What Is Ethereum?

Mar 30, 2017 at 9:07 p.m.
Dec 4, 2020 at 12:22 a.m.

Ethereum is a blockchain-based software platform that is primarily used to support the world's second-largest cryptocurrency by market capitalization after Bitcoin. Like other cryptocurrencies, Ethereum can be used for sending and receiving value globally and without a third party watching or stepping in unexpectedly.

Value exchange is the main use case of the Ethereum blockchain today, often via the blockchain's native token, ether. But many of the developers are working on the cryptocurrency because of its long-term potential and the ambitious vision of its developers to use Ethereum to give users more control of their finances and online data. The ambitious idea – which sometimes leads to Ethereum being referred to as "world computer" – has been met with its share of critics who say it probably won't work. But if this experiment rolls out as planned, it would spawn apps very different from Facebook and Google, which users knowingly or unknowingly trust with their data.

Ethereum enthusiasts aim to hand control back to users with the help of a blockchain, a technology that decentralizes data so that thousands of people around the world are handed a copy. Developers can use Ethereum to build leaderless applications, which means that a user's data cannot be tampered with by the service's creators.

Ethereum was first proposed in 2013 by developer Vitalik Buterin, who was 19 at the time, and was one of the pioneers of the idea of expanding the technology behind Bitcoin, blockchain, to more use cases than transactions.

While Bitcoin was created with the goal of disrupting online banking and day-to-day transactions, Ethereum's creators aim to use the same technology to replace internet third parties – those that store data, transfer mortgages and keep track of complex financial instruments. These apps aid people in innumerable ways, such as paving a way to share vacation photos with friends on social media. But they have been accused of abusing this control by censoring data or accidentally spilling sensitive user data in hacks, to name a couple of examples.

The platform officially launched in 2015, turning the idea of Ethereum into a real, functioning network.

Ethereum and a decentralized internet

Before you can understand Ethereum, it helps to first understand intermediaries.

Today intermediaries are everywhere. Behind the scenes, they help us accomplish all sorts of digital tasks. Gmail for instance helps us send emails. Venmo helps us send $10 to a friend.
This means that our personal data, financial information, and so forth are all largely stored on other people's computers – in clouds and servers owned by companies like Facebook, Google or PayPal. Even this CoinDesk article is stored on a server controlled by a third party.

This structure can be problematic, according to decentralization advocates. It means less direct control for users, and it also opens up opportunities for censorship, where the intermediary can step in and prevent a user from any action, whether buy a certain stock or post a certain message on social media, or block them altogether.

The idea of Ethereum is to change how apps on the internet work today, awarding users more control by replacing intermediaries with smart contracts that execute rules automatically.
Many, including inventors of the internet, believe the internet was always meant to be decentralized, and a splintered movement has sprung up around using new tools to help achieve this goal. Ethereum is one of the technologies to join this movement.

Ethereum FAQ

How is Ethereum different from Bitcoin?

Ethereum draws inspiration from Bitcoin. They are both cryptocurrencies. Ethereum uses the same technology behind Bitcoin, a blockchain, which uses a shared, decentralized public ledger to decentralize the network so it's not under the control of just one entity.
But while Bitcoin is used primarily as a store of value, the idea behind Ethereum is to decentralize other kinds of applications and services, from social media networks to more complex financial agreements.

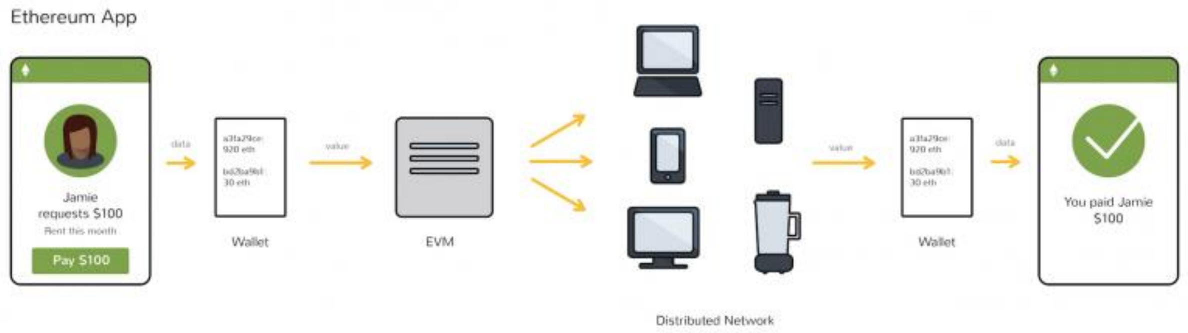
Why is Ethereum sometimes called a 'world computer?'

Many advocates see Ethereum as a "world computer" that could decentralize the internet.

With Ethereum, centralized servers are replaced by thousands of so-called "nodes" run by volunteers all over the world thus forming a "world computer." The hope is that one day, anyone in the world will be able to use it.

How does an Ethereum app work?

Scrolling through a typical app store you'll see a variety of colorful squares representing everything from banking to fitness to messaging apps. The long-term vision of the Ethereum community is to make apps that look just like these, but that work differently under the hood.



How an Ethereum app works*(Maria Kuznetsov)*

In short, the goal is for Ethereum apps to return control of the data in these types of services to its owner.

The apps built on Ethereum that offer this functionality are known as decentralized apps. Users need ether, **Ethereum's** native token, to use them.

What are the next steps for Ethereum?

It's worth noting that Ethereum has been met with healthy skepticism. For one, Ethereum is far from scalable, meaning it can't support many users right now, throwing a wrench in the idea of a "world computer" that disrupts Google, Facebook and other centralized platforms.

Ethereum 2.0, which was launched Dec. 1, 2020, aims to fix some of these issues. Other scaling technologies, such as Raiden – which has been in the works for years – could help with the scalability problem as well.

Authored by Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 02

How to Use Ethereum

Mar 30, 2017 at 9:09 p.m.
Dec 4, 2020 at 12:28 a.m.

Ethereum apps aim to give people more control over their online data. Using these apps is a matter of learning how to buy, store, and use its native token, ether.

If the Ethereum protocol, sometimes called the "world computer," develops as its proponents expect, it could provide alternatives to tech platforms, such as Facebook and Google, that many people have come to depend on. Generally, those alternatives would give users more control over their digital information. However, this control comes at a cost: ether. Every action on an Ethereum app, even as small as posting a short message to a microblogging platform, costs a little bit of ether. With ether fees, users can tap into a variety of apps on the platform.

These apps, also known as decentralized apps (dapps), are not free because the computing resources of the Ethereum platform are limited. The more people using the platform, the higher the fees. Since the number of services that interact with Ethereum right now is relatively high, so are the fees.

In this regard, Ethereum is still a work in progress. A network upgrade, Ethereum 2.0, is gradually being phased in to tackle Ethereum's underlying scalability issues. That will theoretically push fees lower while bolstering the security of the network.

Ethereum apps might not be as intuitive as the apps we use today, but anyone with a computer or smartphone can access them, as long as they have ether.

What is an Ethereum wallet?

Before we get some ether, we need a place to put it. This brings us to the idea of an Ethereum "wallet." Like its real-world counterpart, an ethereum wallet is made for storing value. (It is common practice to use lower case for "ethereum" or "ether" when referring to the currency, but upper for the network or protocol.)

Most wallets are digital apps that can be accessed from a smartphone or laptop. Furthermore, these digital wallets store digital money in the form of cryptocurrencies like bitcoin and ether.

Ethereum wallets store a user's private keys, which are secret keys that can be used to access ether. Each key is a unique long and jumbled string of letters and numbers that looks like this:

073d9dbee8875e7c91422d80413c85ba5e8e9fe7cad5dc001871dac882d07f2f

Only the owners of the private keys can use them to spend the money associated with them. These days, ethereum wallets

There are several types of Ethereum wallets made specifically for storing these private keys:

- Desktop wallets
- Mobile wallets
- Hardware wallets

- Paper wallets

Choosing one depends on your preferences for convenience and security. Usually these two concepts are at odds with one another: the more convenient, the worse the security (and vice versa).

When it comes to cryptocurrency wallets, there's one major caveat to keep in mind: losing your private key means losing your ether, forever. It is a much bigger deal than misplacing a password for an online service. This is where the absence of trusted third parties becomes a double-edged sword. While intermediaries are no longer needed to verify transactions, there's no help desk to turn to for help recovering your secret key.

Desktop and mobile wallets

Desktop wallets run on a PC or laptop, while some wallets are more portable and can be run on a smartphone. Some wallets offer both.

Desktop, mobile, and web wallets can be either:

- **Custodial**: Custodial wallets take care of your private key, which is like a password to your money. This is an easy option for users who are new to Ethereum or worried about losing their private key. However, with this type of wallet, users are still relying on a third party, which poses its own risks. These entities can get hacked, for instance.
- **Non-custodial**: With non-custodial wallets, you and only you are in control of your private key.

Because desktop and mobile wallets are running on a laptop or smartphone that's connected to the internet, they're less secure. As such, experts suggest keeping only a little money in them. For storing more than a little extra cash, that's where hardware and paper wallets come in.

Hardware wallets

Hardware wallets, electronic devices that are often as small as a thumb, offer more security. These devices are built for security and detached from the internet, and can sign and send ether transactions without being online. This is more secure because it is much harder to hack and is best used for storing large ether holdings.

Ledger and Trezor are two popular hardware wallets that can be used for holding ether.

Paper wallets

Another cold storage option is to print or carefully handwrite a private key on a slip of paper, a "paper wallet," and lock it somewhere secure like a safety deposit box.

MyEthereumWallet, or MEW, is one popular service for generating key pairs directly on your computer – not on a website's servers. Storing private keys on a server would mean trusting the company with access to your private keys, essentially a custodial wallet (see above). It would also leave those keys vulnerable if the site is ever hacked.
Tech-savvy users can generate keys using the command-line interface on a regular computer, which is used to directly input commands via text, provided they have the necessary cryptographic packages installed.

All that said, it bears repeating that if you lose your private key, it — and any ether associated with it — is gone for good. The best practice is to spend some extra time creating multiple copies of the private key and stashing them in different secure locations, in case one is lost or destroyed.

How can I buy ether?

The easiest way to obtain ether varies by location.

There are several methods to buy ether:

- A centralized exchange
- A compatible ATM
- Buying in person or via a peer-to-peer marketplace that connects users directly to one another

Finding an online ether exchange

Buying ether via a centralized exchange is usually the easiest option.

