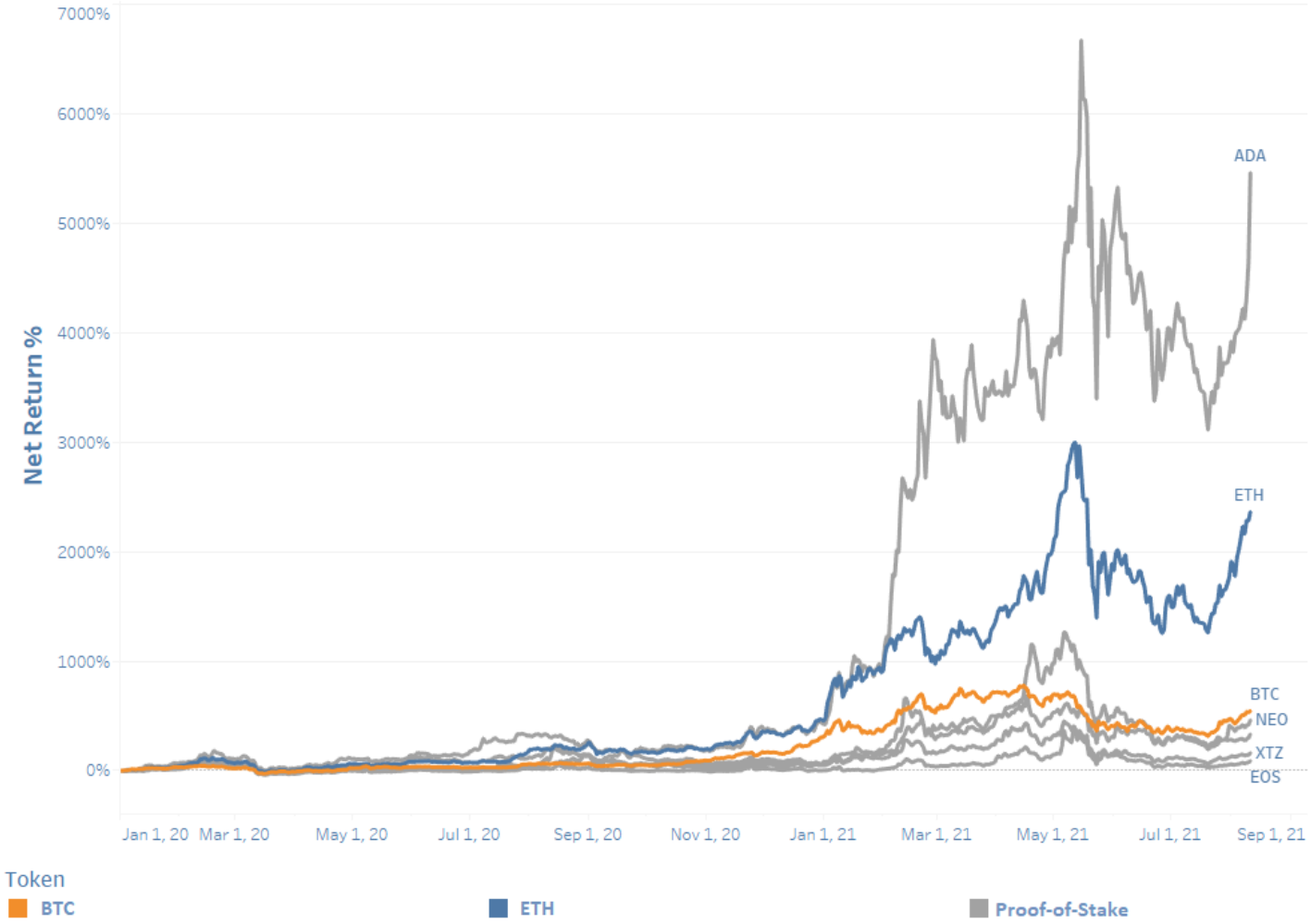
There are several types of Proof-of-Stake consensus mechanisms – including Delegated Proof-of-Stake and Hybrid Proof-of-Stake – that vary their design to meet the protocol's need for scalability and decentralization.

