RESEARCH

RESEARCH BRIEF

What Is Ethereum?

April 21, 2021

Blockchain Explainer

We dive into one of the world's most popular blockchain networks, from a simple explanation of what Ethereum is to some of its uses and drawbacks (and what it has to do with cats).

Ethereum — one of the most frequently used open-source blockchains — is seeing a resurgence in the mainstream, especially amid the explosive popularity of NFTs (the vast majority of which are built using Ethereum standards).

As of mid-April 2021, its market capitalization tops $291B, up from $712M in early January 2017.

RESEARCH

In this report, we'll explain what Ethereum is and how people are leveraging the protocol to develop decentralized applications spanning lending, trading, games, and more.

TABLE OF CONTENTS

What is blockchain?

To understand Ethereum, you first have to understand what blockchain technology is.

transact on it, or hold their own copy of the digital ledger, and no single central entity can alter past information.

There are also private and permissioned blockchains, but these tend to serve a different purpose, such as being leveraged by enterprises to track supply chain data. For an in-depth look at Bitcoin and blockchain technology, check out our explainer.

What is Ethereum?

Ethereum is an open-source, decentralized blockchain. What sets it apart is the built-in functionality of smart contracts. A smart contract is essentially code that binds 2 parties to an agreement and can execute on its own, without an intermediary.

This functionality earned it the name of a "world computer" (technically known as the Ethereum Virtual Machine, or EVM), because it acts as much more than a payments method or a store of value — what Bitcoin does. The EVM environment enables developers to build decentralized applications on top of it, from social media to games to banking, like an app store that isn't controlled by Apple or Google.

Source: State of the DApps

However, the promise and potential of Ethereum remains a bit bolder than its present-day implementation due to the current costs of computing, which we'll cover later on.

What is a smart contract?

To illustrate a smart contract, let's say Alice and Bob enter into a bet.

Alice thinks that the temperature tomorrow morning will reach 70 degrees Fahrenheit. Bob thinks that it won't. They wager 0.01 bitcoin on the outcome. (In this example, the digital currency is bitcoin, but any other cryptocurrency could be used as well.)

If Alice and Bob don't trust each other, they will have to use a trusted third party as an escrow agent. In other words, they will each have to give the agent that amount of money, and the agent will distribute the winnings and the amount staked to the winner.

There's no way around the middleman in this scenario, even using a cryptocurrency like bitcoin. And the Bitcoin blockchain has no way to record this "contract."

Ethereum, on the other hand, offers a solution. Alice and Bob could agree to use some basic code — an "if, then" contract of sorts — that pays out based on the temperature. If the temperature is higher than 70 degrees Fahrenheit, the code is programmed to pay Alice; otherwise, it pays Bob. Alice and Bob could then place their "programmed" bet on Ethereum's blockchain. At that point, it becomes binding from a technological standpoint.

This is a “contract," because Alice and Bob have agreed to its terms, to a degree transforming code into law. It's “smart" and “decentralized" because all participants in the Ethereum blockchain hold a copy of this contract.

Just as all Bitcoin “nodes," or participants in the system, know that Alice sent Bob 0.01 bitcoin, all Ethereum nodes know that Alice and Bob have entered this bet.

Let's watch this smart contract execute in real time:

- Alice and Bob enter into a bet and place this bet on the Ethereum blockchain. All “nodes" on the Ethereum blockchain now hold a copy of this smart contract.

- This entire process is recorded on Ethereum's blockchain, creating a "common digital history" around this bet.

Smart contracts like these are what make Ethereum so compelling. A smart contract allowed Alice and Bob to build a very small "decentralized application" — their wager "self-executed" and paid out without using a middleman. What if we could build larger and more complex decentralized applications, i.e., souped-up smart contracts that can do complex things?

Source: Intellias

Thus, Ethereum creates a blockchain for any programmable use case — which we delve into below with dapps — whereas Bitcoin's blockchain was pioneered exclusively as a payments application.

What is Ether / ETH?

Ether (ETH) is the native cryptocurrency built into the Ethereum blockchain.

In order to transact or run decentralized applications, users of the blockchain must pay in ether. (The Bitcoin network's native cryptocurrency is called bitcoin, or BTC; similarly, users must use BTC to transact on the Bitcoin network.) The more computationally expensive an Ethereum-based application is, the more ETH that's required to run it. Like other cryptocurrencies, ETH is also traded by speculators and can be exchanged for USD or other currencies.

Note that because every single operation on Ethereum is executed by every node, computing is expensive. Therefore, the best current use cases for Ethereum are for running business logic: "if this, then that."

Other use cases might be prohibitively expensive. Due to current issues around scalability and the size of Ethereum's blockchain, more computationally intensive programs will find it difficult and expensive to operate. We dig into this later on.

on these secondary exchanges.