Popular exchanges such as Coinbase and Kraken allow users to buy ether directly with dollars or bitcoin. Typically there’s a sign-up process. These exchanges usually comply with Know-Your-Customer (KYC) laws, meaning they need to confirm a user’s identity before they can buy cryptocurrencies from the platform.

Buying ether with a currency other than the dollar might take an extra step.

Bitcoin is the most commonly used cryptocurrency, and people around the world are more likely to want to trade for it in their currency. So if you want to buy ether for Russian rubles, for instance, one easy option is to purchase bitcoin at an exchange and then trade that for ether.

That said, the official Ethereum website provides a list of buying options based on the country you reside in.

Ether ATMs

There are also hundreds of ether ATMs dotting the globe. This map from CoinATMRadar shows where these ATMs are located.
ATMs are less convenient since they can only be used in person, but they do offer a couple of advantages. While exchanges accept only digital forms of payment (such as credit cards), ATMs accept cash. Sometimes exchanges take a couple of days to send a user their ether, but ATMs are instantaneous.

Buying ether in person

Some users are privacy-conscious and would rather not use centralized exchanges, which often require a form of ID to use.

For these users, there's always the option of meeting in person to buy or sell ether, and some cities have frequent Ethereum meetups, including New York and Toronto. However, this isn't always an easy option in less populated areas.

Sites such as LocalCryptos connect users who want to trade by another peer-to-peer method, including directly by way of a bank transfer.

What can I do with ether?

What can users do once they have ether?

Once you have ether, you can use it to fuel decentralized apps (often called "dapps"), which are often similar to apps we use today, except they aim to cut intermediaries out of the picture.
These dapps are built from Ethereum smart contracts, code that automatically executes the terms of an agreement so that users don't have to rely on a third party to enforce the rules.
Examples of decentralized applications include:

- **CryptoKitties**: A game for collecting and breeding funny looking digital cats. Ethereum's innovation is that it allows users more control of their digital collectibles. For instance, the digital cat cannot be deleted, unlike in other games, where the collectibles only survive as long as the company that created them.
- **PeepEth**: PeepEth is a decentralized Twitter alternative. Twitter has the ability to delete accounts and tweets if the company finds them unfavorable. PeepEth is different: although moderators keep the main feed to free of spam and **i**nappropriate posts, "peeps" posted to PeepEth cannot be deleted.
- **DeFi**: decentralized finance (DeFi) is the term for the array of financial applications built on top of ethereum.

Some Ethereum apps have their own token, derived from ether. To participate in these, users need to trade ether for the token powering the app. For instance, Decentraland is a virtual world where users can buy virtual plots of land. It's different from games that don't use blockchain because users control the game, rather than a central entity.
Aggregator State of the Dapps lists nearly 3,000 such Ethereum dapps. While many are promising services and projects, sending ether to unvetted apps is not recommended.
Authored by Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 03

How Ethereum Works

Mar 30, 2017 at 9:12 p.m.
Dec 4, 2020 at 12:26 a.m.

Many of the apps we use day to day have companies in the middle making the app work. YouTube stores videos for people to view. Robinhood holds our money for investing in stocks. Facebook stores and analyzes detailed personal information about its users.

Ethereum is a platform that aims to make it easier to create applications that aren't managed or controlled by one entity. Instead they are governed by code.
Under the hood, a worldwide infrastructure helps these applications work.

Ethereum borrows heavily from Bitcoin's protocol and its underlying blockchain technology, but it adapts the tech to support applications beyond money. Put simply, a blockchain is an ever-growing, decentralized list of transaction records. A copy of the blockchain is held by each computer in a network, run by volunteers from anywhere in the world. This global apparatus replaces intermediaries.
At a high level, Ethereum is composed of several key pieces:

- **Smart contracts**: Rules governing under what conditions money can change hands.
- **The Ethereum Virtual Machine (EVM)**: The part of Ethereum that executes the rules of Ethereum, and makes sure a submitted transaction or smart contract follows the rules.
- **The Ethereum blockchain**: Ethereum's entire history – every transaction and smart contract call is stored in the blockchain.
- **Ether**: Ethereum's token, which is required to make transactions and execute smart contracts on Ethereum.
- **Proof-of-work**: This is Ethereum's consensus model, the glue holding the whole system together that ensures everyone on the network is following the rules.

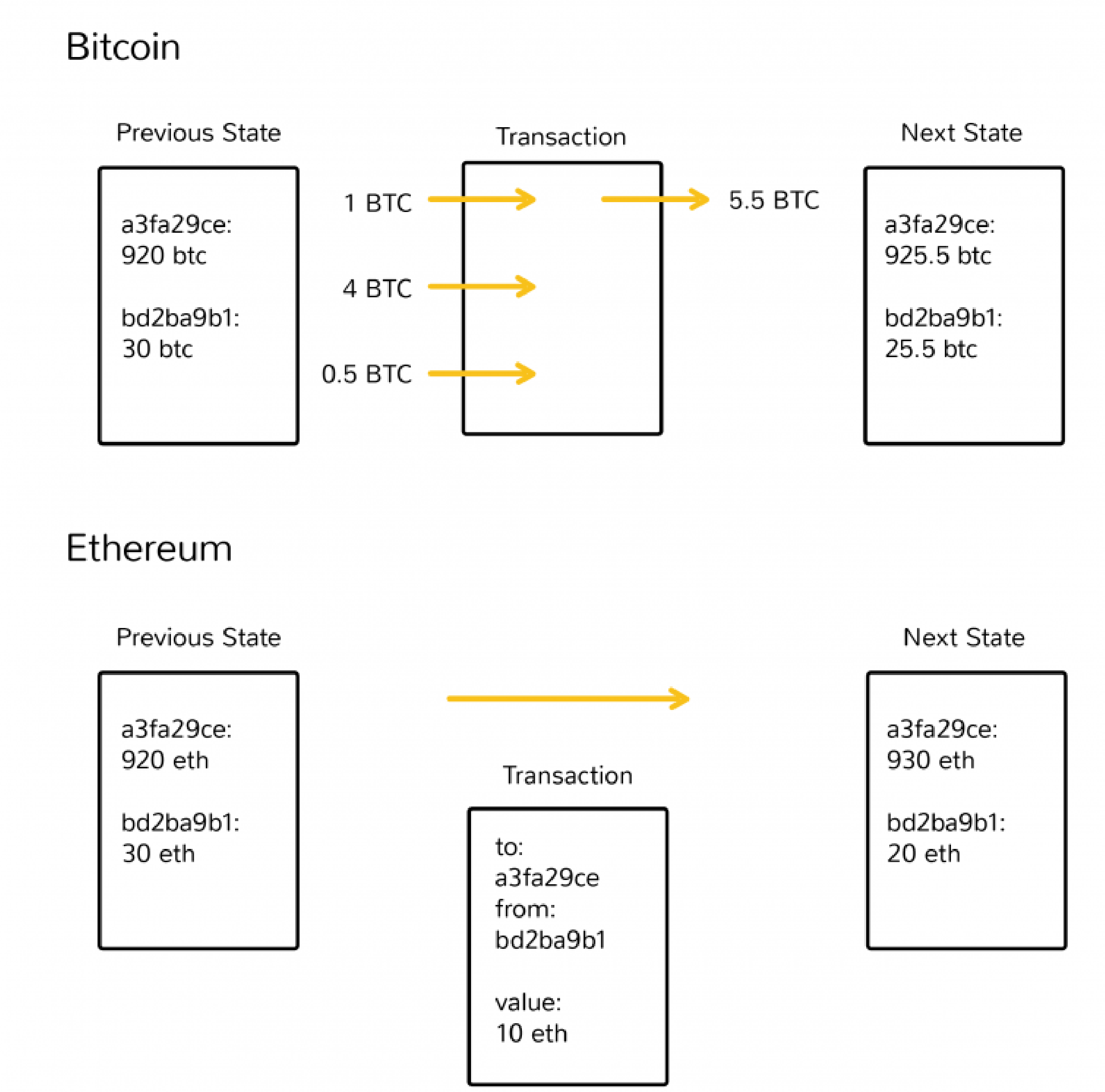
Ethereum developers are projected to enact some sweeping changes over the coming years, however. Ethereum 2.0, which began rolling out on Dec. 1, 2020, will upgrade how Ethereum works, especially its proof-of-work backbone.

Ethereum smart contracts

Let's start with smart contracts, because they're kind of the whole point of Ethereum.

Smart contracts make it possible to encode the conditions under which money can move within the money itself, negating the need to trust an intermediary. They are a part of any cryptocurrency. Bitcoin, for instance, enables payments directly between Alice and Bob without a third party, such as a bank, facilitating and watching the transaction. Before cryptocurrency, that was not possible in online commerce.

Ethereum aims to expand smart contracts by abstracting away Bitcoin's design so developers can use the technology for more than simple transactions, expanding its use to agreements with additional steps and new rules of ownership. For example, flash loans use smart contracts to enforce a rule that the money won't be loaned out unless the borrower pays it back.



(Maria Kuznetsov)

Some Ethereum services, such as Compound, are experimenting with allowing users to loan or borrow money with smart contracts managing the money rather than a company.
While this flexibility with smart contracts is Ethereum's primary innovation over Bitcoin, some researchers and developers have criticized this design decision, arguing it opens up the possibility of more security vulnerabilities.

The Ethereum blockchain

The history of all these smart contracts is stored in the Ethereum blockchain. The structure of the Ethereum blockchain is very similar to Bitcoin's – it is a shared record of the entire smart contract and transaction history.

Hundreds of volunteers from around the world store a copy of the complete Ethereum blockchain, which is quite long. This is one feature that makes Ethereum decentralized.

Each of these is called a “node” in Ethereum’s network. Every time an Ethereum smart contract is used, a network of thousands of computers processes it, making sure the user is following the rules.

All of these nodes are connected. In addition to storing this data, each Ethereum node follows the same set of rules for accepting transactions and running smart contracts.

In contrast to Bitcoin, Ethereum nodes store more than just transaction details. The network needs to keep track of the “state” – or the current information – of all of these applications, including each user’s balance, all the smart contract code, where it’s all stored, and any changes that are made.

