BLOCKCHAIN INVESTMENT & ADVISORY

Sector: Infrastructure

Ethereum review

2 October 2018

Ethereum is the largest by market capitalisation and the most popular platform among developers and ICO fundraisers. Currently, there are 573 ERC20 tokens, and 121 tokens ERC721 issued on the platform. The number of distributed applications launched on Ethereum is c.1500. Ethereum currently has c.40mn unique addresses and the number of transactions is c.750,000 a day.

The idea of Ethereum as a blockchain with the capability to be programmed to perform any arbitrary complex computation was first announced in 2013. Since then, the smart contract feature has made the Ethereum platform the most successful to run fundraising efforts on the blockchain and to create Dapps.

This review is a part of the DLT platforms review by NKB Group

Date	**2 October 2018**
Ethereum MktCap, $bn	23,856

Research Analyst:

Marina Alekseenkova
Marina.Alekseenkova@nkbgroup.io

ETHEREUM

Native token	ETH, gas	**Languages**	Solidity, Go, C++, Rust
MktCap, $mn	23,856	**Protocol**	POW/ POS exp in 2019
Circulating supply	102,317,972	**Number of TXS**	14
Maximum supply	Not capped	**License**	GPLv3, LGPLv3, MIT
Governance	Ethereum Foundation	**Roadmap**	Casper/POS - 2019

Ethereum is the largest by market capitalisation and the most popular platform among developers and ICO fundraisers. Currently, there are 573 ERC20 tokens, and 121 tokens ERC721 issued on the platform. The number of distributed applications launched on Ethereum is c.1500. Ethereum currently has c.40mn unique addresses and the number of transactions is c.750,000 a day.
The idea of Ethereum as a blockchain with the capability to be programmed to perform any arbitrary complex computation was first announced in 2013. Since then, the smart contract feature has made the Ethereum platform the most successful to run fundraising efforts on the blockchain and to create Dapps.

Governance system

The Ethereum Foundation was created to promote and support the Ethereum platform, base layer research, development and education. The Foundation is run by the Council, which includes the creator of Ethereum Vitalik Buterin and Patrick Storchenegger, who is an attoney at law and notary public in Canton Zug, Switzerland. The Technical Steering Group is headed by Jeffrey Wilcke, who is the co-founder of Ethereum.
In 2015, Ethereum introduced an Ethereum Improvement Proposal (EIP) standard to amend the development of the platform. The core development group and community process and implement EIPs. Most important EIPs include EIP-20, a technical standard used for smart contracts on the platform (ERC – Ethereum Request for Comment). There were a total of 103,621 ERC-20 compatible tokens as of end Jul 2018. Usually the proposals (EIS) are submitted by the developers, discussed, and several development teams implement the technological innovations. Ethereum made one major hard fork after the DAO hack in 2016, when Ethereum was split into two separate blockchains Ethereum (ETH) and Ethereum Classic (ETC). Ethereum runs a number of meetings for the Ethereum community and developers (devcons, hackathons, meetups).
In 2017, several blockchain startups, research groups and companies announced the creation of the Enterprise Ethereum Alliance (EEA) with 30 founding members. Now the list of members exceeds 150, and includes ConsenSYS, CME Group, Toyota Research Institute, Microsoft, JP Morgan, Merck, DTCC, Accenture, BNY Mellon, National Bank of Canada, Sberbank, Cisco Systems, MasterCard, Deloittee and others.
The criticism of the Ethereum platform is usually related to ease of Ethereum use to run Ponzi schemes and other investment fraud. According to the University of Cagliari paper, c. 10% of 1382 smart contracts examined were facilitating Ponzi schemes, however only 0.05% of the transactions on the network were related to such contracts.

