The World Computer
INTRODUCTION TO ETHEREUM

Ether is the second-largest cryptocurrency by market capitalization, behind bitcoin. Its current market capitalization stands at $290.69 billion, representing approximately 14% of the total cryptocurrency market.[1]

Imagined in 2013 and created in 2015, the blockchain network Ethereum has grown in innovation and utility. Different from bitcoin's primary function as a peer-to-peer electronic cash system, Ethereum has invented a new world of peer-to-peer applications.

Before we dive into details, it's important to distinguish ether from Ethereum. **Ether** refers to the cryptocurrency used on the Ethereum blockchain. **Ethereum** refers to the blockchain network.

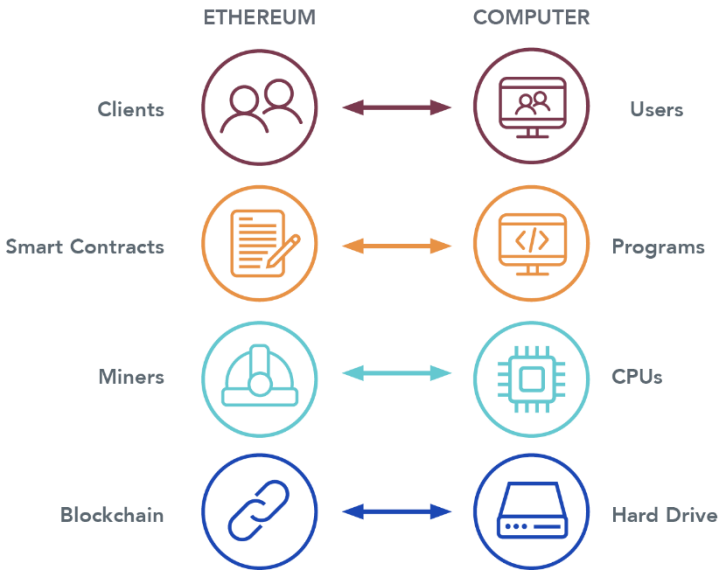
What's Ethereum?

Ethereum is a blockchain platform that handles programs and applications without relying on a centralized party. It is "the world's programmable blockchain."[2]

The platform is built on the public, open-sourced, decentralized and cryptographic blockchain technology. It powers decentralized applications (**dApps**) that are supported by a transaction protocol called **smart contract**.

With its collective computing power on the distributed network (the **Ethereum Virtual Machine**), it executes peer-to-peer transactions to realize automatic, conditional transfers of value and information, including money, voting rights and property.

Ethereum can be compared to a "world computer" on a blockchain, where the underlying blockchain technology is the virtual machine's hard drive, smart contracts are programs, miners are CPUs and users pay with ether to use this "computer".



[1] As of 4/15/21

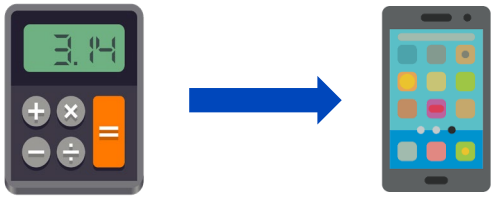
[2] https://ethereum.org/en/what-is-ethereum

WISDOMTREE®

Solving the Problem

Ethereum's invention was inspired by bitcoin.

Bitcoin established the foundation for decentralized blockchain technology. But its functionality is limited to peer-to-peer electronic cash transfers. Ethereum expands bitcoin's functionality to programmable apps. Essentially, it aims to create a decentralized computer network to run various applications. To borrow the metaphor of its founder, Vitalik Buterin: Bitcoin is like a calculator, but Ethereum wants to become a smart phone running many applications.[3]



This decentralized network would automate decisions and transactions, thus reducing the need for a trusted central party. It can lower the need for intermediaries, prevent fraud and minimize accidental incidents.

How Does Ethereum Work?

Smart Contracts

At the core of Ethereum are smart contracts.