Critics of Proof-of-Stake argue that it could provide a small set of centralized entities, like staking pools and institutional investors, with too much power over the network. While debate over the merits of this criticism continues, the Ethereum network's efforts to adopt Proof-of-Stake indicate that maintaining decentralization is possible.

Notable Proof-of-Stake Assets

Some notable protocols currently using Proof-of-Stake consensus mechanisms include Cardano (ADA), EOS (EOS), Neo (NEO), and Tezos (XTZ). See how their returns have compared to BTC and ETH in the chart below.

Figure D – Sample Proof-of-Stake asset price movement – Overall returns



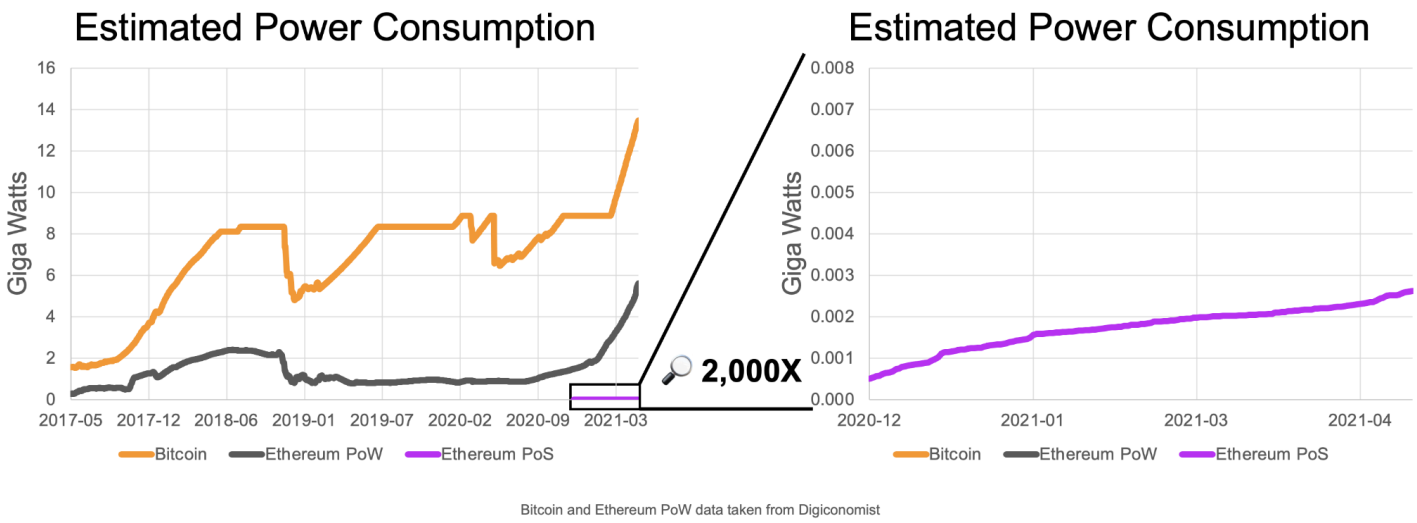
Source: Digital Asset Research; data from 1-Jan-2020 to 1-Sep-2021

Case example: Ethereum 2.0

Ethereum, the second largest digital asset by market capitalization and the most widely used blockchain platform for decentralized applications (dApps), is currently transitioning from Proof-of-Work to Proof-of-Stake as part of an initiative known as Ethereum 2.0. The Ethereum community sees Proof-of-Stake as a solution that will address scalability concerns by increasing transaction capacity and reducing gas fees associated with transactions. Previously, popular dApps, such as CryptoKitties in 2017 and Uniswap in 2020, have clogged the Ethereum network, leading to high network fees and preventing scalability and mass adoption.

The change to Proof-of-Stake is also Ethereum's answer to environmental concerns. The Ethereum Foundation estimated that the existing Proof-of-Work system consumes 5.13 gigawatts on a continuing basis, , whereas the Proof-of-Stake system consumes 2.62 megawatts on a continuing basis, meaning it uses about 99.95% less energy than Proof-of-Work. Put another way, the Ethereum Proof-of-Work network is estimated to use 2,000 times more energy than the Ethereum Proof-of-Stake test network that has been running in parallel. When the switch to Proof-of-Stake is made, the Ethereum network will go from using roughly the same amount of energy as a medium-sized country to the same amount of energy as around 2,100 American homes.