Token economics

The fees on the Ethereum platform are paid with native token Ether (ETH). The ETH supply is uncapped. The current supply is c.101mn. The transfer from PoW to PoS will result in a capped supply at some point. According to the discussed proposals, Ethereum supply may be capped at c.120mn, with some 2%

inflation following the implementation of Casper FFG and CBC. In 2017, mining generated 9.2mn new Ether, which is c .10% of its total supply.
Ether is used to paying fees to miners and to paying for gas to run smart contracts. Although Ether is not the fuel for the Ethereum Virtual Machine (EVM), which runs smart contracts using gas, another 'fuel' token on the Ethereum platform, the price of transaction sent to the Ethereum network costs some discreet amount of gas depending on how many EVM instructions need to be executed. The gas price versus Ether depends on the sender of transaction to specify the price they want to pay, and the miner to verify transactions they like . The average gas price is c. 20Gwei (or 0.00000002ETH), but can vary depending on market activity. Different transactions have different gas limits and the miners will stop executing the moment the gas runs out. The Dapp shall pay for gas to make the smart contract work.
The switch to Casper from POW will change the economics for Dapps and for block validations. Apart from a different fee structure, which is in the process of discussion, it will be a requirement that miners (stakers) should have at least 1000ETH to mine (current proposal). The lauch of a more scalable version with sharding will likely result in a lower limit for stakers.

Protocol

The transactions on the network are received, propagated, verified and executed by nodes or "miners" on the network, who collect the fees for their work. Miners group transactions into blocks and add them to the blockchain, competing with other miners for the next block to add. Miners are rewarded for each successful block they add to the network solving a complex mathematical problem to mine a block, or executing a "proof of work" algorithm. Ethereum has chosen a memory-hard computational problem that eliminates the risk of centralisation due to the usage of a special hardware (ASICs), thus declaring that Ethereum's PoW is ASIC-resistant.
The protocol switch from PoW to PoS encounters several issues: 1) censorship, when the ETH block is lost by one miner, it might be found and made by other miners, while POS require "coordinated game", 2) cost, which supports the satisfactory security in PoW, while PoS is costly for attackers. The switch from PoW to PoS is scheduled for 2019, by which time Ethereum will gradually release two versions of Casper, FFG (Friendly Finality Gadget) and Casper CBC (Correct by Construction) before any other solutions. However, the plan may change to reach the targeted network scalability using Casper and sharding together. The Ethereum team is approaching the problem with the tools of formal verification, including verification of hypothesis around the cost of bribing validators.

Security

Users on the Ethereum blockchain must pay transaction fees to the network that protects the Ethereum blockchain from malicious computational tasks like DDoS attacks of infinite loops. The sender of the transaction must pay for each step of the activated program, including computation and memory storage.

Technology

The central part of the Ethereum platform is the Ethereum Virtual Machine (EVM), which can execute code of arbitrary algorithmic complexity. Ethereum includes a peer-to-peer network protocol with many nodes connected to the Ethereum network maintaining and updating the database. Each node on the network runs the EVM and executes the same instructions, creating a "world computer". This process of computing by many nodes of the same task makes the Ethereum network slower and more expensive compared to a task computation on a single computer. Ethereum created a twin-unit system to separate the main token ETH from the functional unit (gas) powering transactions. The successful smart contract execution requires gas, a unit separate from ETH designed to pay the fees on the platform.

Ethereum's smart contracts were major innovation widely accepted by developers, and boosted the Ethereum popularity. Compared to Bitcoin blockchain, which represents a list of transactions, Ethereum blockchain tracks the state of every account and all state transactions on the Ethereum blockchain are transfers of value and information between accounts. There are two types of accounts: externally owned accounts (EOA), which are controlled by private keys, and contract accounts, which are controlled by their contract code and can only be activated by an EOA. Contract accounts are governed by their internal code. Smart contracts, which refer to code in the contract accounts, are programs executed when a transaction is sent to that account.

The bottlenecks of the Ethereum platform became obvious in 2017, when the number of transactions increased a few times and caused essential growth of transaction fees. Scaling solutions proposed by Ethereum team include Raiden Network (RDN), Plasma, Sharding and Casper.

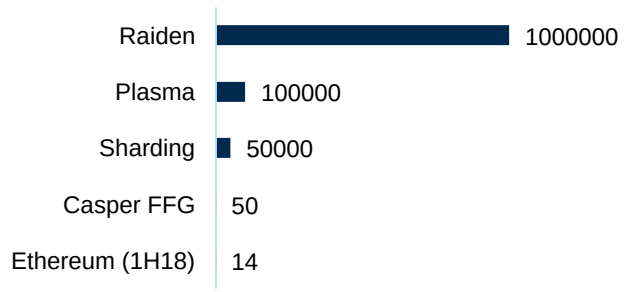
Raiden Network (RDN), which represents an off-chain scaling solution, allows users to make transactions through transaction channels off the main blockchain, settling periodically accumulated transaction volume on the main blockchain. The network relies on off-chain channels that create a potential risk of misbehaviour by agents who may get control over those channels. The estimated throughput of the RDN is 1mn TXS.