Smart contracts are one of the two types of Ethereum accounts in which a set of instructions is programmed to tell the system what to do. Nick Szabo, developer of the concept, often compared it to the codes behind vending machines.

A smart contract is executed when triggered by a transaction. In the example of a vending machine, the transaction is when a user inserts a coin. Once the smart contract is triggered, actions are executed based on the "if…then…" conditions embedded in the smart contract code.

For example, by pressing a combination of buttons on a vending machine, a bottle of water is dropped. The specific good that gets dropped in the vending machine is the outcome of the smart contract. On the Ethereum network, that could be either a value transfer of ether to another account or a transaction to trigger another smart contract.

A smart contract abides by a pre-defined set of rules that allows it to automatically execute code the same way on any Ethereum node on the network. This eliminates the need for a third party to carry out code execution on behalf of users, making the system decentralized. It empowers coders to create a wide range of applications layering together different smart contracts.

To provide a concrete example, consider Etherisc, a decentralized insurance application on the Ethereum network. Members can purchase insurance directly on the application with its native token. Then, a pool of money is established, aggregating insurance payments from all members. If a disaster hits and prescribed smart contract conditions are met, payouts are made to impacted members without the need to go through the traditional insurance industry's cumbersome reimbursement process. Crop insurance, for example, could automatically pay out money if drought or flood events are reported in the area by government agencies.

[3] Vitalik mentioned this metaphor during a speech he gave on 19/10/16, called "Ethereum in 25 Minutes."

Gas

Fees need to be paid in ether to miners in order to facilitate transactions and execute smart contracts. The fee that's charged is called **gas**. Gas price is often a small fraction of ether, which is denoted in the unit of Gwei (10^9 Gwei = 1 ether).

Gas is essential in sustaining the Ethereum network. It motivates miners to process and verify transactions for a monetary reward. The amount of gas needed in a transaction is roughly equivalent to the value of energy needed plus a small transaction fee. **Gas price** fluctuates with supply and demand for processing power since miners can choose to not process transactions when gas prices are low.

Gas has another important function in preventing unintentional waste of energy. Because the coding language for Ethereum is Turing-complete, there is the possibility of a program running indefinitely, and a transaction could be left consuming a lot of energy. A **gas limit** is imposed as the maximum price users are willing to pay to facilitate transactions. When gas runs out, the program is terminated and no additional energy is used.

Applications

Ethereum's applications take advantage of blockchain technology's decentralized and immutable nature. They can be created and contributed to by anyone, without tempering the system's security. Their functions range widely. Here are a few important examples:

- **Decentralized Finance (DeFi):** DeFi aims to build an open and global financial system that can be accessed by anyone with access to the Internet. Unlike the trust-based finance industry or FinTech, DeFi is trust-minimized, meaning that the system's operation does not rely on any single individual entity but is owned by users. This structure enables it to be accessible, on-demand, transparent, and potentially faster and cheaper. It connects peer-to-peer supply and demand, eliminating the need for intermediaries.

  DeFi's functionalities have grown to create a financial ecosystem since its launch. Now, users can borrow, lend, invest, trade, earn interest, buy insurance and transfer money like they would in the traditional financial system.

- **Decentralized Autonomous Organization (DAO):** A DAO refers to an organization without a third party that is established for a common purpose. This organization operates and collaborates through a shared, defined and automated protocol to ensure all group members' voices are heard and the decision-making process is transparent. Each DAO has an embedded treasury in which the funds are stored, and the funds are spent according to decisions made by members' voting.

  One of the examples of DAO is a decentralized venture capital fund named "The DAO" launched in 2016. Members could purchase DAO tokens to gain rights to vote on investment proposals. If the voted project became profitable, members would be given a return according to their stakes. Although the DAO was an innovative idea, it failed due to a bug that existed in its smart contract code. Hackers stole a portion of the organization's funds. This event resulted in a decision to implement a hard fork on the Ethereum network, creating a branch called Ethereum Classic. Other examples of a DAO have continued to operate successfully. MakerDAO enables the continued generation of Dai, a decentralized stablecoin.