Figure E – Proof-of-work vs Proof-of-Stake Ethereum power consumption



Source: https://blog.ethereum.org/2021/05/18/country-power-no-more/

After years of work and decentralized collaboration, the Ethereum network has tangible next steps that the protocol will go through to fully transition to a Proof-of-Stake system. The Ethereum Foundation announced its intention to move to Proof-of-Stake in April 2020 and predicted that the transition will be complete by the end of 2021.

There are three main steps involved in the transition to Ethereum 2.0: the Beacon Chain, the merge and shard chains.

Beacon Chain

The Beacon Chain successfully went live on December 1, 2020 and introduced Proof-of-Stake to the Ethereum network while remaining separate from the Ethereum Mainnet. It acts as a coordinating mechanism that allows network participants to stake and validate transactions in parallel to the Ethereum Mainnet, which continues to operate as normal. Eventually, the Beacon Chain will also be responsible for randomly assigning network validators/stakers to validate shard chains, which will help ensure that network validators will be unable to collude and take over a shard.

The Merge

The merge will combine the legacy Ethereum Mainnet with the Beacon Chain, officially switching the Ethereum network consensus mechanism from Proof-of-Work to Proof-of-Stake. This part of the transition process is expected to happen by the end of 2021 or early 2022. After the merge happens, stakers will become network validators to the Ethereum mainnet and the legacy mining process that uses Proof-of-Work will stop.

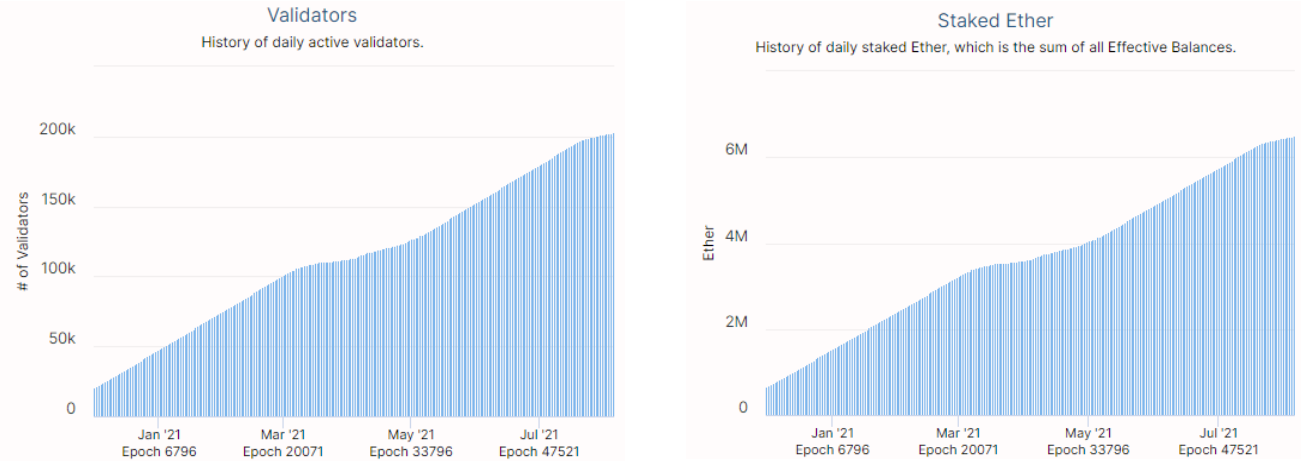
Shard Chain

After the Ethereum Mainnet merges with the Beacon Chain and Proof-of-Stake is implemented, “shard chains” will be introduced. These shards will extend the network to 64 new chains, splitting the network load horizontally to reduce network congestion and increase transaction throughput. Initially, the shard chain process was planned to be implemented before the merge. However, recent progress in Ethereum layer 2 scaling solutions has led to a shift in priorities.

