

2023/2024 S2

Ethereum I

Dr. Hui Gong (h.gong1@westminster.ac.uk)

UNIVERSITY OF
WESTMINSTER 



What is Ethereum?

What Is Ethereum?

Compared to Bitcoin

Ethereum is often described as “the world computer.” But what does that mean?

*From a computer science perspective, **Ethereum is a deterministic but practically unbounded state machine**, consisting of a globally accessible singleton state and a virtual machine that applies changes to that state.*

*From a more practical perspective, **Ethereum is an open source, globally decentralized computing infrastructure that executes programs called smart contracts**. It uses a blockchain to synchronize and store the system’s state changes, along with a cryptocurrency called ether to meter and constrain execution resource costs.*

Ethereum’s purpose is not primarily to be a digital currency payment network. While the digital currency ether (ETH) is both integral to and necessary for the operation of Ethereum, ether is intended as a utility currency to pay for use of the Ethereum platform as the world computer.

Unlike Bitcoin, which has a very limited scripting language, Ethereum is designed to be a general-purpose programmable blockchain that runs a virtual machine capable of executing code of arbitrary and unbounded complexity. Where Bitcoin’s Script language is, intentionally, constrained to simple true/false evaluation of spending conditions, **Ethereum’s language is Turing complete**, meaning that Ethereum can straightforwardly function as a general-purpose computer.

What Is Ethereum?

The Birth of Ethereum

All great innovations solve real problems, and Ethereum is no exception. Ethereum was conceived at a time when people recognized the power of the Bitcoin model, and were trying to move beyond cryptocurrency applications. But developers faced a conundrum: they either needed to build on top of Bitcoin or start a new blockchain.

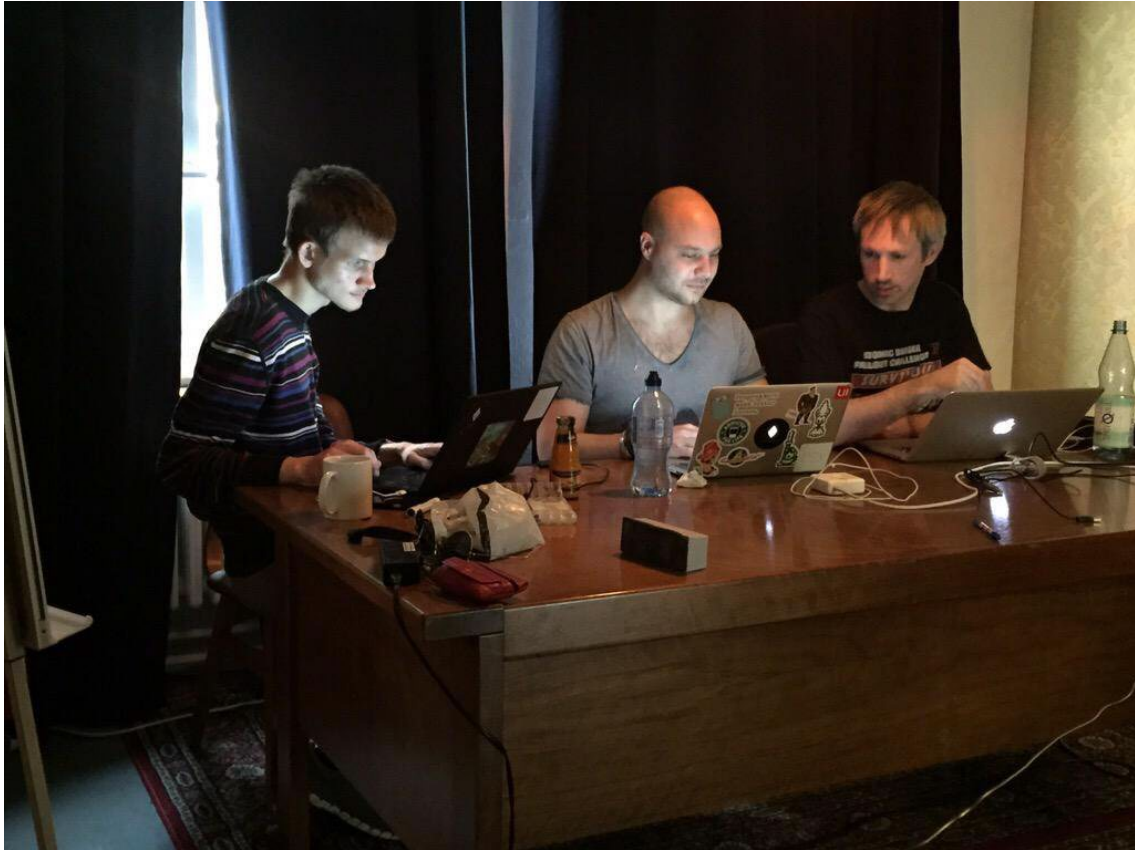
Toward the end of 2013, Vitalik Buterin, a young programmer and Bitcoin enthusiast, started thinking about further extending the capabilities of Bitcoin and Mastercoin (an overlay protocol that extended Bitcoin to offer rudimentary smart contracts). In October of that year, Vitalik proposed a more generalized approach to the Mastercoin team, one that allowed flexible and scriptable (but not Turing-complete) contracts to replace the specialized contract language of Mastercoin. While the Mastercoin team were impressed, this proposal was too radical a change to fit into their development roadmap.