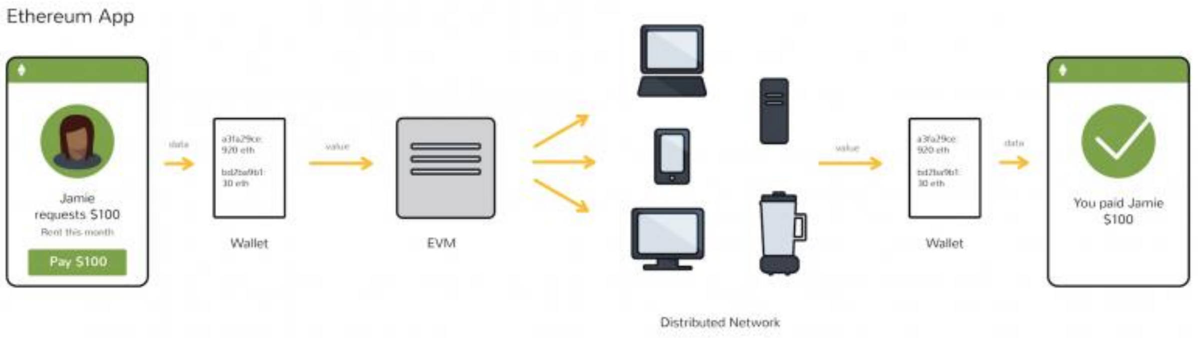
Here’s a summary of what’s stored in each node:

- **Accounts**: Each user can have an account, which shows how much Ether the user has.
- **Smart contract code**: Ethereum stores smart contracts, which describe the rules that need to be met for money to be unlocked and transferred.
- **Smart contract state**: The state of the smart contracts.

The Ethereum Virtual Machine (EVM)

Each Ethererum node also has an Ethereum Virtual Machine (EVM) that executes the smart contracts. All the nodes run in sync.

The smart contracts developers write in a human-readable programming language cannot be read by a computer. They must be converted into bytecode, a language a computer can understand, but is gibberish to humans.



(Maria Kuznetsov)

Then the EVM takes over. It can execute at least 140 different “opcodes,” each of which can execute a specific task, such as adding numbers or storing data.

Ether and Ethereum transactions

(Chris Liverani/Unsplash)

How do users interact with Ethereum?

Using smart contracts and using Ethereum apps requires money in the form of ether, Ethereum’s native token. Ether is needed for doing just about anything on Ethereum, and when it’s used to execute smart contacts on the network it’s often referred to as “gas.” The ether can be used to call smart contracts: For example, a contract could trigger a post on Twitter (or an alternative), or it could trigger an account to begin borrowing coins on an Ethereum-based lending platform.
Ethereum uses accounts to store the ether, analogous to bank accounts.

There are two types of accounts:

- **Externally owned accounts (EOAs)**: The accounts that normal users use for holding and sending ether.
- **Contract accounts**: These separate accounts are the ones that hold smart contracts, which can be triggered by ether transactions from EOAs or other events.

Calling smart contracts isn’t free. Each transaction costs *some* ether, which increases depending on how much computation the transaction is using. Also, when Ethereum is congested, fees go up.
Find more about accounts here.

Ethereum proof-of-work

Remember that every node in the network holds a copy of the transaction and smart-contract history of the network. Every time a user performs some action, all of the nodes on the network need to come to agreement that this change took place.

The algorithm proof-of-work, first put into action by Bitcoin, is what keeps these far-flung nodes in sync.

Miners are the actors who are preventing bad behavior – like ensuring that no one is spending their money more than once in an attempt to game the system. Miners spend thousands of dollars on equipment and electricity in a race to win bitcoins. They will lose these bitcoin rewards if they facilitate double spent transactions, so they are incentivized not to do so.

The goal here is for the network of miners and nodes to take responsibility for transferring the shift from state to state, rather than some authority such as PayPal or a bank. Bitcoin miners validate the shift of ownership of bitcoins from one person to another. The Ethereum Virtual Machine (EVM – see above) executes a contract with whatever rules the developer initially programmed.

But, Ethereum might not be using proof-of-work for long. Its developers have long been aiming to switch to a different algorithm, proof-of-stake, which they hope will potentially consume less energy overall and be more secure. The algorithm is controversial in some circles. Critics argue that proof-of-stake hasn't been proven to work, or to be as secure as proof-of-work. Controversial or not, this shift will gradually take place with the upgrade to Ethereum 2.0, which started on Dec. 1, 2020.

Ethereum FAQ

How will Ethereum 2.0 change how Ethereum works?

When fully implemented (estimated in a few years), Ethereum 2.0 will dramatically change how Ethereum works. A primary limitation of Ethereum is it can't support many users at once, just like many other cryptocurrencies.

Even with Ethereum 2.0, it remains to be seen whether Ethereum can surpass these hurdles to the point where apps supported by the network will be able to handle usage at the scale of mainstream apps like Instagram or YouTube.

Why have Ethereum gas fees been going up recently?

This is an integral part of Ethereum. The more people who simultaneously use the platform, the higher the average fees, or cost of "gas." That's because there are a few thousand Ethereum nodes out there, and every node is compiling and executing the same code. But, you might be thinking, isn't that much more expensive than a normal computation? Yes, it is. Developers are trying to make it cheaper.

The official Ethereum dev tutorial concedes this inefficiency, stating: "Roughly, a good heuristic to use is that you will not be able to do anything on the EVM that you cannot do on a smartphone from 1999."

Where can I learn more about how Ethereum works?

We've only just scratched the surface. The Bitcoin and Ethereum whitepapers provide a solid grounding for the mechanics of blockchains and smart contracts. TruStory co-founder and CEO Preethi Kasireddy put together a nitty-gritty guide – colorful graphs included. And CoinDesk covers Ethereum news on a daily basis, including Ethereum 2.0 progress and setbacks, which will overhaul how Ethereum works.

By Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 04

What Is a Decentralized Application?

Mar 30, 2017 at 9:13 p.m.
Dec 17, 2020 at 1:09 a.m.

Decentralized applications (also known as "dapps") provide services similar to those offered by typical consumer applications, but they use blockchain technology to grant users more control over their data by eliminating the need for centralized intermediaries to manage the data, thus making the service "decentralized."

Digital apps are ubiquitous in today's world. Consumers use apps for sending email, paying for parking, finding dates and myriad other use cases. Under conventional models of control and ownership, consumers usually hand over personal data to the company providing the service. With a decentralized app, users theoretically gain more control over their finances and personal data since they don't have to trust anyone else to store and secure the information. However, some experts are skeptical this will work in practice.

One of the main goals of the founders of Ethereum, the platform that supports the world's second-largest cryptocurrency, is to make these kinds of apps easier to create. There are many challenges in trying to reach this goal.
But there has been progress. Hundreds of dapps exist today on Ethereum, ranging from a Twitter replacement to a decentralized virtual reality game. Many are slow and difficult to use, but they give a taste of the potential for decentralized apps in the long term. Developers hope Ethereum 2.0, a long-awaited upgrade that officially started being rolled out on Dec. 1, 2020, will ease these problems in the coming years.

How does a dapp work?

Dapps built on Ethereum use blockchain technology under the hood to connect users directly. Blockchains are a way to tie together a distributed system, where each user has a copy of the records. With blockchains under the hood, users don't have to go through a third party, meaning they don't have to give up control of their data to someone else.
By their nature, centralized entities have power of the data that flows into and out of their networks. For example, financial entities can stop transactions from being sent, and Twitter can delete tweets from its platform. Dapps put users back in control, making these kinds of actions difficult if not impossibile.

There isn't one agreed-upon definition of a dapp as it's a relatively new concept. But the key characteristics of a dapp include:

- **Open source**: The code is public for anyone to look at, copy and audit.
- **Decentralized**: Dapps don't have anyone in charge, so no central authority can stop users from doing what they want on the app.

- **Blockchains**: If there isn't a central entity, then what's holding the app together? Dapps use an underlying blockchain (such as Ethereum) to coordinate instead of a central entity.
- **Smart contracts**: Decentralized applications use Ethereum smart contracts, which automatically executes certain rules.
- **Global**: The goal is for anyone in the world to be able to publish or use these dapps.

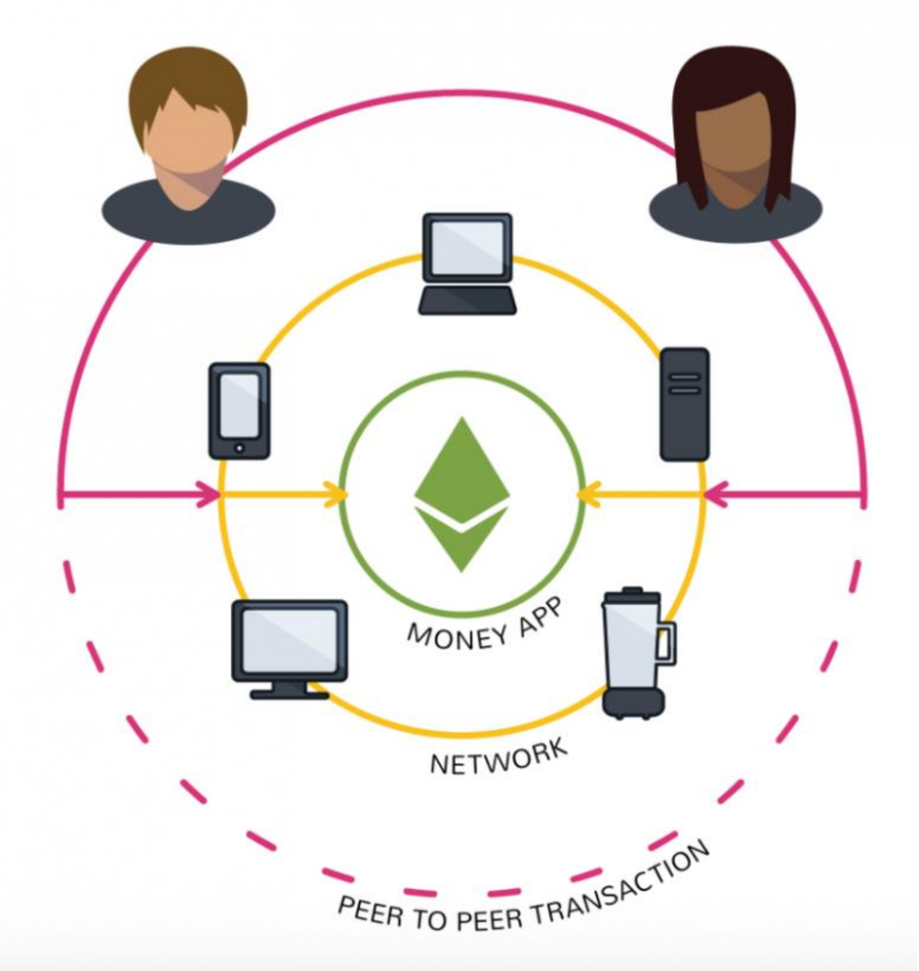
What are dapps used for?