Ethereum Staking

As of August 5, 2021, the Beacon Chain using Proof-of-Stake has more than 200,000 daily active validators and more than 6 million staked ETH. The charts below show the growth of the Ethereum 2.0 network since its launch.

Figure F – ETH staking statistics



Source: https://beaconcha.in/charts

A hidden Proof-of-Stake benefit: yield

In addition to solving scalability problems and reducing energy consumption, Proof-of-Stake offers another benefit for token protocols: the ability to generate yield. In digital asset markets, yield works similarly to traditional assets, with a few key differences. Yield on digital assets can be generated from interest received from lending out capital like in traditional markets, but it can also be generated by receiving rewards for participating in the protocol. Yield generated from staking and participating in a protocol can be thought of as similar to a stock dividend that is automatically reinvested in the underlying equity.

By contrast, in Proof-of-Work systems, there is no pathway for an asset owner to receive more of the same asset by participating in the network. Proof-of-Work assets such as Bitcoin require asset owners to lend out the asset in order to receive yield.

In Proof-of-Stake systems, the risks associated with generating yield vary by protocol. In addition to industry-wide risks like regulation or protocol-specific risks like network security, a key risk is the volatility and performance of the token because stakers receive yield in the underlying token, rather than in USD or another fiat currency.

Today, several assets that use a Proof-of-Stake system and offer yield opportunities fall within the top 30 digital assets by market cap. See the table below for details on these assets, as well as their classification within the DAR Industry Taxonomy.

Figure G – Top 30 assets by market capitalization with staking yield

Name	Symbol	Supersector	Sector	Subsector
Etherium	ETH	Computation Platforms	Smart Contract Platforms	General Purpose Smart Contract Platforms
Cardano	ADA	Computation Platforms	Smart Contract Platforms	Security-Focused Smart Contract Platforms
Polkadot	DOT	Computation Platforms	Smart Contract Platforms	General Purpose Smart Contract Platforms
Solana	SOL	Computation Platforms	Smart Contract Platforms	General Purpose Smart Contract Platforms
Terra	LUNA	Computation Platforms	Smart Contract Platforms	General Purpose Smart Contract Platforms
Polygon	MATIC	Computation Platforms	Smart Contract Platforms	Scalability-Focused Smart Contract Platforms
TRON	TRX	Computation Platforms	Smart Contract Platforms	Scalability-Focused Smart Contract Platforms
Cosmos	ATOM	Computation Platforms	Smart Contract Platforms	Scalability-Focused Smart Contract Platforms

Conclusion

As the digital asset industry matures, concerns around energy consumption will continue to be a prominent issue. Proof-of-Stake consensus mechanisms reduce energy usage significantly when compared to the Proof-of-Work consensus mechanism used by the Bitcoin network. The Ethereum network is transitioning to a Proof-of-Stake system in an effort to reduce its energy consumption. Proof-of-Stake consensus mechanisms also introduce yield opportunities, which may aid the adoption and value of the protocols that use them. The energy efficiency and yield benefits associated with Proof-of-Stake consensus mechanisms have led to an increase in their popularity, which is a trend that may continue or accelerate as institutional investors enter the space and seek avenues toward profits.

Disclaimers

You are permitted to store, display, analyze, modify, and print this report, but only for your own use. You are not permitted to (a) reverse engineer, decompile, decode, decrypt, disassemble, or in any way derive source code from this report; (b) modify, translate, adapt, alter, or create derivative works from this report; (c) copy (except as expressly permitted in the Subscription Services Agreement), distribute, publicly display, transmit, sell, rent, lease or otherwise exploit this report or grant any third party access to it; (d) frame or scrape or in-line link to the this report or use web crawlers, web spiders or other automated means to access, copy, index, process and/or store any of the information herein; (e) create apps, extensions, programs or other products or services that use any of the information herein; or (f) make or have made a service or product using similar ideas, features, functions or graphics of or providing a similar benefit as that provided by this report.