In December 2013, Vitalik started sharing a whitepaper that outlined the idea behind Ethereum: a Turing-complete, general-purpose blockchain. A few dozen people saw this early draft and offered feedback, helping Vitalik evolve the proposal. Dr. Gavin Wood, however, was one of the first people to reach out to Vitalik and offer to help with his C++ programming skills. Gavin became Ethereum's cofounder, codesigner, and CTO. Much like Satoshi, Vitalik and Gavin didn't just invent a new technology; they combined new inventions with existing technologies in a novel way and delivered the prototype code to prove their ideas to the world.

The founders worked for years, building and refining the vision. And on July 30, 2015, the first Ethereum block was mined. The world's computer started serving the world.

What Is Ethereum?

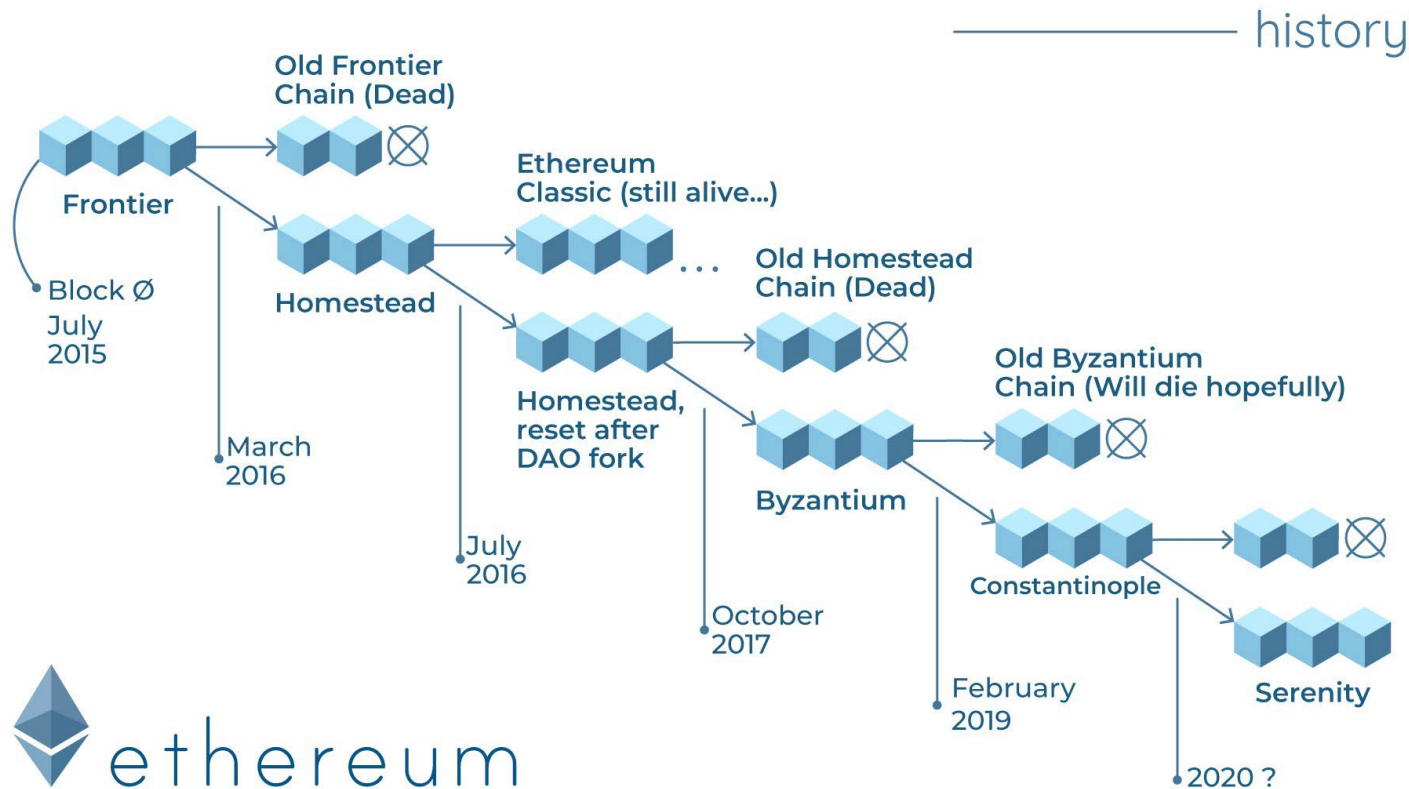
The Birth of Ethereum



Ethereum's founders were thinking about a blockchain without a specific purpose, that could support a broad variety of applications by being programmed. The idea was that by using a general-purpose blockchain like Ethereum, a developer could program their particular application without having to implement the underlying mechanisms of peer-to-peer networks, blockchains, consensus algorithms, etc. The Ethereum platform was designed to abstract these details and provide a deterministic and secure programming environment for decentralized blockchain applications.

What Is Ethereum?

Ethereum's Four Stages of Development



- Frontier-testing of a platform that would support decentralized apps and also smart contracts.
- Homestead-Ethereum Virtual Machine process formalization, ecosystem consolidation for the smart contract further development.
- Metropolis-Incoming problem solving-Ethereum will be available to large-scale applications and stronger performance for all users. Byzantium-Laying the foundation. Constantinople-Improving performance and setting timeline for next step serenity.