Plasma is an off-chain solution that allows "child chains" which may allow interchangeability of assets in separate chains which are branches of the main blockchain. The child chain will use a different method of consensus allowing higher transactions throughput. The return on the main blockchain from a child chain may be required in the event of a dispute. The estimated throughput is 100k TXS. The Plasma project may be launched in 2020.

Sharding is a scaling solution which may come with the Casper protocol. Sharding will allow to split the workflow of nodes between them, thus all the data sets will be split into "shard" or micro-chains. Each node will deal with all data and transactions responsible for a part of transaction data. Sharding will increase the throughput of transactions, dividing them among nodes. The estimated throughput is 50k TXS.

Casper is the most important modification on the Ethereum network, which realizes the transfer from proof-of-work to proof-of-stake and essentially changes the economics on the blockchain. The lower costs and faster transactions, which may be achieved using POS, are the main incentives for the Ethereum team to complete this project as soon as possible. Casper protocol is planned to be launched in two stages: 1) Casper Friendly Finality Gadget (FFG) and 2) Casper Correct by Construction (CBC). Casper FFG is a transition protocol, which combines POW and POS , while CBC will include full POS implementation. The throughput of the Ethereum network may increase to 50k TXS. The launch of CBC may happen in mid-2019, together with Sharding, while the Ethereum team may skip the FFG phase.

Figure 15. Ethereum scaling solutions transactions throughput, TXS



Source: Ethereum

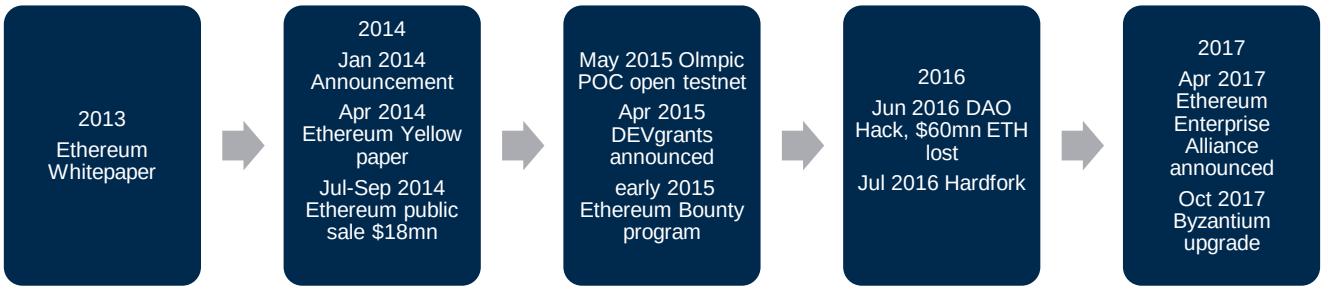
Ethereum 2.0 will incorporate the Casper protocol and the addition of sharding. High demand for decentralised platform services is pushing the Ethereum team to implement additional features improving the Ethereum blockchain. Casper, the Ethereum's proof-of-stake (POS) algorithm, will reduce the cost of consensus thus cutting down the cost of transaction for a user. The sharding will be a solution to a scalability problem at Ethereum. Sharding will allow the Ethereum network to cope with a greater number of users and transactions without losing speed or becoming congested. Currently, the team is going to implement both the Casper upgrade and sharding at the same time. Shards on the network will communicate with each other via cross-links or checkpoints, while Casper will strengthen the checkpoints adding security and scalability. Ethereum 2.0 will be launched in 2019, with Casper launched first in 2019 and sharding happening in two phases – the first in 2020 and the second in 2021. The version of Ethereum 3.0 will be the network that enables systems that can withstand and support the power of quantum computers.