DAR DOES NOT MAKE AND HEREBY EXPRESSLY DISCLAIMS ALL WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE. WITHOUT LIMITING THE FOREGOING, YOU AGREE THAT YOUR USE OF THIS REPORT IS AT YOUR SOLE RISK AND ACKNOWLEDGE THAT THIS REPORT IS PROVIDED “AS-IS” AND DAR DOES NOT MAKE ANY WARRANTIES WITH RESPECT TO THE OPERATION, AVAILABILITY, RELIABILITY, ORIGINALITY OR ADEQUACY OF THE SAME. THIS REPORT (INCLUDING ANY INFERENCES OR CONCLUSIONS DRAWN HEREIN) IS BASED ON INFORMATION DAR CONSIDERS RELIABLE, HOWEVER, DAR DOES NOT REPRESENT IT AS ACCURATE OR COMPLETE, AND IT SHOULD NOT BE RELIED ON AS SUCH. THIS REPORT (INCLUDING ANY INFERENCES OR CONCLUSIONS DRAWN HEREIN) IS PROVIDED FOR GENERAL INFORMATIONAL PURPOSES ONLY AND YOU ARE RESPONSIBLE FOR DETERMINING WHETHER ANYTHING CONTAINED HEREIN IS SUITABLE FOR YOUR PARTICULAR CIRCUMSTANCES, AND FOR SEEKING PROFESSIONAL TAX AND/OR INVESTMENT ADVICE AS APPROPRIATE. DAR DOES NOT GIVE TAX, LEGAL OR INVESTMENT ADVICE OR ADVOCATE THE PURCHASE OR SALE OF ANY SECURITY, INVESTMENT, CRYPTOCURRENCY OR DIGITAL ASSET. NONE OF THE INFORMATION CONTAINED IN THIS REPORT CONSTITUTES OR IS INTENDED TO CONSTITUTE A RECOMMENDATION BY DAR TO ACQUIRE, HOLD, INVEST IN, OR USE ANY PARTICULAR COIN, TOKEN, CRYPTOCURRENCY, PROTOCOL, COMPANY OR FOUNDATION.

You assume the entire risk of any use you make or permit to be made from this report. Without limiting the foregoing and to the maximum extent permitted by applicable law, in no event shall DAR have any liability regarding this report for damages, even if notified of such possibility. The information contained herein is as of the date hereof and is subject to change without prior notice. We may provide oral or written market commentary or trading strategies to our clients that reflect opinions that are contrary to the opinions expressed in this research. Information containing any historical information, data or analysis should not be taken as an indication or guarantee of any future performance as past performance does not guarantee future results. None of DAR’s products or services recommend, endorse, or otherwise express any opinion regarding any “coin”, “token”, “cryptocurrency” “protocol”, “company” or “foundation” and none of DAR’s products or services are intended to constitute investment advice or a recommendation to make (or refrain from making) any kind of investment decision and may not be relied on as such.

About FTSE Russell and Digital Asset Research

FTSE Russell is a leading global index provider creating and managing a wide range of indexes, data, and analytic solutions to meet client needs across asset classes, style, and strategies. Covering 98% of the investable market, FTSE Russell indexes offer a true picture of global markets, combined with the specialist knowledge gained from developing local benchmarks around the world. Digital Asset Research (DAR) is a provider of crypto market data, research, and analysis to professional investors. In its partnership with FTSE Russell, DAR acts as an asset specialist, providing digital asset data as well as research on token projects and technologies. Since 2018, FTSE Russell and DAR have worked to align digital asset data with traditional investment infrastructure. Initially, the firms launched a suite of live, ticking indicative digital asset indices as a proof of concept. Later initiatives focused on an expansion of SEDOL reference data coverage to include digital assets, and the launch of the FTSE DAR Reference Price, a vetted digital asset price data to enable quality index development. A growing digital asset index family follows, providing a complex methodology for global index research and product development.

To learn more, visit ftserussell.com/digitalasset; email info@ftserussell.com; or call your regional Client Service Team office

EMEA
+44 (0) 20 7866 1810

North America
+1 877 503 6437

Asia-Pacific
Hong Kong +852 2164 3333
Tokyo +81 3 4563 6346
Sydney +61 (0) 2 8823 3521