- **Serenity**-the goal for Ethereum is to eventually be self-sufficient while still maintaining the high-level security of the blockchain.

What Is Ethereum?

Ethereum 2.0

What is Ethereum 2.0?

Ethereum 2.0, also known as Eth2 or “Serenity”, is an upgrade to the Ethereum blockchain. The upgrade aims to enhance the speed, efficiency, and scalability of the Ethereum network so that it can process more transactions and ease bottlenecks.

Ethereum 2.0 is launching in several phases. The first stage in the release of Ethereum 2.0, went live at 12:00 pm UTC on December 1, 2020.

How does Ethereum 2.0 differ from Ethereum?

While Ethereum 1.0 uses a consensus mechanism known as proof of work (**PoW**), Ethereum 2.0 will use a proof of stake (**PoS**) mechanism.

How will Ethereum 2.0 scale better than Ethereum 1.0?

One of the main reasons for the upgrade to Ethereum 2.0 is scalability. With Ethereum 1.0, the network can only support around 30 transactions per second; this causes delays and congestion. Ethereum 2.0 promises up to 100,000 transactions per second. This increase will be achieved through the implementation of shard chains.

How will Ethereum 2.0 be more secure?

Ethereum 2.0 has been devised with security in mind. Most proof of stake networks have a small set of validators, which makes for a more centralized system and decreased network security. Ethereum 2.0 requires a minimum of 16,384 validators, making it much more decentralized - and hence, secure.

What Is Ethereum?

The Merge

The Merge is the most significant update to Ethereum since its launch in 2015. As crypto approaches an inflection point of mainstream adoption, hard questions have arisen about the sustainability, security and scalability of its leading networks.