The Ethereum white paper published by Ethereum creator Vitalik Buterin in 2013 splits dapps into three main types:

- **Financial apps**: These are applications where money is involved.
- **Semi-financial apps**: Decentralized apps that involve money, but also require another piece, such as data from outside the Ethereum blockchain.
- **Other apps**: Every other type of decentralized app developers are looking to create, including online voting and storage apps.

Financial applications

Financial applications are popularly known as DeFi applications, short for "decentralized finance." The idea is to use blockchains (especially Ethereum) to improve more complex financial applications – such as lending, wills and insurance – and stablecoins, alternative coins that aim to stabilize cryptocurrency prices.



(Maria Kuznetsov)

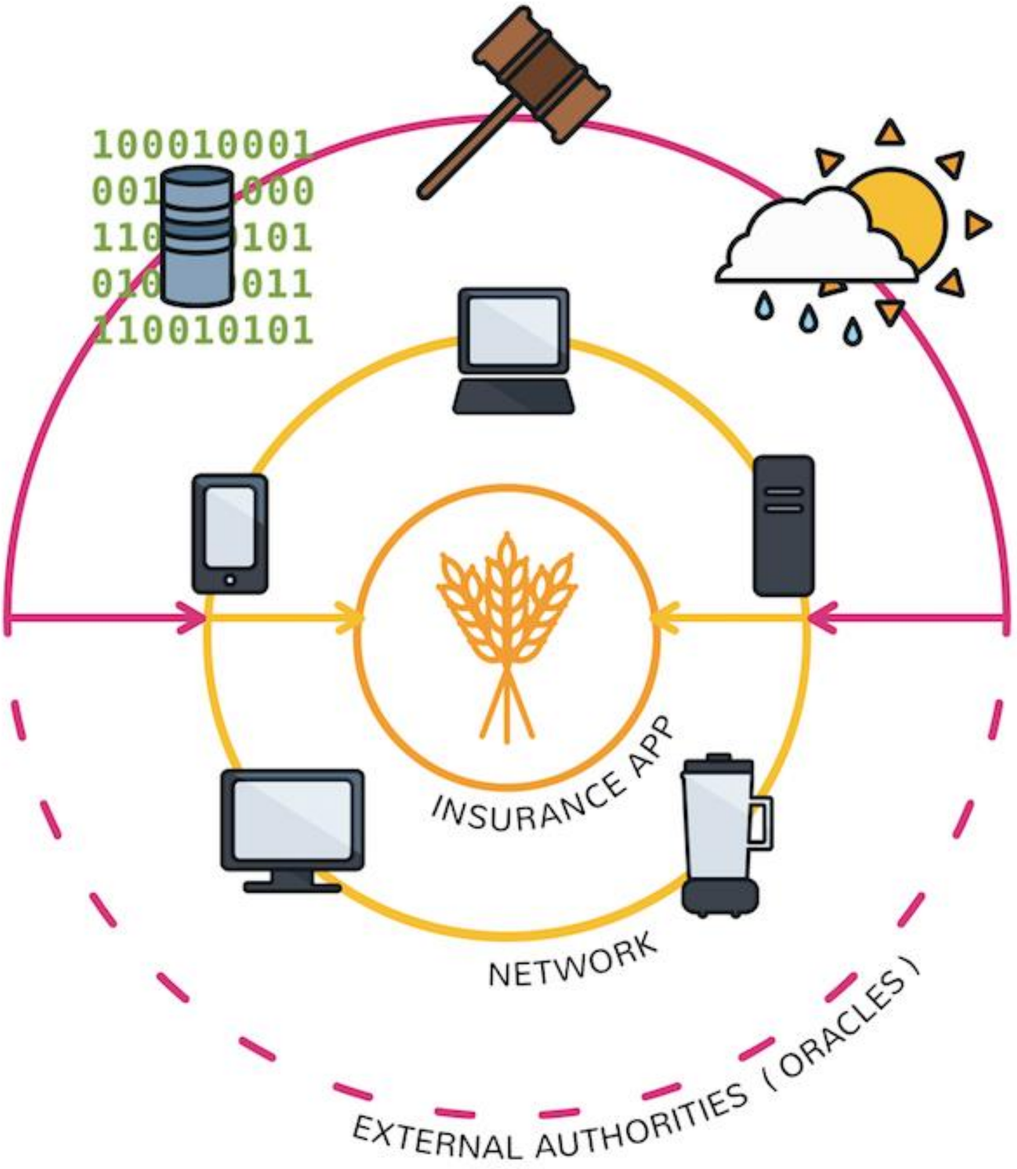
Semi-financial apps

The second type of app is similar, but it mixes money with “a heavy non-monetary side” as Buterin puts it in the Ethereum white paper.
Buterin gives the example of Ethereum developers setting up “bounties,” rewards that can only be unlocked if someone accomplishes a task. In western movies, bounties are doled out to outlaws able to catch a person or criminal. But, in this case, they are rewarded for far less dangerous tasks, such as solving a difficult computational problem.

The magic here is the smart contract is (in theory) able to tell if the bounty hunter has provided a working solution, only disbursing the funds if this condition is met.

Another example is a crop insurance application that’s dependent on an outside weather feed. Say a farmer buys a derivative that automatically pays out if a drought wipes out her crops.

These smart contracts rely on so-called “oracles” that relay up-to-date information about the outside world, like how many inches of rain fell last season.



(Maria Kuznetsov)

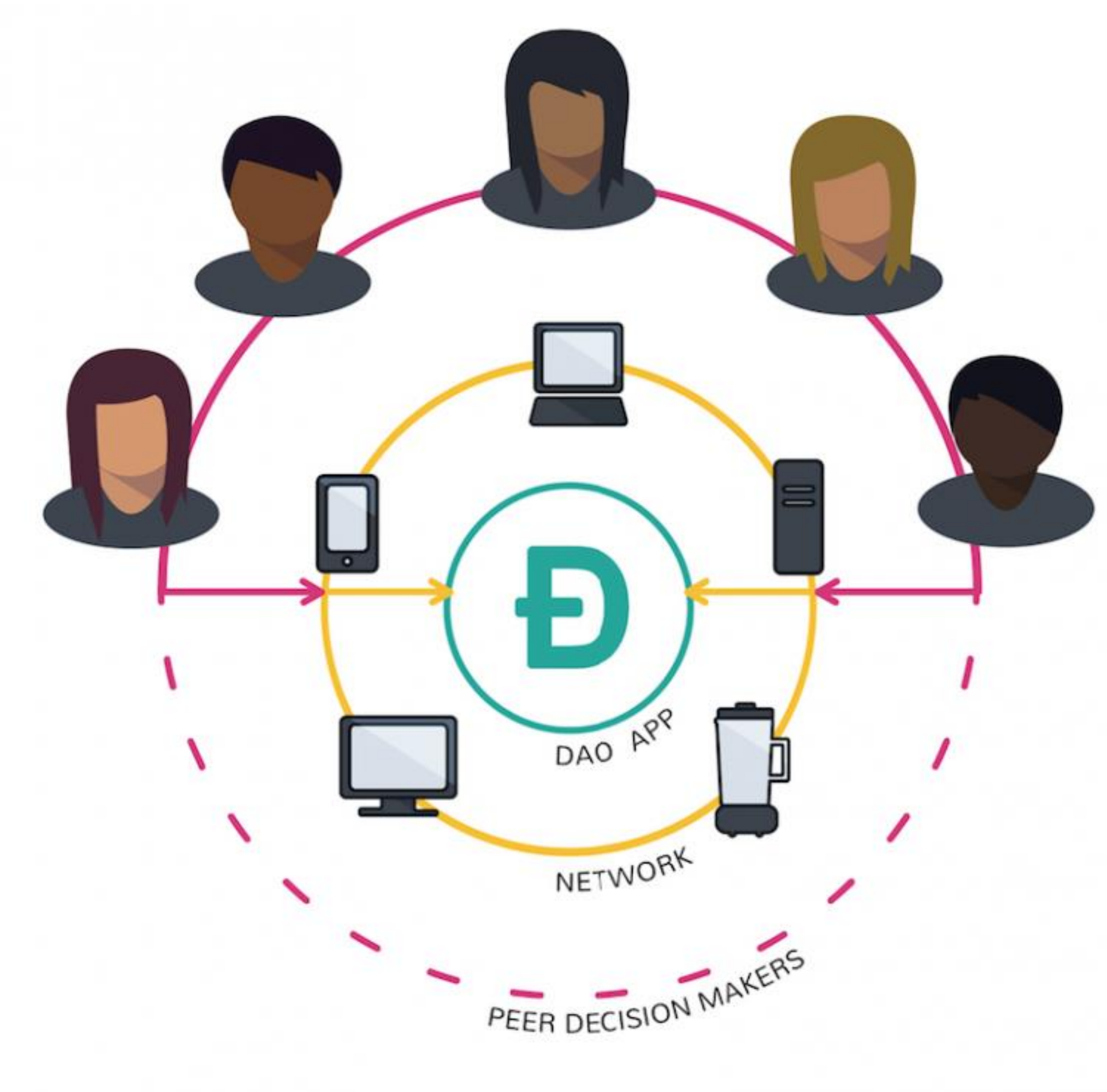
The major caveat, though, is that many developers are skeptical oracles can be used in a decentralized way. Users have to trust that the data feed is providing the correct data, and not gaming the data for their own financial interest.

Other applications: DAOs and beyond

Ethereum is a flexible platform, so developers are dreaming up other ideas that don't fit into the usual financial classifications.

One example is to use this approach to create a decentralized social network that's resistant to censorship. Most mainstream social apps, such as Twitter, censor some posts, and some critics argue those social apps apply inconsistent standards about what content is censored or "downranked."

