Ethereum: A Deconstruction of Crypto Supply

Published August 2, 2021

Blake Heimann
Senior Associate, Quantitative Research

One of the well-known differences between bitcoin and ether is the fact that ether does not have an explicit cap on supply, while the number of bitcoins in circulation will never exceed 21 million. This supply limit attributes bitcoin its current primary investment case due to its perceived store of value. This is one of the few conclusions that has reached some level of consensus in the investment community given the nascence of crypto assets. So, what does this mean for those that do not have a supply cap? In this blog post, we will dive into the issuance of ether, the second-largest crypto asset by market cap, and why some upcoming changes to its issuance mechanism may support the case for it as not only a store of value, but also a deflationary asset.

Reminder: Bitcoin's Issuance Mechanism

The issuance mechanism for bitcoin follows a process of minting brand-new bitcoin as incentive for miners to verify transactions and secure the blockchain. This freshly minted bitcoin is referred to as the *block subsidy* and declines over time, halving in value roughly every four years1. The total outstanding supply will eventually reach 21 million and stop growing.

Once the full supply is in circulation, the incentives for securing the blockchain are fully supported by transaction fees paid to the miners by those transacting on the network, rather than newly minted bitcoin. These transaction fees exist today, serving as an incentive paid by the transactor to the miner for higher priority in writing the transaction to the block.2 In traditional finance speak, these fees serve as a means for faster execution. As the network matures, these fees should reach an equilibrium between serving as the sole incentive for miners to secure the network and network participants paying fees to transact on the network efficiently.

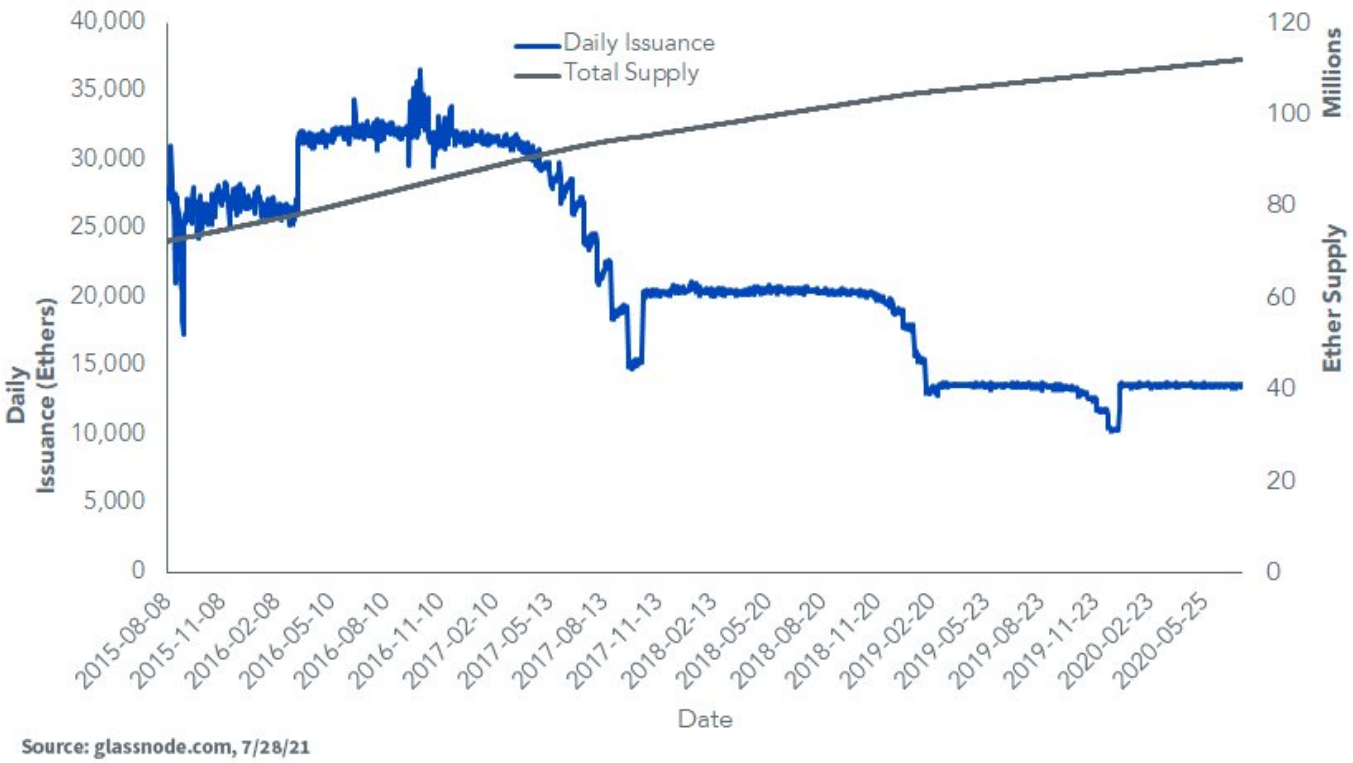
Ether's Issuance Mechanism: An Evolving System