- **Non-fungible Tokens (NFT):** NFTs are records of data on the blockchain, which make the underlying assets immutable and differentiated. They range from digital assets such as photos, audios, videos, shares and certificates to physical assets such as properties and paintings.

  Since digital files are easy to replicate, having NFTs that prove ownership of the digital files is important. When an NFT is bought, the owner gains an unchangeable ownership record. The appeal of NFTs for digital assets lies in the sense of rarity it creates, thereby improving the asset's collectable value. For artists selling the assets, NFTs allow more direct distribution of their work without a third-party platform, which can better protect their copyrights and increase their profits.

  For NFTs backed by real physical assets, tokenization proves digital ownership of the item and preserves the uniqueness of the item. Although the market of physical asset NFTs is not as developed as the market for digital assets, there are a lot of possibilities in putting tokenized assets into use. These could include facilitating selling and buying NFTs and using them as collateral to borrow funds.

Nyan Cat GIF created by Chris Torres was sold for 300 ethers (~$600,000) on 2/19/21.

Where Is Ethereum going?

The idea of Ethereum was proposed in 2013. On July 30, 2015, the first version of Ethereum was released, called "Frontier." There are four main stages of Ethereum's development:

- Frontier (July 2015–March 2016)
- Homestead (March 2016–October 2017)
- Metropolis (October 2017–December 2019)
- Serenity (December 2019–2022)

Source: WisdomTree, CoinDesk. as of 4/15/2021.

Currently, we are at the still-developing **Serenity** stage, which is also known as **Ethereum 2.0**. This version aims to solve two main challenges Ethereum is facing: a clogged network that can only handle a limited number of transactions per second (with increased gas fees for faster transactions), and the large consumption of energy that comes with the proof-of-work mechanism.[4]

Two of the major upgrades include the shift from proof-of-work to proof-of-stake, and the implementation of shard chains that would spread the workload of the network.[5] Ethereum 2.0 is envisioned to be more scalable, secure and sustainable, although when (or if) it will ultimately be implemented, and other potential issues, remain unclear.

[4] Proof-of-work is a consensus mechanism that is used to verify the validity of blockchain transactions, through solving of computationally intensive puzzles using miners' computers' processing power.

[5] Proof-of-stake is another consensus mechanism used to verify blockchain transactions. However, it does so by using miners' existing coins as a stake in the validation process, which demands less computer processing power.

Comparison vs. Bitcoin

Since Ethereum is inspired by bitcoin's blockchain framework, the two share in the general attributes of blockchain technology and thus are decentralized, public and immutable.

But there are some main differences between Ethereum and bitcoin.

	Bitcoin	Ethereum
Live Inception	January 2009	July 2015
Use Case	Peer-to-peer electronic cash system, focusing on the use of cryptocurrency	Blockchain platform, focusing on building dApps
Functionalities	Record keeping	Record keeping + code execution
Coding Language	Bitcoin Script is less coder-friendly, not Turing-complete	Solidity is the primary language. It is more coder-friendly and Turing-complete
Hashing Algorithm	SHA-256	Ethash
Block Time	10 minutes	10-19 seconds
Total Supply Cap	21 million	No cap

In summary, bitcoin's system is more defined and rigid because of its focus on the use case of cryptocurrency. Ethereum's system is more flexible, accessible and ever-evolving, as its development relies heavily on participation to build an expansive network of applications.

Conclusion

A decentralized application platform—Ethereum—might sound like an idea from science fiction. Yet it is already a blooming ecosystem. There are currently 148 million unique addresses receiving and sending transactions, 6,867 computer nodes connecting to the Ethereum network, an average of 1.3 million transactions are executed per day and more than 3,500 dApps are available.[6]

Ethereum offers an exciting opportunity to disrupt traditional industries by removing intermediaries and maximizing efficiency. Its innovation and execution bode a strong potential to make a huge impact in the real world.