So, with a decentralized app like Peepeth, once you publish a message to the blockchain, it can't be erased, not even by the company that built the platform. It will live on Ethereum forever.
Some have explored taking this idea of decentralization even further. If Bitcoin can do away with financial authorities, is it possible to do the same for companies and other types of organizations?



(Maria Kuznetsov)

Decentralized Autonomous Organizations (DAOs) are one particularly ambitious breed of dapp that attempts to answer "yes" to that question. The goal is to form a leaderless company by programming rules at the beginning about how members can join, vote, how to release company funds and more. Once launched, the DAO would operate under these rules indefinitely.

What challenges do dapps face?

Dapps are early, experimental, and developers have yet to solve several crucial problems with the underlying network holding them back. For one, dapps can be very expensive to run when Ethereum grows more congested with users. Although traditional apps sometimes have issues with scale, those issues are exacerbated in a decentralized environment, which by its nature can't operate without a certain level of cooperation and coordination among multiple stakeholders.

How do developers create decentralized apps?

Ethereum developers have created many low-level coding tools, like smart contract builder Truffle and Web3, a way to interact with Ethereum with the popular programming language Javascript, so developers from around the world can experiment with dapps in an effort to turn the dream into reality.

Authored by Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 05

What Is a DAO?

Mar 30, 2017 at 9:14 p.m.
Dec 23, 2020 at 2:48 a.m.

A Decentralized Autonomous Organization, or DAO, is a theoretical organization or company operated by code instead of people. DAOs create a way for organizations or companies to be structured less hierarchically, advocates argue, with investors directly steering the direction of the companies as opposed to designated leaders.

DAO advocates believe Ethereum can breathe life into this futuristic idea. Ethereum is the second-largest cryptocurrency by market capitalization and is the largest platform for using the technology behind cryptocurrency – blockchain – for uses beyond money. The thought is that if bitcoin can do away with middlemen in online payments, can the same or comparable technology do the same for middlemen in companies? What if entire organizations could exist without a central leader or CEO running the show? Many consider DAOs to be one of the loftiest ideas stemming from Ethereum, and many argue the real-world realization of the idea will likely not lead to wise decision-making.

But others think the idea of an organization with decentralized control holds promise and are experimenting to bring it to life. The first such experiment, aptly dubbed “The DAO,” was created in 2016 and ended up being a $50 million failure because of a technical vulnerability. However, organizations like Aragon, Colony, MakerDAO and others are picking up where The DAO left off.

A driverless car as a DAO

Imagine this: a driverless car cruises around in a ridesharing role, essentially an autonomous Uber. Due to its initial programming, the car knows exactly what to do, given the variables it needs to deal with. It finds passengers, transports them, and accepts payments for its transportation services.

A ridesharing service of driverless cars could theoretically work like a DAO.*(Smith Collection/Gado/Getty Images)*

After dropping someone off, the car uses its profits for a trip to an electric charging station, using ether – Ethereum's native token used for paying to use decentralized apps – to pay for the electricity.
This car is just one in a fleet of vehicles owned by a DAO. As the cars earn ether, the money goes back to the shareholders that have invested in the entity.

That's one "thought experiment" brought to you by former bitcoin contributor Mike Hearn in which he describes how cryptocurrency and blockchains could help power leaderless organizations in the future. What Hearn described is one fanciful use case for a DAO, an idea that began to get traction in the crypto community not long after bitcoin was released in 2009.

DAO FAQ

Why run a company with code?

One inherent advantage of DAOs, advocates argue, is that they enable the building of fairer organizations than the human-run kind.

Most companies today have leaders who sometimes make unilateral decisions that affect the entire company. A DAO would make this kind of decision-making impossible; stakeholders (i.e. investors in the company) have more direct control over how the company should operate.

How does a DAO work?

In short, DAOs aim to hard-code certain rules to drive the company or organization from the get-go.

DAOs are based on Ethereum smart contracts, which can be programmed to carry out certain tasks only when certain conditions are met. These smart contracts can be programmed to automatically execute typical company tasks, such as disbursing funds only after a certain percentage of investors agree to fund a project.
Many see DAOs as a way to more rigorously guarantee democracy. Stakeholders can vote on adding new rules, changing the rules or ousting a member, to name a few examples. And the DAO simply won't be able to change unless the required threshold of people vote for the change.

Some proposed characteristics of a DAO include:

- **No hierarchy**: There's often no hierarchical management. Stakeholders usually make decisions instead of leaders or managers.
- **Transparent**: The code is open source, meaning anyone can look at it. On the blockchain, anyone can scan through the history to see how decisions were made.
- **Open access:** Anyone with internet access could hold DAO tokens or buy them, thus giving them decision-making power in the DAO.
- **Democratic changes:** Investors can change the rules of a DAO by voting on new proposals.
- **Recruiting:** A DAO could even theoretically hire outside talent, since there are still tasks that only humans can do. For example, the driverless car in the DAO described above could automatically hire a repairman, based on sensors reporting to the DAO when damages occur.

Has a DAO been tried before?

Yes. The best-known attempt at creating such an organization was aptly called “The DAO.”

Launched in 2016, The DAO failed in a matter of months, but it’s still the preeminent example of what people have in mind when they talk about the technology.

The plan was for investors in The DAO to receive tokens proportional to how much ether they invested in the project. With those tokens they could vote for which projects to fund. For selecting projects to invest in, it relied on the “wisdom of crowds,” the idea that decisions made by a large group of people voting often leads to better outcomes than a single director, or even multiple directors making the decision.
If the projects that were invested in profited, the profits would be distributed back to the investors.

Why did The DAO fail?

It’s easy to see why “unstoppable code” can pose a security problem.

That was the problem with The DAO. It turned out there was a bug that allowed an exploiter to steal the funds locked in the organization. Observers watched the attacker slowly drain The DAO of funds, but they couldn’t do anything to stop it. Technically, the hacker was following the rules as they were deployed.

Ethereum’s lead coders reversed the transaction history to return funds to their owners – a controversial decision that led to a rift in the community. The best way to handle a similar situation in the future is still up to debate.

What are some problems with DAOs?

As shown with The DAO, unstoppable code can pose a problem. It’s difficult to change the rules of the DAO once it’s deployed to the Ethereum blockchain. The same framework that prevents a person or entity from altering the organization without consensus from the community can also cause problems, the main one being that any gaps in the framework aren’t easily closed. That can lead to potential theft, money loss or other disastrous consequences.

Authored by Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 06

How Do Ethereum Smart Contracts Work?

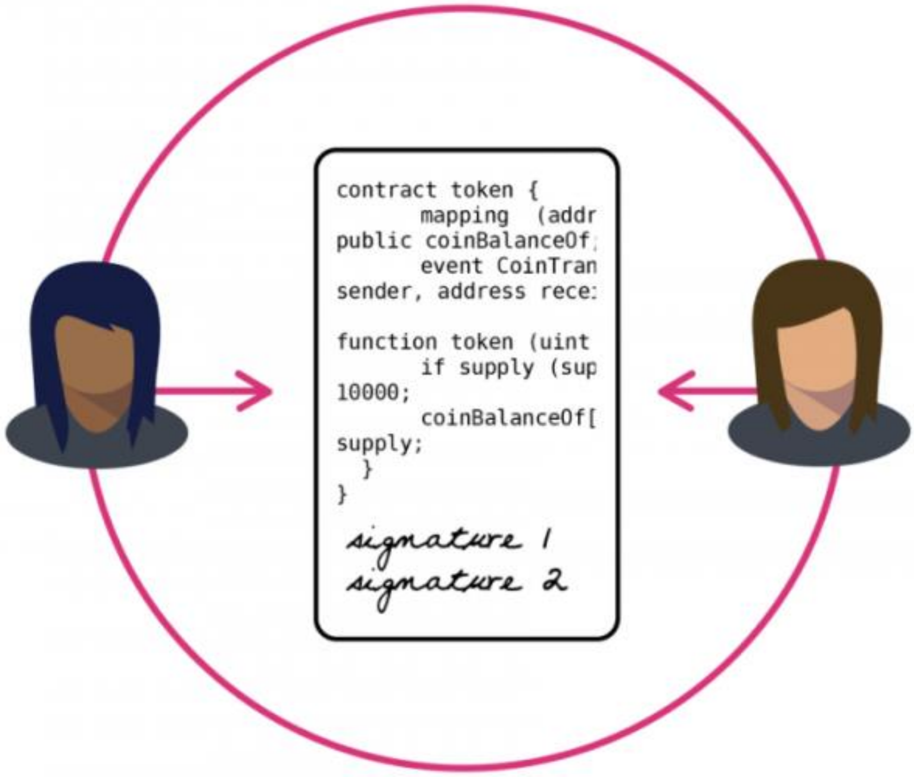
Mar 30, 2017 at 9:15 p.m.
Dec 30, 2020 at 8:18 p.m.

Smart contracts are tools that can automatically execute transactions if certain conditions are met without requiring the help of an intermediary company or entity. They are often associated with Ethereum, a blockchain that was designed to accommodate smart contracts, but the idea isn't restricted to any particular platform or network.

Whether obvious or not, intermediaries permeate our digital lives. Even simply sharing a cat photo with friends online requires the services of an intermediary like Facebook or Twitter – a central authority that doesn't just manage the network, but also set the rules and enforce their violation. Smart contracts make it possible to automate these digital tasks without needing a centralized entity to manage and approve the transaction.

Smart contracts are made possible by blockchains, a network of computers that work together to enforce rules on the network without requiring the help of an intermediary.

With conventional contracts, a document outlines the terms of a relationship between two parties, which is enforceable by law. If one Party A violates the terms, Party B can take Party A to court for not complying with the agreement. A smart contract fortifies such agreements in code so the rules are automatically enforced without courts (or any third party) getting involved.



```
contract token {
       mapping  (addr
public coinBalanceOf
       event CoinTran
sender, address rece:

function token (uint
       if supply (sup
10000;
       coinBalanceOf[
supply;
  }
}
```

(Maria Kuznetsov)

Ethereum, the world's second-largest cryptocurrency by market cap, was created in 2013 specifically for creating smart contracts. To date, it is the most popular platform for doing so.

Smart contracts aren't widely used outside of Ethereum, and some are skeptical they'll ever achieve mainstream popularity as a way to manage transactions. Ethereum proponents, however, believe they could eventually become the norm for executing and securing online relationships.

Hundreds of apps that use smart contracts are already up and running. Popular Ethereum apps MakerDAO and Compound use smart contracts at their core for lending and allowing users to earn interest.