Constantinople will be activated some time before October, when Ethereum will hold Devcon4. The implementation stage continues until 13th August, followed by two months of testing and the launch of the Constantinople-specific test network. It includes EIP-210, which reorganizes how block hashes are stored on Ethereum, EIP-145 and which increases the speed of arithmetic in the Ethereum Virtual Machine (EVM), EIP-1014, which focuses on the addition of Ethereum state channels, and EIP-1052 which optimizes how the contract interacts, and which aims to improve the efficiency of the blockchain. Constantinople is the second part of the two-part upgrade after Byzantium, activated in October 2017. Two changes to the protocol, including a difficulty bomb and new gas pricing model, are delayed.

Roadmap

The Ethereum team divided the Ethereum platform development into four stages: 1) Frontier (since June 2015, when the network was launched), 2) Homestead (since March 2016), 3) Metropolis (since October 2017), 4) Serenity (final phase, dates TBA). At the Serenity stage, the network will use the Casper proof-of-stake algorithm.

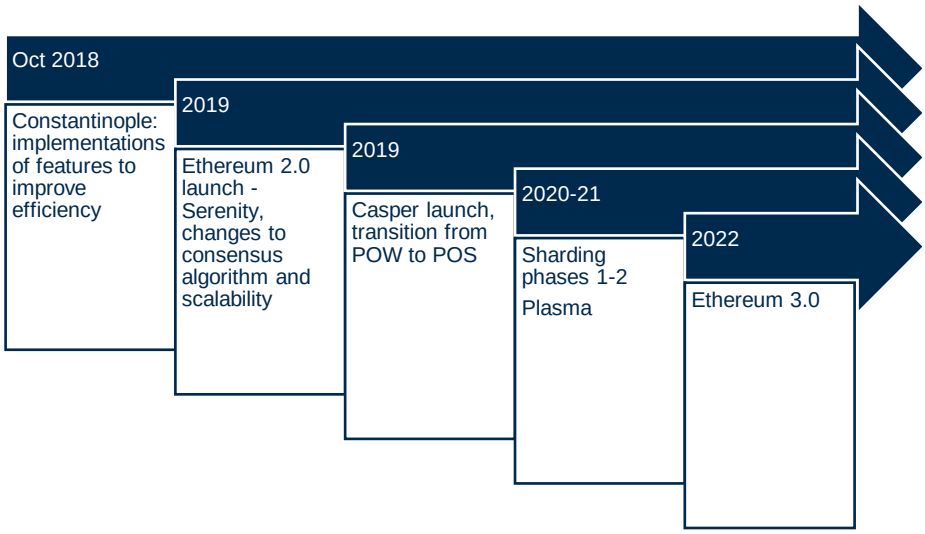
Figure 16. Ethereum timeline



Source: Ethereum

The switch from POW to POS is the major event expected on the Ethereum platform. The Casper transition protocol will be launched together with the Sharding solution to improve the scalability in 2019, while the complete scalable version of the network Ethereum 3.0 is scheduled for 2022.

Figure 17. Ethereum roadmap



Source: Ethereum

Use cases

The list of use cases already implemented on the Ethereum platform is wide and includes finance, the IoT applications, delivery and food tracking systems, electricity sourcing and pricing, sports betting, gaming and gambling, and predictive analytics. Some applications include digital signature algorithms, securitized tokens, digital right management, crowdfunding, remittance, social media platforms, identity systems and more.

Gaming and gambling applications recently became the most popular (in terms of largest number of daily users and transactions a day), followed by Cryptokitties and other entertainment applications.

There are several permissioned blockchains created on the Ethereum platform, including those of J.P. Morgan Chase (Quorum system for derivatives and payments) and Royal Bank of Scotland (Clearing and Settlement Mechanism).