What are dapps?

Dapps are decentralized applications that are governed by smart contracts, rather than specific individuals or corporations. Once a smart contract is deployed, it cannot be altered (barring later upgrades or a new fork — i.e., splitting off into a new blockchain entirely). For example, a traditional bank may be able to reverse transactions, but anything recorded on the Ethereum blockchain cannot be reversed.

The bulk of today's existing dapps are built on Ethereum, though developers can opt to develop dapps on other blockchains as well.

Current dapps span a variety of use cases, including finance, storage, insurance, and health. Examples include:

- Compound, which allows people to borrow and lend digital assets
- Uniswap, which allows people to swap tokens through liquidity pools
- Etherscan, which allows users to read Ethereum transactions
- Decentraland, a metaverse where users can buy and sell virtual land, assets, interact with others, etc.

the network as a whole will always be able to serve clients looking to interact with the contract. Malicious actors therefore cannot launch denial-of-service attacks targeted toward individual dapps.

- **Privacy** – You don't need to provide real-world identity to deploy or interact with a dapp.
- **Resistance to censorship** – No single entity on the network can block users from submitting transactions, deploying dapps, or reading data from the blockchain.
- **Complete data integrity** – Data stored on the blockchain is immutable and indisputable, thanks to cryptographic algorithms called "primitives." Malicious actors cannot forge transactions or other data that has already been made public.
- **Trustless computation and verifiable behavior** – Smart contracts can be analyzed and are guaranteed to execute in predictable ways, without the need to trust a central authority. This is not true in traditional models; for example, when we use online banking systems, we are trusting that financial institutions will not misuse our financial data, tamper with records, or get hacked.

However, all of these benefits are contingent on well-written smart contracts. Bugs or vulnerabilities in smart contracts are easily hacked and are hard to fix given the immutable nature of being recorded on the blockchain.

Other potential issues with dapp development include network congestion (if the dapp requires too much computing power), poor user experience (given the difficulty of developing dapps), and inadvertent centralization in the pursuit of more user- or developer-friendly applications. In 2017, a bug in an Ethereum wallet, Parity, froze more than 500,000 ether — at the time worth over $150M and now worth more than $1B.

Regardless, there are more than 3,500 dapps being used by 150K+ daily active users, according to State of the DApps.

Source: State of the DApps

Many teams building on top of Ethereum launch their own "tokens" that provide utility within their decentralized applications. These are specialized tokens built on top of Ethereum.

A decentralized application's token might do any number of things. Most of the time, it provides utility within the decentralized application — for example, privacy-focused web browser Brave uses its own Ethereum-based token, the Basic Attention Token (BAT), to enable rewards and transactions within the browser.

What is Cryptokitties and how does it work?

Launched in November 2017 by Dapper Labs, CryptoKitties is an Ethereum-based game centered around digital, collectible cats. According to its website, each cat is "one-of-a-kind and 100% owned by you; it cannot be replicated, taken away, or destroyed." The game's "tokens" are the digital cats themselves, with ether used to purchase them.

CryptoKitties represented one of the earliest mainstream uses of non-fungible tokens (NFTs).

Let's have a look at Jaguar, a cryptokitty for sale:

Source: CryptoKitties

According to its profile, Jaguar has unique “cattributes” and is a “Gen 8” cat, or an eighth-generation cat. Jaguar has parents, who themselves had parents — all the way back to Gen 0. Ownership of these digital cats is tracked via the Ethereum blockchain, and pre-defined smart contracts determine each cat's unique “genetic and physical” characteristics and allow for buying, selling, and breeding.

Why does Ethereum matter?

In the original whitepaper, Ethereum founder Vitalik Buterin envisioned 3 branches of potential applications: financial, semi-financial, and other apps.

Financial applications, also known as decentralized finance (DeFi) apps, deal primarily with money — anything that traditional financial institutions handle, such as sub-currencies, derivatives, lending, wallets, and wills.

Currently, there is $56B locked in DeFi applications, which by and large are based on the Ethereum blockchain. MakerDAO represents one of the biggest applications, accounting for about 16% of this. On MakerDAO, users can lock in collateral to generate its stablecoin Dai, which is soft-pegged to the US Dollar.

Other examples include Compound, which allows users to borrow crypto assets against collateral or lock in their assets to earn interest, and Aave, another lending and borrowing protocol. Some investors have been able to earn interest at rates as high as 100% APR in apps like Compound and Aave by taking advantage of a process called "yield farming."

Semi-financial applications involve money but also have a "heavy non-monetary aspect" to them. This category would encompass apps like insurance, art trades, and more. With insurance, for example, a smart contract could leverage outside data to ensure that conditions have been met, then dole out compensation appropriately without need for a third party — insurance without the insurance company.