First conceived in 1993, the idea of a "smart contract" was originally described by computer scientist and cryptographer Nick Szabo as a kind of digital vending machine. In his famous example, he described how users could input $1, and receive an item from a machine, in this case a snack or a soft drink.

Smart contracts are the same in that with a certain input (the $1), the user should be able to expect a certain outcome (the chosen drink).

In a simple example of an Ethereum smart contract, a user sends a friend 10 ether – the token native to Ethereum – but requires that it can't be dispersed until after a certain date using a smart contract.

Why Ethereum smart contracts?

The world's first cryptocurrency, Bitcoin, was the first to support basic smart contracts, although they are extremely limited in comparison with Ethereum. Each transaction is a smart contract because the network will only approve of the transactions if certain conditions are met – that the user provides a digital signature proving that they indeed own the cryptocurrency they claim to own. Only the owner of a Bitcoin private key can produce such a digital signature.

By contrast, Ethereum replaces Bitcoin's more restrictive language, replacing it with language that allows developers to use the blockchain to process more than just cryptocurrency transactions. The language is "Turing-complete," meaning it supports a broader set of computational instructions. Without limits, programmers can write just about any smart contract they can think of.

While this has obvious advantages, it also means that, because novel smart contracts are less tested, there is a higher chance of vulnerabilities. Ethereum has already seen millions of dollars of losses from exploited vulnerabilities in smart contracts.

Smart contract FAQs

What can smart contracts be used for?

Some common ways of using smart contracts are:

- **Multisignature accounts**: Funds can only be spent when a required percentage of people agree.
- **Encoding financial agreements**: Manage agreements between users. Say, if one person buys insurance from an insurance company, the rules of when the insurance can be redeemed can be programmed into a smart contract.
- **Agreements based on the outside world**: Pull in data from the outside world (financial, political, or whatever) with the help of oracles.
- **Provide third party**: Similar to how a software library works, smart contracts can work with other smart contracts in a chain.
- **Storage**: Store information about an application, such as domain registration information or membership records. Storage in a blockchain like Ethereum is unique in that the data is immutable and can't be erased.

How can smart contracts work together?

Smart contracts aren’t intended to be used in isolation. Some smart contracts are built to assist other smart contracts.

When someone, say, places a simple bet on the temperature on a hot summer day via a smart contract, it might trigger a chain reaction of contracts under the hood. One contract would use outside data to determine the weather, and another contract could settle the bet based on the information it received from the first contract when the conditions are met.

With this in mind, smart contracts form the building blocks for decentralized applications and even whole companies, dubbed decentralized autonomous companies, which are controlled by smart contracts rather than human executives.

How is a smart contract set up?

A developer can create a smart contract by writing a slab of code – spelling out the rules, such as that 10 ether can only be retrieved by Alice 10 years from now.

The developer then pushes the smart contract to the Ethereum network, which is what enforces the contract – not allowing anyone to take the money unless they follow the exact rules in the code. Thousands of computers from around the world then all have a copy of this smart contract.

How do I use a smart contract?

Anyone can use smart contracts if they have Ethereum's native token ether, which can be bought on cryptocurrency exchanges.
Ethereum apps will usually provide instructions for how to use their specific app and underlying smart contracts. A common method is to use an Ethereum wallet tool, such as Metamask, to send the ether.

Users can use smart contracts for a range of use cases. Users can publish uncensorable posts to microblogging apps or lend out money without an intermediary, using a variety of Ethereum apps.

Do smart contracts cost anything?

Getting thousands of computers across the world to validate smart contracts often isn't cheap, though, as recent ballooning Ethereum fees highlight. The user must pay a fee, typically in ether (Ethereum's native token), to keep the network up and running**.** Fees go up when the network grows more congested.

Are smart contracts legally enforced?

To many Ethereum advocates, smart contracts are intended to live outside of the legal system because they are enforced automatically. If they work as they're supposed to, users won't need to go to a court to settle conflicts.

That said, many wonder how these contracts would be treated under the current legal system. The answer is complicated. One 2018 research paper from partners Stuart D. Levi and Alex B. Lipton determined that U.S. law should recognize many smart contracts.
But, every country has a different legal approach to cryptocurrencies and blockchains, with some more accepting of the new technology than others.

Are smart contracts the future?

Many developers, researchers, and even lawyers and doctors are excited about the promises of smart contracts.

But it's early days for smart contracts. While users of smart contracts don't need to trust intermediaries, users must trust that the code was written correctly, which is a big ask seeing as there are still plenty of security issues. Many bug exploits have been unearthed over the years which allowed bad actors to steal user funds. The hope is these issues will grow rarer as the code matures.

By Alyssa Hertig
DISCLOSURE
The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 07

How Ethereum Mining Works

Mar 30, 2017 at 9:11 p.m.
Dec 23, 2020 at 10:04 a.m.

With Ethereum, the world’s second-largest cryptocurrency by market capitalization, participants known as “miners” use expensive hardware to run calculations in an effort to earn rewards. By doing this, they mint Ethereum tokens, known as ether, at a steady pace.

Cryptocurrency mining was invented by Bitcoin creator Satoshi Nakamoto, a figure shrouded in mystery – no one knows their real identity. Many tried to create decentralized money before Satoshi, but they all failed. Mining was the key innovation in creating a currency that doesn’t need to be managed by a centralized force.

Ethereum copied this technique in pursuit of its own mission of decentralizing the internet and building decentralized apps that don’t have central entities that manage the service and can stop users from doing what they want.

Before exploring how Ethereum mining works, it’s important to understand why mining exists at all. There are a couple of key reasons:

- **To mint ether without a central issuer**: Ethereum’s tokens, ether, are used to pay for apps on the network and are created through the process of mining at a rate of five ether roughly every 13 seconds.
- **To keep the network working correctly**: Without mining, tokens could be double-spent by nefarious actors, which would devalue or even destroy the entire network.

Mining ether

Approximately every 12-15 seconds, an Ethereum miner finds a block. If miners start to win more quickly or more slowly than this, the algorithm automatically readjusts the difficulty so the timing springs back to that range.

The miners “win” these ether by mining them. Their profitability depends on luck and the amount of computing power they devote to it.

Keep the Ethereum working correctly`

The second point is important. Usually, banks are in charge of keeping accurate records of digital transactions. They ensure that money isn’t created out of thin air, and that users don’t cheat and spend their money more than once.

Blockchains such as Ethereum, with the help of mining, use a new way of record-keeping, one where a network of global users, rather than an intermediary, verifies transactions and adds them to the public ledger.

Although a “trustless” or “trust-minimizing” monetary system is the goal, someone still needs to secure the financial records, ensuring that no one cheats.

Mining is the key innovation that makes decentralized record-keeping possible.

How Ethereum mining works

Ethereum’s current mining process is almost the same as bitcoin’s.
For each block of transactions, miners use computers to repeatedly and very quickly produce random values until one of them stumbles upon the correct one. The correct answer unlocks the ether.

It’s very (very) difficult for miners to cheat at this game. There’s a less than microscopic chance that a miner can fake this work and come away with the correct answer. That’s why the puzzle-solving method, also called the “consensus mechanism,” is called “proof-of-work.”

“Nodes” are another important piece of the Ethereum network, each of which contains a copy of the ledger that records all ether transactions. There are thousands of Ethereum nodes throughout the world, maintained by companies or enthusiasts for the purposes of validating transactions. Each of these nodes verifies every block that a miner creates.

It takes just a second for nodes on the Ethereum network to verify that the hash value is correct. If it isn’t, they reject the miner’s block.

If the miner finds a hash that matches the current target, the miner unlocks the ether and broadcasts the block across the network for each node to validate and add to their own copy of the ledger. If miner A finds the hash, miner B will stop work on the current block and start the computational process over again for the next block.

Ethereum's shift to proof-of-stake

Ethereum might not need miners forever, though.

Ethereum developers have long planned to drop mining in favor of a different method of verifying transactions called proof-of-stake, which helps the network reach consensus about whether transactions are valid in a different way. The hope is that proof-of-stake would require less electricity than proof-of-work, making it a greener alternative.
The shift to proof-of-stake is part of the ongoing Ethereum 2.0 upgrade to Ethereum, but it will take time to implement. However, some blockchain experts are skeptical proof-of-stake can work and will be as resistant to attacks as proof-of-work.

Ethereum mining FAQ

Is Ethereum mining profitable?

The answer is complex. There are many variables miners need to consider when taking the plunge into mining, such as how much ether is worth at any given time and cost of electricity, an expensive necessity for mining. Not to mention, the cost of electricity varies across the globe.

To be profitable, most Ethereum miners join mining pools – groups of miners – which give miners a better chance of winning ether.Another pressing factor is that when the Ethereum 2.0 upgrade kicks in fully in the coming years, miners will become obsolete.

How decentralized is Ethereum mining?

Much of the Ethereum mining power is concentrated in the hands of just a few mining pools. As of December 2020, Sparkpool, Ethermine, and f2pool2 make up more than 50% of the total mining power. The situation is similar for Bitcoin and other popular cryptocurrencies.

How do you mine Ethereum?

In short: Buy the equipment that is powerful enough and join a mining pool. Our guide goes into more detail.

Is Ethereum mining different from Bitcoin's?

The specific algorithm that ethereum uses is called “ethash,” designed to require more memory to make it harder to mine using expensive ASICs – specialized mining chips that are now the only profitable way of mining bitcoin. Despite this effort, Ethereum ASICs do exist.

Authored by Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 08

Can Ethereum Scale?

Mar 30, 2017 at 9:15 p.m.
Dec 30, 2020 at 9:00 p.m.

"Scalability" is one of the toughest problems for cryptocurrencies, including the second-largest by market cap, Ethereum. In short, developers and enthusiasts want the cryptocurrency to support as many users as it can. Right now it can't support very many – just a few transactions per second, which isn't very much compared to Visa, Facebook and other apps Ethereum's developers hope the cryptocurrency will ultimately compete with.

Ethereum is a cryptocurrency platform that uses smart contracts – rules that execute automatically exactly as written. Ethereum advocates hope the platform will give users more control over their online data. With traditional apps and services, the platform owners have a window into much of what their users do online. For example, Gmail has a copy of all of its users' emails, and Twitter habitually bans accounts that don't follow its rules. Ethereum is a platform for building applications similar to the apps we use today, but without centralized control.