Currently, the issuance mechanism for ether loosely imitates that of bitcoin but does not follow the halving schedule. Right now, every time a block on the Ethereum network is mined, two ethers are minted and gifted to the miner, creating new supply of ether. Like bitcoin, these subsidies have been reduced over time based upon the total number of blocks mined on the blockchain, first starting at five ethers for the first 4.4 million blocks, then three for the following 2.9 million, and now two ethers3. These changes in block subsidy, as well as other improvements to the network protocol, are implemented via Ethereum Improvement Proposals, or EIPs.

EIPs are proposed changes to the Ethereum code that are reviewed by the community of users, developers and validators via a lifecycle of technical reviews, research and discussion.4 With a focus on maintaining the sanctity of the network, EIPs are approved and implemented alongside current versions of the code in network upgrades. Network participants may operate on different versions of the network but may be forced to choose between two versions when upgrades are incompatible across versions. These events are well broadcasted and documented prior to implementation, and network participants may choose to operate on either version but are expected to gravitate toward the "better" of the two, which will presumably have more users and serve the majority of network participants. In this way, the "best" version of Ethereum prevails.

In addition to the block subsidy, the miner receives a fee paid by the party making the transaction, called gas5. This gas serves the same purpose as the fee described for bitcoin, but it will come to play a greater role in the coming months. Approximately 6,500 blocks are mined per day on the Ethereum network6, which would therefore result in an additional supply of 13,000 ethers per day, or an annual issuance rate of approximately 4%. With no explicit supply cap and issuance rates as such, those who are skeptics of ether's store of value are rightly justified. But with newly proposed changes to the issuance mechanism for the near future, the narrative around the supply-side economics may change drastically.

Ether Issuance and Supply



Source: glassnode.com, 7/28/21

Upcoming Changes: EIP 1559 and Proof of Stake

Now that we've touched on the current supply mechanism, we need to address changes to the supply mechanism that are scheduled to occur in Ethereum upgrades in the near future. The first of these is an