Ethereum anticipated these concerns and from its early days viewed Proof of Stake as the mechanism to secure its future, but it has taken years to achieve a design that makes Ethereum's economic model more durable, its infrastructure more scalable, and its consensus engine more sustainable. In short, to ensure that when the world was ready to adopt web3, Ethereum would be ready to serve as its foundation.

The Merge represents the Ethereum network's shift to proof-of-stake (PoS), its new system (also called a "consensus mechanism") for authenticating crypto transactions. The new system will replace proof-of-work (PoW), the more power-hungry mechanism pioneered by Bitcoin.

Ethereum already has a PoS network called the Beacon Chain (introduced in 2020), but it is not yet used for processing transactions. For now, it's essentially just a staging area for computers operating the Ethereum network to prepare for the PoS upgrade.

Ethereum's full transition to PoS requires merging the Beacon Chain (called the "Consensus" layer) with Ethereum's PoW mainnet (the "Execution" layer).

What Is Ethereum?

The Merge Q&A

Will Ethereum fees decrease after the Merge?

No.

Ethereum transaction fees are not expected to change as a result of the Merge. Future network updates, like danksharding and proto-danksharding, may help to address Ethereum's high network fees, but these updates are not expected until 2023 at the earliest. The main salve for Ethereum's transaction fee woes remains rollups – third-party networks like Arbitrum and Optimism that bundle transactions and process them separately from Ethereum's mainnet.

Will Ethereum transaction speeds increase after the Merge?

Yes, but barely.

On average, Ethereum blocks are issued once every 13 or 14 seconds in today's proof-of-work (PoW) system. After the merge, proof-of-stake (PoS) blocks will be issued in regular 12-second intervals. This is not an improvement that most users will notice, and it still places Ethereum behind rival blockchain networks like Solana and Avalanche (though well ahead of Bitcoin, where a new block is mined every 10 minutes on average).

What Is Ethereum?

The Merge Q&A

Will the Merge increase the price of ether (ETH)?

It's hard to say.

With so many variables and unknowns, it is impossible to predict what will happen to Ethereum's token price as a result of the Merge.

The Ethereum community has for years positioned the Merge as a massive upgrade to the network's core technology. Along with addressing concerns about the network's environmental impact, PoS will introduce a new form of utility for Ethereum's native ether (ETH) token in the form of staking.

But the Merge is not guaranteed to boost the ETH price. The Merge will also introduce changes to the rate at which ether is issued and how it is distributed. These changes could be positive or negative depending upon whom you ask. There is also a risk (however small) that the Merge will fail, or that PoS will prove less secure than PoW.

When was the Merge happened?

Sept. 15, 2022.

What Is Ethereum?

The Merge Q&A

Can I become an Ethereum validator or staker?

Yes, if you have some ETH.

It is already possible to “stake” 32 ether and earn rewards for validating Ethereum’s PoS Beacon Chain. Staked ether will accrue network rewards, but it will be impossible to withdraw until an update expected around six to 12 months after the Merge.

Staking requires some know-how; if you screw up or go offline, your stake can be “slashed” (ie, reduced).

Those with less blockchain expertise can stake via centralized services like those offered by Coinbase (COIN) or Kraken. In addition to handling the technical nitty-gritty, these services – in exchange for a cut of users’ rewards – open up staking to those with less than 32 ETH.

Will Ethereum users or ETH holders need to take any action after the Merge?

No.

What Is Ethereum?

The Merge Q&A

What's on the Ethereum roadmap after the Merge?

After the Merge, Ethereum's core developers will continue working on the open-source network as they did before, with improvements to network fees, speeds and security slated for the months and years ahead.

One focus for developers post-Merge will be sharding, which aims to expand Ethereum's transaction throughput and decrease its fees by spreading network activity across several "shards" – almost like lanes on a highway. (Updates of this sort were initially slated to accompany the Merge – originally called "Ethereum 2.0," or "ETH2" – but were deprioritized with the success of third-party rollups at addressing some of the same problems).

What happens to proof-of-work miners after the Merge?