And finally, the third bucket would encompass all other applications that don't deal primarily with traditional financial use cases. This would include file storage, like a decentralized Dropbox, as well as decentralized autonomous organizations (DAOs). Whereas traditional corporations or organizations typically have several layers of governance, a DAO consists of a distributed network of stakeholders that each have power.

Here's another way to think about it: where Bitcoin could help users avoid banks, Ethereum could help users bypass all manner of platforms, from Facebook to Amazon to any number of more complex middlemen. Once upon a time, developers of a game or a collectible like CryptoKitties might have launched a Farmville-style game on Facebook or a physical product on Amazon.

leverages the proof-of-work (PoW) consensus mechanism to validate its blocks. While decentralization promises that recorded transactions can't be erased, hacks can theoretically still occur in the form of the 51% attack, in which a hacker takes over more than half of all of the network's mining power. This type of attack is difficult due to the immense cost; to pull off this type of attack on Ethereum today would cost more than $400,000 per hour.

But bugs and vulnerabilities can still make their way into smart contracts.

In 2016, a hacker stole $60M in ether from The DAO, one of the first decentralized autonomous organizations built on Ethereum. The hacker exploited a loophole in The DAO's smart contracts, sending the Ethereum community — still nascent at the time — into a panic.

Eventually, the stakeholders voted by majority to "hard fork" the blockchain, splitting it into 2 versions: one where the hack didn't happen and the funds were returned to the investors (this is what is known as Ethereum, and what the majority of people use now), and the original blockchain (now known as Ethereum Classic, which was expected to die off, though some still use it).

What are some issues with Ethereum?

For Ethereum to work, lots of participants need to hold up-to-date copies. This means that the same database is held by thousands of nodes. This is fairly inefficient.

Consider cloud computing: cloud computing allows multiple nodes to interact on a single database. These nodes don't have to hold their own private copy of this database.

Ethereum — and blockchain technology generally — mandates the inverse. All nodes have to hold a copy of Ethereum's blockchain. As of April 2020, running a full Ethereum archive node requires 4TB of space. By comparison, laptops typically offer 256GB, 512GB, or at most 1TB of internal storage.

Further, Ethereum nodes receive constant updates with the latest "state" of the Ethereum blockchain. Because nodes are distributed around the world, blockchains tend to have high latency (the amount of time it takes for data to move through the network).

Therefore, Ethereum is a relatively slow decentralized computer. It takes a while for every node to process every transaction: Ethereum maxes out at about 20 transactions per second. By comparison, Visa can process over 1,500 transactions per second.

Combined, Ethereum's size and transaction speed make it difficult to scale. For perspective, consider again that, at one time, CryptoKitties comprised over 10% of all transactions on Ethereum's

hours of electricity, which is comparable to the power consumption of Bulgaria, per Digiconomist.

Though individual transactions do not contribute to energy consumption, the significant carbon footprint of the overall PoW blockchain remains a hotly debated inefficiency issue.

Source: Digiconomist

In response, some have pushed back on the idea of equating base-layer emissions with the direct environmental impact of every single transaction. While many transactions still occur on the main chain, "Layer 2" applications aim to provide more scalable transactions that are off the main chain, allowing for faster transaction speeds and lower costs.

Up next: Ethereum 2.0

Ethereum in its current form has run into a number of issues. According to the Ethereum website, "high demand is driving up transaction fees that make Ethereum expensive for the average user. The disk space needed to run an Ethereum client is growing at a fast rate. And the underlying proof-of-work consensus algorithm that keeps Ethereum secure and decentralized has a big environmental impact."

Still, there's room for optimism.

to split the database into new chains, thereby reducing network congestion and increasing the number of transactions per second. Shard chains are expected to ship in 2021. The final step of completing Ethereum 2.0 — known as docking, which will merge the current Ethereum blockchain with each of the previous 2.0 upgrades — is expected to ship between 2021 and 2022.

The Ethereum 2.0 vision is one that has evolved over the years, but conviction around the platform has grown with the development of more practical applications. Questions of market value remain up in the air, but many remain bullish that greater scalability will drive usage and demand — potentially propelling Ethereum to realize the world computer vision it has for itself.

RESEARCH

JOIN 700,000+ CB INSIGHTS NEWSLETTER READERS

Email SIGN UP

www.cbinsights.com
info@cbinsights.com
212 292 3148
498 Seventh Avenue 12th floor New York, NY 10018

MOST POPULAR RESEARCH

Fintech

Fintech 250
State of Fintech
Amazon in Fin Services
Stripe Teardown

Healthcare

Digital Health 150
State of Healthcare
Future of Clinical Trials

Consumer

Retail Tech 100
State of Retail Tech
Corps in Self-Driving Cars
D2C Strategies

Emerging Tech

AI 100
Unicorn Companies

RESEARCH