[6] According to https://etherscan.io, www.ethernodes.org, https://www.stateofthedapps.com/rankings/platform/ethereum, as of 4/16/21.

Important Information

This material is for informational purposes only and contains the opinions of the author, which are subject to change, and should not be considered or interpreted as a recommendation to participate in any particular trading strategy or deemed to be an offer or sale of any investment product, and it should not be relied on as such. This material is not intended to provide investment recommendations and is not an official statement of WisdomTree. This material represents an assessment of the environment discussed at a specific time and is not intended to be a forecast of future events or a guarantee of future results. Readers of this information should consult their own financial advisor, lawyer, accountant, or other advisor before making any financial decision.

There are risks associated with investing, including the possible loss of principal. Crypto assets, such as bitcoin and ether, are complex, generally exhibit extreme price volatility and unpredictability, could become illiquid at any time, should be viewed as highly speculative assets, may not be an appropriate or prudent diversifier in all portfolios and may result in an entire loss of investment. Crypto assets are frequently referred to as crypto "currencies," but they typically operate without central authority or banks, are not backed by any government or issuing entity (i.e., no right of recourse), have no government or insurance protections, are not legal tender and have limited or no usability as compared to fiat currencies. Federal, state or foreign governments may restrict the use, transfer, exchange and value of crypto assets, and regulation in the U.S. and worldwide is still developing. Crypto asset exchanges and/or settlement facilities may stop operating, permanently shut down or experience issues due to security breaches, fraud, insolvency, market manipulation, market surveillance, KYC/AML (know your customer / Anti-Money Laundering) procedures, non-compliance with applicable rules and regulations, technical glitches, hackers, malware or other reasons, which could negatively impact the price of any cryptocurrency traded on such exchanges or reliant on a settlement facility or otherwise may prevent access or use of the crypto asset. Crypto assets can experience unique events, such as forks or airdrops, which can impact the value and functionality of the crypto asset. Crypto asset transactions are generally irreversible, which means that a crypto asset may be unrecoverable in instances where: (i) it is sent to an incorrect address, (ii) the incorrect amount is sent, or (iii) transactions are made fraudulently from an account. A crypto asset may decline in popularity, acceptance or use, thereby impairing its price, and the price of a crypto asset may also be impacted by the transactions of a small number of holders of such crypto asset. Crypto assets may be difficult to value and valuations, even for the same crypto asset, may differ significantly by pricing source or otherwise be suspect due to market fragmentation, illiquidity, volatility and the potential for manipulation. Crypto assets generally rely on blockchain technology and blockchain technology is a relatively new and untested technology which operates as a distributed ledger. Blockchain systems could be subject to internet connectivity disruptions, consensus failures or cybersecurity attacks, and the date or time that you initiate a transaction may be different then when it is recorded on the blockchain. Access to a given blockchain requires an individualized key, which, if compromised, could result in loss due to theft, destruction or inaccessibility. In addition, different crypto assets exhibit different characteristics, use cases and risk profiles. Information provided by WisdomTree regarding digital assets, crypto assets or blockchain networks should not be considered or relied upon as investment or other advice, as a recommendation from WisdomTree, including regarding the use or suitability of any particular digital asset, crypto asset, blockchain network or any particular strategy. WisdomTree is not acting and has not agreed to act in an investment advisory, fiduciary or quasi-fiduciary capacity to any advisor, end client or investor, and has no responsibility in connection therewith, with respect to any digital assets, crypto assets or blockchain networks.

Market capitalization: Market cap = share prices x number of shares outstanding. Firms with the highest values receive the highest weights in approaches designed to weight firms by market cap. Cryptocurrency: a digital or virtual currency that is secured by cryptography, which makes it nearly impossible to counterfeit or double-spend. Blockchain: a distributed ledger system in which a record of transactions made in cryptocurrencies is maintained across computers linked in a peer-to-peer network.