After the Merge, Ethereum miners – many of whom have invested in fancy mining-optimized computers – will be unable to mine new blocks on the network. Many miners will abandon mining and "stake" ether to earn rewards on the PoS network.

For those who wish to put their mining hardware to continued use, they'll need to move to another proof-of-work network, like Ethereum Classic.

After the Ethereum Merge, some miners also plan to create a "forked" version of the proof-of-work blockchain – basically, a clone of the blockchain that still runs using the old miner-friendly system. It is unclear whether these chains will gain enough traction to become lucrative for miners in the long term.

What Is Ethereum?

Ethereum and Turing Completeness

As soon as you start reading about Ethereum, you will immediately encounter the term “Turing complete.” Ethereum, they say, unlike Bitcoin, is Turing complete. What exactly does that mean?

The term refers to English mathematician Alan Turing, who is considered the father of computer science. In 1936 he created a mathematical model of a computer consisting of a state machine that manipulates symbols by reading and writing them on sequential memory (resembling an infinite-length paper tape). With this construct, Turing went on to provide a mathematical foundation to answer (in the negative) questions about universal computability, meaning whether all problems are solvable.

He proved that there are classes of problems that are uncomputable. Specifically, he proved that the halting problem (whether it is possible, given an arbitrary program and its input, to determine whether the program will eventually stop running) is not solvable.

Alan Turing further defined a system to be Turing complete if it can be used to simulate any Turing machine. Such a system is called a Universal Turing machine (UTM). Ethereum’s ability to execute a stored program, in a state machine called the Ethereum Virtual Machine, while reading and writing data to memory makes it a Turing complete system and therefore a UTM. Ethereum can compute any algorithm that can be computed by any Turing machine, given the limitations of finite memory.

Ethereum’s groundbreaking innovation is to combine the general-purpose computing architecture of a stored-program computer with a decentralized blockchain, thereby creating a distributed single-state (singleton) world computer. Ethereum programs run “everywhere,” yet produce a common state that is secured by the rules of consensus.

What Is Ethereum?

The Third Age of the Internet

Ethereum started as a way to make a general-purpose blockchain that could be programmed for a variety of uses. But very quickly, Ethereum's vision expanded to become a platform for programming DApps. DApps represent a broader perspective than smart contracts. A DApp is, at the very least, a smart contract and a web user interface. More broadly, a DApp is a web application that is built on top of open, decentralized, peer-to-peer infrastructure services.

A DApp is composed of at least:

- Smart contracts on a blockchain
- A web frontend user interface

In addition, many DApps include other decentralized components, such as:

- A decentralized (P2P) storage protocol and platform
- A decentralized (P2P) messaging protocol and platform

In 2004 the term “Web 2.0” came to prominence, describing an evolution of the web toward user-generated content, responsive interfaces, and interactivity. Web 2.0 is not a technical specification, but rather a term describing the new focus of web applications.

The concept of DApps is meant to take the World Wide Web to its next natural evolutionary stage, introducing decentralization with peer-to-peer protocols into every aspect of a web application. The term used to describe this evolution is web3, meaning the third “version” of the web. First proposed by Dr. Gavin Wood, web3 represents a new vision and focus for web applications: from centrally owned and managed applications, to applications built on decentralized protocols.

Ethereum Basics

Ethereum Basics

Ether Currency Units

Ethereum’s currency unit is called ether, identified also as “ETH” or with the symbols Ξ (from the Greek letter “Xi” that looks like a stylized capital E) or, less often, \blacklozenge : for example, 1 ether, or 1 ETH, or $\Xi 1$, or $\blacklozenge 1$.

Ether is subdivided into smaller units, down to the smallest unit possible, which is named wei. One ether is 1 quintillion wei ($1 * 10^{18}$ or 1,000,000,000,000,000,000). You may hear people refer to the currency “Ethereum” too, but this is a common beginner’s mistake. Ethereum is the system, ether is the currency.

The value of ether is always represented internally in Ethereum as an unsigned integer value denominated in wei. When you transact 1 ether, the transaction encodes 1000000000000000000 wei as the value.