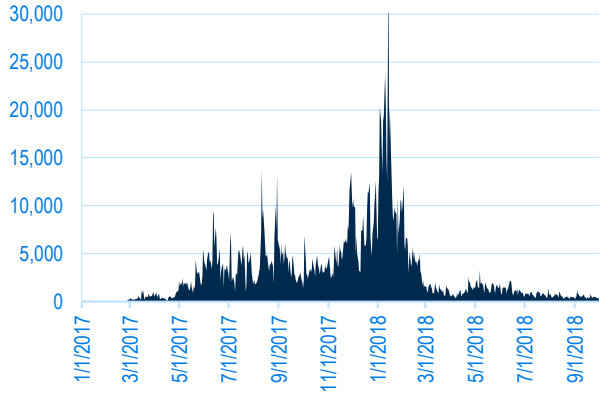
Team

Vitalik Buterin	Ethereum creator, Ethereum Foundation Council	Jeffrey Wilcke	Co-founder, Head of Technical Steering Group
Gavin Wood	Co-founder, Ethereum	Vlad Zamfir	Lead developer of Casper protocol upgrade
Joseph Lubin	Co-founder, Ethereum		

Fundraising

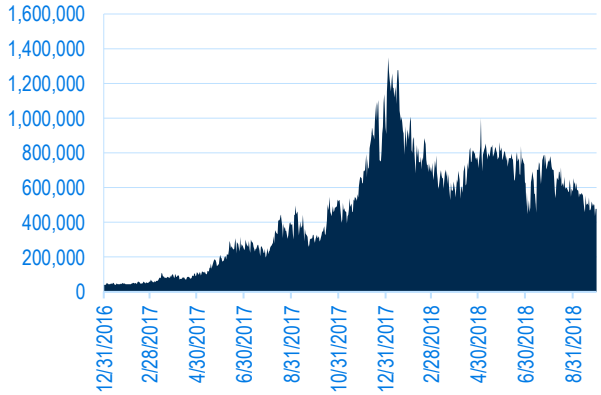
The development of the Ethereum platform was funded by a crowdsale in July-August 2014. There were 11.9mn coins premined for crowdsale (c.13% of the current circulating supply). The Ethereum team launched its ICO in 2015 raising c. $18mn of new funds. In 2016, the DAO project raised c. $160mn, however this was hacked.