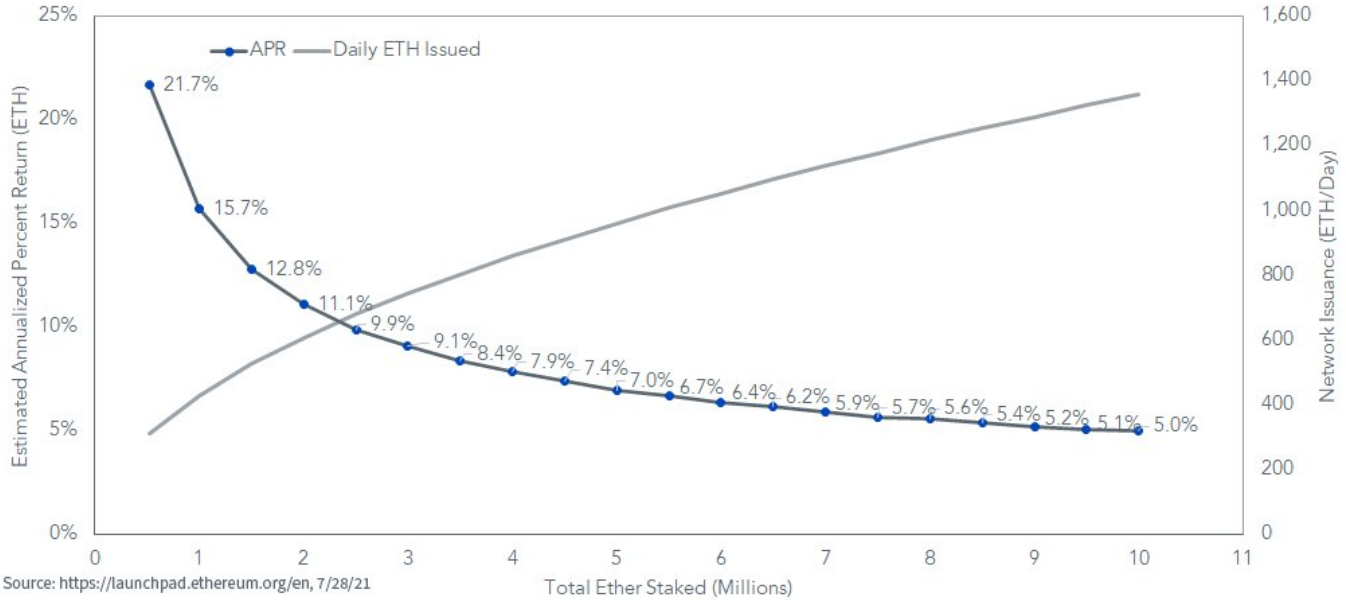
update called the *Ethereum Improvement Proposal 15597*, or EIP 1559, and the second of these is the transition to proof of *stake*8 from *proof of work*9. These changes in the Ethereum protocol arguably have reductive effects on the circulating supply of ether in the network2.

The first major change, EIP 1559, is scheduled to be effective later this week; it has been in the works since April 2019, first proposed by the creator of Ethereum himself, Vitalik Buterin. It consists of a change to the protocol regarding the gas that we mentioned above. After the update, this gas will no longer be paid in full to the miners. Rather, a portion of this gas will be "burned"—i.e., destroyed. This burned gas will be predetermined as the "market rate" of the transaction fee based on current congestion in the network among those transacting, seeking to write changes in ownership to the ledger. This base rate will be burned, and any additional fees on top (the tip) will be passed on directly to the miner10. From the transactor's purview, this "tip" will be for the purpose of receiving expedited transactions. The miner will still receive their freshly minted two ethers in addition to this "tip."

The second major change replaces the proof of work consensus mechanism with proof of stake, which is currently live in ETH 2.011 and is expected to replace the legacy ETH blockchain in late 2021 or early 202212. The proof of work mechanism is currently in place for ETH 1.0 and many competing crypto assets, including bitcoin. This consensus mechanism is what maintains the integrity of the blockchain (and its transactions) via miners solving cryptographic hash functions to "seal" the block after validating the constituent transactions.9 Solving these hash functions requires significant computing power and electricity, which is the source of debate around the overall sustainability of the mining required to secure a crypto asset network.

Proof of stake would take the place of this as the consensus mechanism, requiring miners (henceforth called validators) to stake (or lock up) 32 ethers to begin processing transactions on the network.8 Rather than requiring the solving of a puzzle, the validators can secure the network free of these computation-intensive efforts. The 32 ethers staked serve as a form of collateral that the validator loses if they validate a "bad" or fraudulent block2. It is burned, and this results in a reduction of supply just like the base rate for gas referred to earlier. In return for performing validation to secure the network, the validator still receives their freshly minted ether and transaction fees (any gas greater than the base rate), but the amount of ether issued to the validator changes based upon the aggregate amount of ether staked13. This reward is determined programmatically to entice more validators when staking is low and to refrain from doing so when there is a lot of ether staked, and plenty of validators. The implications of this are that the network's issuance fluctuates to yield an optimal level of security while issuing the least amount of new ether, an equilibrium that is forecasted to result in a fraction of the current annual rate of issuance.