Ether’s various denominations have both a scientific name using the International System of Units (SI).

Value (in wei)	Exponent	Common name	SI name
1	1	wei	Wei
1,000	10^3	Babbage	Kilowei or femtoether
1,000,000	10^6	Lovelace	Megawei or picoether
1,000,000,000	10^9	Shannon	Gigawei or nanoether
1,000,000,000,000	10^{12}	Szabo	Microether or micro
1,000,000,000,000,000	10^{15}	Finney	Milliether or milli
1,000,000,000,000,000,000	10^{18}	Ether	Ether
1,000,000,000,000,000,000,000	10^{21}	Grand	Kiloether
1,000,000,000,000,000,000,000,000	10^{24}		Megaether

Table shows the various units, their colloquial (common) names, and their SI names. In keeping with the internal representation of value, the table shows all denominations in wei (first row), with ether shown as 10^{18} wei in the 7th row.

Ethereum Basics

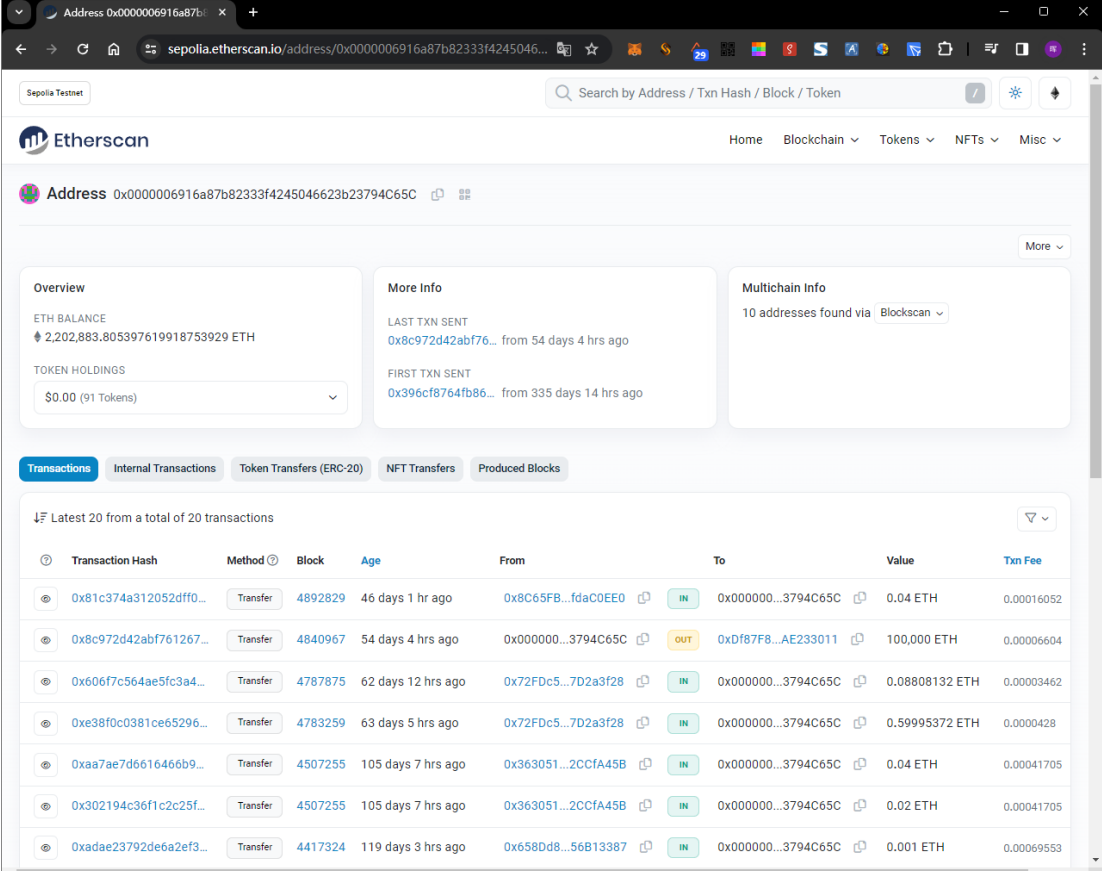
Exploring the Transaction History of an Address

By now you have become an expert in using MetaMask to send and receive test ether.