Providing a decentralized alternative to tech platforms has challenges. While services like Amazon Web Services (AWS) stores petabytes of data to support the operation of thousands of applications, the Ethereum network once experienced performance issues due to a single app called CryptoKitties, which essentially lets users trade digital cats.

That's because blockchains like Ethereum are fundamentally different from server-based models; they're highly specialized peer-to-peer networks that require thousands of volunteers from around the world to store a copy of the entire transaction history of the network. This is a big task – one traditional apps don't have to contend with.

Ethereum manages this issue partly by requiring apps that run on the network to expend Ethereum tokens, called ether, to perform tasks. These transaction fees, sometimes called "gas," are set by Ethereum miners and vary directly with activity on the network. When many Ethereum-backed cryptocurrencies spiked in popularity in the summer of 2020, the corresponding fees rose greatly.

Why is scaling Ethereum so difficult?

Instead of having a central authority, Ethereum depends on a network of volunteers running "nodes," each of which stores the entire transaction history and the current "state," consisting of all of the account balances, contracts, and storage. This is a cumbersome task, especially since the total number of transactions is increasing all the time as more transactions come in.

To make sure the network is decentralized, it should be as easy as possible for as many people as possible to run these nodes. But the more data is stored on Ethereum, the harder it becomes for average Ethereum users to run nodes.

So if, say, Ethereum's developers decided to allow users to post unlimited data to the platform, each node would balloon to a size that the average enthusiast wouldn't be able to accomodate. Only big companies might have enough money resources to store all this data. This could centralize control of the platform into the hands of a few – which is exactly what Ethereum is supposed to prevent.

This limitation of Ethereum and other blockchain systems has long been discussed by developers and academics. Researchers have been exploring technologies for getting around the limitation for years, some of which will fall into the coming upgrade, Ethereum 2.0, which officially began rolling out on Dec. 1, 2020. Ethereum's top developers say changes will gradually be phased in over the coming years.

The big caveat is that no one knows ahead of time how successful these upgrades will be, nor how many people the system will successfully support once the series of upgrades are in place. The upgrade has its fair share of skeptics.

Here are the most-discussed scaling techniques in the Ethereum pipeline.

Ethereum rollups

Rollups are expected to be the Ethereum scalability technique to arrive in the short term. Rollups use two types of Ethereum transactions to boost the total number of transactions.

There are two types of Ethereum transactions:

- **On-chain transactions**: A limited, expensive type of transaction. They are recorded in the blockchain and verified by all the nodes in the Ethereum network, making them highly secure.
- **Off-chain transactions**: Are not recorded in the Ethereum blockchain, but are tied to it nonetheless, so that the type of transactions makes many of the same security guarantees.

Rollups make it possible for a single on-chain transaction to handle a series of secure off-chain transactions. The on-chain transaction "rolls up" the off-chain transactions, so to speak, using the on-chain transactions more efficiently.

There are two types of rollups:

- **Zk-rollups**: These use zero-knowledge proofs, a relatively new cryptographic technique used to prove that some information exists, without revealing what the information is.
- **Optimistic rollups**: These rollups rely on financial incentives for their security instead of cryptography. Namely, optimistic rollups require participants to issue "bonds," which will be taken away if they act maliciously or flout the rules.

Rollups are seen as a short-term way to push Ethereum scaling to new heights, and are expected to be rolled out over the next couple of years. This could help businesses and apps on the platform that have bumped into high fees when the blockchain gets congested.

In 2020, Ethereum creator Vitalik Buterin published a roadmap with rollups at the center.

Sharding Ethereum

Sharding could provide more dramatic scalability.

As mentioned before, right now each Ethereum node needs to store the state of each and every account on the network. Sharding would change that by drawing from a time-honored computer scaling technique called "database sharding," which breaks a database into more manageable pieces.

The goal of sharding is to move away from requiring users to run "full" nodes – those which store the full state of the network and every transaction that occurs. Instead, each node stores a fraction of this data and only verifies those transactions.

If a node needs to know about transactions or blocks that it doesn't store, then it finds a node that stores the information it needs. This is where things start to get tricky. The problem Ethereum developers have faced here is that the process isn't trustless – a defining characteristic of blockchains — since, in this model, nodes need to rely on other nodes.

Ethereum developers are looking to solve this problem using "cryptoeconomic incentives" that drive users of a system to act a certain way – in this case, ensuring that nodes are passing on valid information to other nodes.

New types of Ethereum transactions

Another capacity-expanding technology borrows from Bitcoin's Lightning Network, a proposed top-layer upgrade to Bitcoin that is meant to address its own scaling issues. Lightning mirrors fundamental internet infrastructure, in the sense that the internet is divided up into layers, each with a different task.

According to this vision, most transactions will be made on off-chain micropayment channels, lifting the burden from the underlying blockchain.

Plasma, TrueBit, and Raiden are a few examples of this technology. But they each have a different goal in mind. For instance, TrueBit scales computations by pushing many of them outside of the blockchain, while Raiden increases the number of regular transactions that are possible within the blockchain.

The reason these techniques would work, in theory, is that either party can kick the transaction back to the blockchain anytime they want, giving both parties the ability to end the interaction.

Ethereum scaling FAQs

Why do people run Ethereum nodes in the first place?

Despite the inconvenience of setting up a node, running one provides a user with boosted security and privacy. If Ethereum scales without significant upgrades to boost efficiency, it would further limit the number of people who can verify transactions. In addition, some argue it's good for the broader Ethereum network. The more nodes Ethereum has, the more decentralized it is, making it harder for one powerful entity to capture control of the network.

What happens if Ethereum nodes have to store ever-greater amounts of data?

The worry is that, if developers raise the size of each block to fit more transactions, the data that a node will need to store will grow larger – effectively kicking people off the network. If each node grows large enough, only a few large companies will have the resources to run them.

In other words, decentralization and scalability are currently at odds, but developers are hunting for ways around this.

How long will it take for Ethereum to scale?

This is unknown. There's still a lot of experimentation happening on the scaling front.

In sum, although Ethereum currently can only handle a handful of transactions per second, its architects have high hopes for the future. In creator Vitalik Buterin’s words, the long-term goal is for the platform to be able to process transactions at “Visa-scale transaction levels” or beyond.

Why does Ethereum sometimes have higher fees?

There’s a limit to how many ether transactions can be sent at once. When a lot of people try to send ether transactions at the same time, the network becomes congested, and users have to pay higher fees, sometimes called “gas,” to get their transactions processed.

Authored by Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 09

How to Mine Ethereum

Mar 30, 2017 at 9:11 p.m.
Jan 7, 2021 at 8:44 p.m.

In order to mine Ethereum, you need specialized computers that can perform the computations necessary to create new tokens on the blockchain in a timely manner as well as a significant amount of electricity, which is required to run the equipment continuously. All of this adds up to significant upfront costs.

Mining is the "glue" that holds together many cryptocurrencies, including Ethereum, by ensuring that the network comes to consensus on each and every change made in the system. Ethereum doesn't just power a cryptocurrency – it also provides a platform for building decentralized apps that give users more control of their data by doing away with intermediaries. Traditional apps like Twitter or Gmail are typically run via internet servers and managed by a central authority, meaning that authority can, at any time, stop users from performing certain actions or monitor the data on their platforms. Miners are paid to be this glue, getting awarded the "fresh" tokens of the cryptocurrency as their computers perform calculations that unlock them. That's why most people take up the venture in the first place.

Miners set computers loose to grind through cryptographic computations in an attempt to win ether, Ethereum's native token. They need to try a huge number of computational problems until one unlocks a new batch of the asset.

In theory, anyone can set their computers to focus on these cryptographic puzzles as a way to win rewards. The catch is that mining on major public blockchains tends to require more and more power over time. As more people invest in more powerful hardware to mine cryptocurrency, the calculations get harder. Miners using regular computers are very, very unlikely to win.

Choosing mining hardware

Before getting started, you will need special computer hardware to dedicate full-time to mining.

There are three types of mining hardware:

- CPUs
- GPUs: Faster than CPUs
- ASICs: Even faster and more powerful than GPUs

GPUs and ASICs boast a higher hashrate, meaning they can guess puzzle answers more quickly. At time of writing, GPUs and ASICs are now the only cost-effective option for ether miners. CPUs aren't powerful enough anymore.

Settling up a GPU is a complex task and you can browse plenty of advice about which ones are the most profitable based on how many hashes the GPU can compute per second, power consumption and the initial expense of the card.

You probably want to set up a mining rig, a machine that might be composed of multiple GPUs and can take a week to build.Online mining profitability calculators, such as the one offered by Etherscan, give some insight into the likely amount of ether you'll earn at a given hashrate, and whether that ether is enough – when cutting out the costs of setup and electricity – to make a profit.

Installing Ethereum software

After selecting some mining hardware, the next step is to install the mining software.

Miners need to install an Ethereum client to connect to the wider Ethereum network. An internet connection is vital for miners. Without an internet connection, the node won't be able to do much of anything.

Programmers familiar with the command line can install Geth, software that runs an Ethereum node written in the scripting language Go, or any of the other Ethereum clients, like Parity or OpenEthereum.
Download Geth here, using the directions for your appropriate operating system (Windows, Mac OS, or Linux), unzip it, and run it.
Once installed, your node can then connect to the Ethereum network where it can then "talk" to other nodes, to catch wind of the latest transactions and blocks. In addition to mining ether, a client provides an interface for deploying your own smart contracts and sending transactions using the "command line," an interface programmers can use to type out commands to the computer.

Install Ethereum mining software

Aspiring miners then need to install the official mining software, Ethminer.

Find the download for the appropriate version of Windows here, or GPU mining instructions for other operating systems here.
Once installed, your node will officially play a part in securing the Ethereum network. For more detailed instructions on any of the above, visit the official ethereum website.