Validator Economics and Issuance



Putting It All Together: A Potential Deflationary Asset

So, what does this mean for overall ether supply? We know that burning gas will reduce supply by destroying ether, staking will reduce the amount of circulating supply by locking up ether as a form of collateral, and the annual issuance of new ether rewarded to validators is forecasted to decrease significantly below current rates. Therefore, combining these three factors, the logical expectation would be a reduced rate of supply growth compared to the current Ethereum protocol. This has been referred to as Ethereum's triple halving. Barring any turn of events that would prevent these updates from taking place, some argue the combination of these changes will have such a strong effect that it will net out the minting of any new ether2—reaching a state at which supply is continually decreasing, attributing to ether deflationary asset status.

1https://www.cmcmarkets.com/en/learn-cryptocurrencies/bitcoin-halving
2https://podcasts.apple.com/us/podcast/ethereum-into-the-ether/id1559120677?i=1000522314009
3https://docs.ethhub.io/ethereum-basics/monetary-policy/
4https://eips.ethereum.org/EIPS/eip-1
5https://ethereum.org/en/developers/docs/gas/
6https://glassnode.com/
7https://eips.ethereum.org/EIPS/eip-1559
8https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/#top
9https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/#top
10https://www.gemini.com/cryptopedia/ethereum-improvement-proposal-ETH-gas-fee
11https://www.gemini.com/cryptopedia/ethereum-blockchain-pos-proof-of-stake
12https://www.thestreet.com/crypto/ethereum/ethereum-2-upgrade-what-you-need-to-know
13https://launchpad.ethereum.org/en/

Important Risks Related to this Article

There are risks associated with investing, including the possible loss of principal. Crypto assets, such as bitcoin and ether, are complex, generally exhibit extreme price volatility and unpredictability, and should be viewed as highly speculative assets. Crypto assets are frequently referred to as crypto “currencies,” but they typically operate without central authority or banks, are not backed by any government or issuing entity (i.e., no right of recourse), have no government or insurance protections, are not legal tender and have limited or no usability as compared to fiat currencies. Federal, state or foreign governments may restrict the use, transfer, exchange and value of crypto assets, and regulation in the U.S. and worldwide is still developing.

Crypto asset exchanges and/or settlement facilities may stop operating, permanently shut down or experience issues due to security breaches, fraud, insolvency, market manipulation, market surveillance, KYC/AML (know your customer/anti-money laundering) procedures, noncompliance with applicable rules and regulations, technical glitches, hackers, malware or other reasons, which could negatively impact the price of any cryptocurrency traded on such exchanges or reliant on a settlement facility or otherwise may prevent access or use of the crypto asset. Crypto assets can experience unique events, such as forks or airdrops, which can impact the value and functionality of the crypto asset.

Crypto asset transactions are generally irreversible, which means that a crypto asset may be unrecoverable in instances where: (i) it is sent to an incorrect address, (ii) the incorrect amount is sent or (iii) transactions are made fraudulently from an account. A crypto asset may decline in popularity, acceptance or use, thereby impairing its price, and the price of a crypto asset may also be impacted by the transactions of a small number of holders of such crypto asset. Crypto assets may be difficult to value, and valuations, even for the same crypto asset, may differ significantly by pricing source or otherwise be suspect due to market fragmentation, illiquidity, volatility and the potential for manipulation. Crypto assets generally rely on blockchain technology, and blockchain technology is a relatively new and untested technology which operates as a distributed ledger. Blockchain systems could be subject to Internet connectivity disruptions, consensus failures or cybersecurity attacks, and the date or time that you initiate a transaction may be different than when it is recorded on the blockchain. Access to a given blockchain requires an individualized key, which, if compromised, could result in loss due to theft, destruction or inaccessibility.

In addition, different crypto assets exhibit different characteristics, use cases and risk profiles. Information provided by WisdomTree regarding digital assets, crypto assets or blockchain networks should not be considered or relied upon as investment or other advice or as a recommendation from WisdomTree, including regarding the use or suitability of any particular digital asset, crypto asset, blockchain network or any particular strategy. WisdomTree is not acting and has not agreed to act in an investment advisory, fiduciary or quasi-fiduciary capacity to any advisor, end client or investor, and has no responsibility in connection therewith, with respect to any digital assets, crypto assets or blockchain networks.