Your wallet has received at least two payments and sent at least one. You can view all these transactions using the ropsten.etherscan.io block explorer. You can either copy your wallet address and paste it into the block explorer's search box, or have Meta-Mask open the page for you. Next to your account icon in MetaMask, you will see a button showing three dots. Click on it to show a menu of account-related options.

Select **“View account on Etherscan”** to open a web page in the block explorer showing your account's transaction history.

You can explore the transaction history of any address. Take a look at the transaction history of the Sepolia Test Faucet address (hint: it is the “sender” address listed in the oldest payment to your address). You can see all the test ether sent from the faucet to you and to other addresses. Every transaction you see can lead you to more addresses and more transactions.



The screenshot shows the Etherscan Sepolia Testnet interface for the address 0x0000006916a87b8233f4245046623b23794c65c. The page displays the address's ETH balance (2,202,883.805397619918753929 ETH) and token holdings (\$0.00). It also shows the last and first transactions sent. The main section displays a list of transactions, including transfers from the faucet to the address and other addresses.

Transaction Hash	Method	Block	Age	From	To	Value	Txn Fee
0x81c374a312052dff0...	Transfer	4892829	46 days 1 hr ago	0x8C65FB...fdaC0EE0	0x000000...3794C65C	0.04 ETH	0.00016052
0x8c972d42abf761267...	Transfer	4840967	54 days 4 hrs ago	0x000000...3794C65C	0xDf87F8...AE233011	100,000 ETH	0.00006604
0x606f7c564ae5fc3a4...	Transfer	4787875	62 days 12 hrs ago	0x72FDc5...7D2a3f28	0x000000...3794C65C	0.08808132 ETH	0.00003462
0xe38f0c0381ce65296...	Transfer	4783259	63 days 5 hrs ago	0x72FDc5...7D2a3f28	0x000000...3794C65C	0.59995372 ETH	0.0000428
0xaa7ae7d6616466b9...	Transfer	4507255	105 days 7 hrs ago	0x363051...2CCfA45B	0x000000...3794C65C	0.04 ETH	0.00041705
0x302194c36f1c2c25f...	Transfer	4507255	105 days 7 hrs ago	0x363051...2CCfA45B	0x000000...3794C65C	0.02 ETH	0.00041705
0xadae23792de6a2ef3...	Transfer	4417324	119 days 3 hrs ago	0x658Dd8...56B13387	0x000000...3794C65C	0.001 ETH	0.00069553

Ethereum Basics

EVM and Accounts

Introducing the World Computer

You've now created a wallet and sent and received ether. So far, we've treated Ethereum as a cryptocurrency. But Ethereum is much, much more. In fact, **the cryptocurrency function is subservient to Ethereum's function as a decentralized world computer**. Ether is meant to be used to pay for running smart contracts, which are computer programs that run on an emulated computer called the Ethereum Virtual Machine (EVM).

The EVM is a global singleton, meaning that it operates as if it were a global, single instance computer, running everywhere. Each node on the Ethereum network runs a local copy of the EVM to validate contract execution, while the Ethereum blockchain records the changing state of this world computer as it processes transactions and smart contracts.

Externally Owned Accounts (EOAs) and Contracts

Externally owned accounts (EOAs)

An externally controlled account

- * has an ether balance,
- * can send transactions (ether transfer or trigger contract code),
- * is controlled by private keys,
- * has no associated code.

Contract accounts

A contract

- * has an ether balance,
- * has associated code,
- * code execution is triggered by transactions or messages (calls) received from other contracts.
- * when executed - perform operations of arbitrary complexity (Turing completeness) - manipulate its own persistent storage, i.e., can have its own permanent state - can call other contracts

References to read

- [1] Ethereum Whitepaper. <https://ethereum.org/en/whitepaper/>
- [2] Ethereum Yellowpaper. <https://ethereum.github.io/yellowpaper/paper.pdf>
- [3] Polkadot Whitepaper. <https://polkadot.network/PolkaDotPaper.pdf>