Joining a mining pool

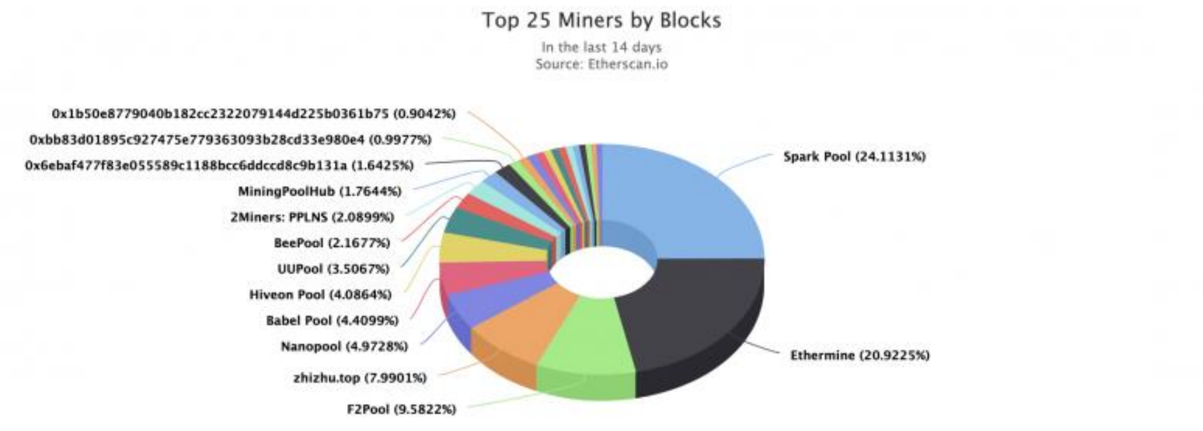
As a miner, you're unlikely to be able to mine ether on your own.

That's why miners "pool" together their computational power into "mining pools," to improve their chances of solving the cryptographic puzzles and earning ether. Then, they split the profits proportional to how much power each miner contributed.

There are many factors involved in joining a mining pool. Each pool might not be around forever, and the computational power of each pool is constantly changing, so there are a number of factors that go into deciding which to join.

One point to keep in mind is that mining pools have different payout structures. And pools charge mining fees.
Today the most popular mining pools are:

- Ethermine
- F2Pool
- Sparkpool
- Nanopool



The distribution of Ethereum mining pools as of Jan. 7, 2021.*(Etherscan.io)*

Mining pools generally have a signup process on their website so miners can connect to the pool and begin mining.

Find cheap electricity

The other biggest mining cost is electricity. Many profitable miners scout for electricity discounts, either by moving to regions around the world with less expensive electricity or by tapping renewable energy sources.

Ethereum Mining FAQs

Is Ethereum mining profitable?

The answer is complex. There are many variables miners need to consider when taking the plunge into mining, such as how much ether is worth at a given time and cost of electricity, an expensive necessity for mining. The cost of electricity varies across the globe.

How could the Ethereum upgrade 'ProgPoW' impact mining?

ProgPoW is a proposed Ethereum upgrade that, if implemented, would hamstring the most powerful miners. The motive for doing so is to keep the network decentralized by trying to ensure that no one in the network gets too much power.
In short, miners using ASICs (hardware even more powerful for mining than GPUs – see above) are the ones that would be affected. Their ASICs, which miners likely paid a premium for, would no longer be able to be used to mine ether.

How will Ethereum 2.0 upgrade impact mining?

The upgrade Ethereum 2.0 started roll out on Dec. 1, 2020, and will be iterated upon over the next several years.

The upgrade will impact mining even more drastically than ProgPoW. Once Ethereum 2.0 is fully rolled out, the goal is to eradicate miners completely, paving the way for a more energy-efficient method of maintaining the integrity of the Ethereum blockchain.

How do I keep abreast of Ethereum events that could impact mining?

The mining world is a whirlwind of change. The tools that you pick up today might be obsolete next year. Some mining pools might fall away while others emerge.

As a miner it’s worth keeping aware of industry shifts by keeping tabs on the latest mining news as well as Ethereum protocol upgrades.

By Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 10

What Is Ether?

Mar 30, 2017 at 9:08 p.m.
Feb 5, 2021 at 8:36 p.m.

Ether (ETH) is the main token of the Ethereum blockchain and the world's second-largest cryptocurrency by market capitalization. Just like the largest cryptocurrency, bitcoin, ether can be used to send payments directly to another person without the need for an intermediary.

The long-term vision for Ethereum is to power more than just financial transactions. Software developers are able to build applications on Ethereum, ranging from decentralized platforms for lending money to social media networks.

For any Ethereum-based app, ether acts as the primary "fuel." Any activity on the blockchain requires an amount of ether to power it, also known as "gas."

In Ethereum, ether can be used for the following things:

- **Payments:** Like bitcoin, ether can be used for payments. Users can send ether to another user and, just like cash, the payment doesn't require a third party to process or approve it.
- **Powering decentralized applications**: Ether is required in order to use decentralized apps (dapps) built on Ethereum, from staking ERC-20 tokens for yield farming to completing functions such as governance voting.
- **Transactions fees:** Every Ethereum action – from payments to using dapps – requires a fee.

Ethereum FAQs

How do I use ether?

First, users need to decide on which ether wallet they plan to store their funds in. Ether can be bought with fiat currencies like the U.S dollar or other cryptocurrency base pairs on a range of different exchanges.

Our guide on how to use Ethereum dives into this in much more detail.

Why are there ether fees?

Every time users send funds to and from a dapp or transfers any ERC20 coin between wallets they must pay a fee to do so. This is because Ethereum currently uses miners to validate transactions on the network. These miners use their specialized hardware to add new transactions to the blockchain. An auction-style system determines how miners choose which transactions to process first. The higher the fee attached to a transaction, the higher up on the miner's list it goes to be added. This incentivizes the miner to continue operating on the network and helps to cover its ongoing running costs.

Why do fees fluctuate so much in price?

Fees on the Ethereum network are not fixed, but in the future they will become more stable once EIP 1559 rolls out. These ether fees occasionally spike because of Ethereum's scalability problems. There is limited space in the Ethereum blockchain. When the network is congested, fees increase in cost as users compete to get their transaction processed ahead of everyone else's transactions. The network can get congested when there's a sharp change in Ethereum's price or when there's a spike in activity on dapps.

What is Ethereum gas?

Ethereum transaction fees are calculated based on how much "gas" the action requires.

Each action costs an amount of gas based on the computational power required and how long it takes to run. A transaction costs 500 gas, for example, which is paid in ether.

In this way, ether has sometimes been called "digital oil" because it's used to pay for a certain amount of mileage, so to speak.

How is ether used to power a dapp?

Ether works like fuel for dapps on the network. Say you're using an Ethereum-based notebook dapp that allows you to write immutable to-do lists that are saved on the blockchain. To post a note, a user might need to pay a transaction fee in ether to add a new list to the notebook.

Dapps each enable this in a different way. When a user goes to post a note, for instance, the notebook app might prompt the user to send the fee. Metamask, an ERC20 wallet built into browsers, can be helpful for this because it sits in the corner of the browser and can automatically understand when to help with sending transactions.

How is ether different from Ethereum?

Ethereum is the entire network. Ether is the main token that runs on it, making it a crucial part of Ethereum.

How many ether are there?

There are currently more than 113,000,000 ether, according to data provider Messari.
Five ether are created roughly every 12 seconds. But beyond that, the rules for ether's economy are open-ended and frequently change as new improvement proposals are agreed upon by the Ethereum developer community. While bitcoin has a hard cap of 21 million bitcoins, Ethereum's main token does not have a set max supply limit.

How many Ethereum tokens were created initially?

Sixty million tokens were purchased by users in Ethereum's initial 2014 crowdfunding campaign. Another 12 million went to the Ethereum Foundation, which is a group of researchers and developers that works on improving the underlying technology.

By Alyssa Hertig

DISCLOSURE

The leader in news and information on cryptocurrency, digital assets and the future of money, CoinDesk is a media outlet that strives for the highest journalistic standards and abides by a strict set of editorial policies. CoinDesk is an independent operating subsidiary of Digital Currency Group, which invests in cryptocurrencies and blockchain startups.

Chapter 11

Who Created Ethereum?

Mar 30, 2017 at 9:10 p.m.
Feb 5, 2021 at 10:37 p.m.

Vitalik Buterin

Vitalik Buterin, a Russian-Canadian entrepreneur and programmer from Toronto, first envisioned Ethereum when he was 19-years-old.

In 2011, the year Buterin first grew interested in Bitcoin, Buterin co-founded the online news website Bitcoin Magazine, writing hundreds of articles on the cryptocurrency world. He went on to code for the privacy-minded Dark Wallet and the marketplace Egora.
Along this journey, he came up with the idea of Ethereum, a platform inspired by Bitcoin, but that could go beyond the financial use cases.
He released a white paper in 2013 describing an alternative platform that would allow developers to create their own decentralized applications using a built-in programming language. Many developers were drawn to this idea because these new applications would be accessible to a global audience, highly secure, and much faster to build because there are no intermediary services to integrate.
To accomplish this, Ethereum makes it easy to create smart contracts, code that automatically creates an outcome when certain conditions are met. For his work, Buterin was also named a 2014 Thiel fellow, winning a $100,000 grant to work on Ethereum.

FAQs

Who helped Buterin create Ethereum?

After Buterin unveiled the Ethereum white paper, several other developers joined the ranks including CEO of IOG Charles Hoskinson, Decentral CEO Anthony Di Iorio and Akasha Founder Mihai Alisie. Buterin also introduced two new members to the team:

- Co-founder Dr. Gavin Wood did much of the early programming and architecting of the platform. He wrote the Ethereum yellow paper, the "technical bible" that outlines the specification for the Ethereum Virtual Machine (EVM), which is responsible for handling the state of the ledger and runs smart contracts.
- Co-founder Joseph Lubin went on to found the Brooklyn-based ConsenSys, a startup that focuses on building decentralized apps.

How much money does Buterin have?

Since Ethereum data and transaction information is public, users can track how much money Buterin has stored in ether, Ethereum's native token.
Buterin's main address is this one, which shows that he owns 333,348 ether, worth approximately $405million at the time this article was published.

What was Ethereum like in its early days?

To get the project off the ground, Buterin and the other founders launched a crowdfunding campaign in July 2014 where participants purchased ether, the Ethereum tokens that function as shares in the project.

Raising more than $18m, it was the most successful crowdsale at that time. It took another year, but the first live release, Frontier, launched on 30th July, 2015. It wasn't a particularly attractive platform, but the command line interface offered developers a platform for creating their own decentralized apps.
The smart contract platform took off, swelling into today's ecosystem of hundreds of developers and even drawing the attention of tech giants like IBM and Microsoft.
The funds from Ethereum's initial $18m crowd sale and project development are now managed by the Ethereum Foundation, a non-profit entity based in Zug, Switzerland.