Figure 18. Ethereum transaction volume, $mn



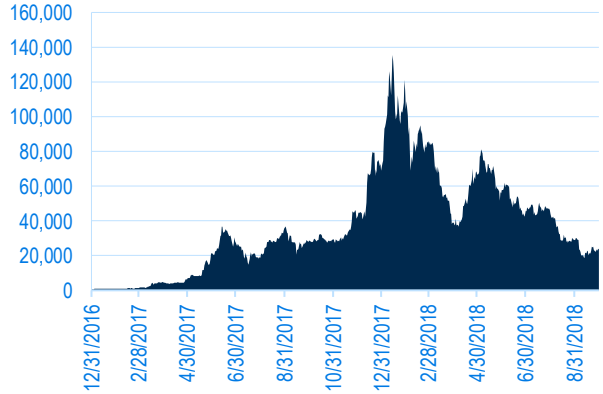
Source: coinmetrics.io

Figure 19. Ethereum transaction count



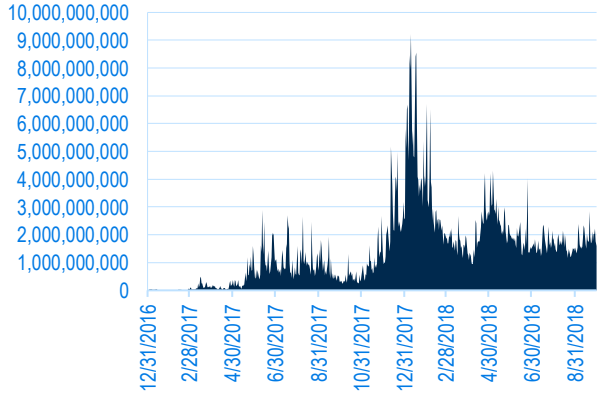
Source: coinmetrics.io

Figure 20. Ethereum MarketCap, $mn



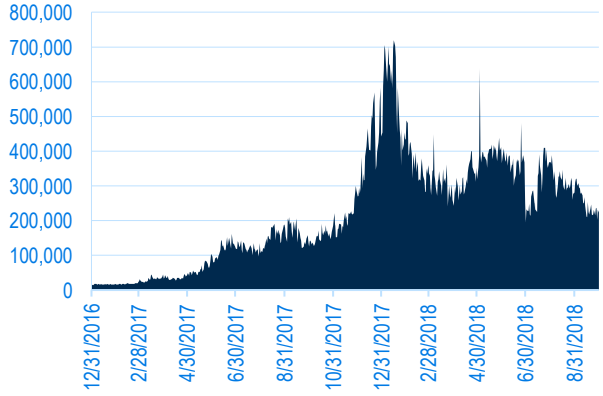
Source: coinmetrics.io

Figure 21. Ethereum exchange volume, $



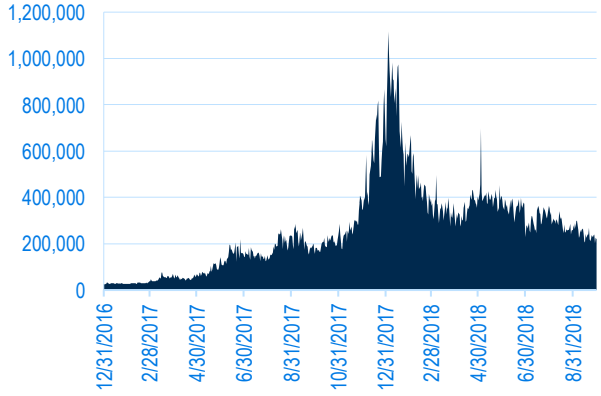
Source: coinmetrics.io

Figure 22. Ethereum active addresses



Source: coinmetrics.io

Figure 23. Ethereum difficulty



Source: coinmetrics.io

ANALYSTS CERTIFICATION AND DISCLAIMER

This report has been prepared and issued by Hypothesis Research Limited ("Hypothesis") in accordance with Hypothesis policies for managing conflicts of interest arising as a result of publication and distribution of investment research. Hypothesis is authorised and regulated by the Financial Conduct Authority ("FCA"). This report has been prepared by the analyst whose name appears on the front page of this report.

The information contained within the report is intended for use by professional clients and eligible counterparties as defined in section 3 of the FCA Conduct of Business rules. Our research must not be acted on or relied upon by persons in the UK who would be categorised as retail clients.

The report must not be distributed in any other jurisdictions where its distribution may be restricted by law. Persons into whose possession this report comes into should inform themselves about, and observe, any such restrictions.

All information used in the publication of this report has been compiled from publicly available sources that are believed to be reliable, however we do not guarantee the accuracy or completeness of this report. Opinions contained in this report represent those of Hypothesis and the analyst at the time of publication.

Hypothesis does not offer or provide personalised advice. The information provided is not intended to be, and should not be construed in any manner whatsoever as, personalised advice as it does not have regard to the specific investment objectives, financial situation and particular needs of any specific person who may receive this report. The information provided by us should not be construed by any subscriber or prospective subscriber as Hypothesis' solicitation or inducement to buy, sell, subscribe, or underwrite any securities mentioned in this report. Investors should make their own investment decisions based upon their own financial objective and resources.

Hypothesis has a restrictive policy relating to personal dealing. Hypothesis, its respective directors, officers, employees and contractors do not hold any positions in the securities mentioned in this report. Hypothesis may perform services or solicit business from any of the companies mentioned in this report.

The value of securities mentioned in this report can fall as well as rise and may be subject to large and sudden swings. In addition, it may be difficult or not possible to buy, sell or obtain accurate information about the value of securities mentioned in this report. Past performance is not necessarily a guide to future performance. Forward-looking information or statements in this report contain information that is based on assumptions, forecasts of future results, estimates of amounts not yet determinable, and therefore involve known and unknown risks, uncertainties and other factors which may cause the actual results, performance or achievements of their subject matter to be materially different from current expectations.

To the maximum extent permitted by law, Hypothesis, its affiliates and contractors, and their respective directors, officers and employees will not be liable for any loss or damage arising as a result of reliance being placed on any of the information contained in this report and do not guarantee the returns on investments in the products discussed in this publication.

NKB Group

Offices: London, Vienna

www.nkbgroup.io

The report is prepared by NKB Group in collaboration with Hypothesis Research Ltd (UK).

N·K·B
BLOCKCHAIN FINANCE GROUP

HYPOTHESIS RESEARCH