Published in HackerNoon.com

Mohit Mamoria Follow

Aug 14, 2017 · 9 min read ·

WTF is Ethereum?

The ultimate guide to understand why Ethereum is not just another cryptocurrency.

Although 'Bitcoin' and 'Ethereum' are terms that are often paired together, the reality is that they are vastly different. The only thing Ethereum shares with Bitcoin is that it's a cryptoasset running on top of blockchain.

Instead of being just a cryptocurrency, like Bitcoin, Ethereum also has features

blockchain, feel free to go directly to the next section.

> *By the way, I am curator of a weekly newsletter, Unmade, which delivers one idea from the future to your inboxes.*

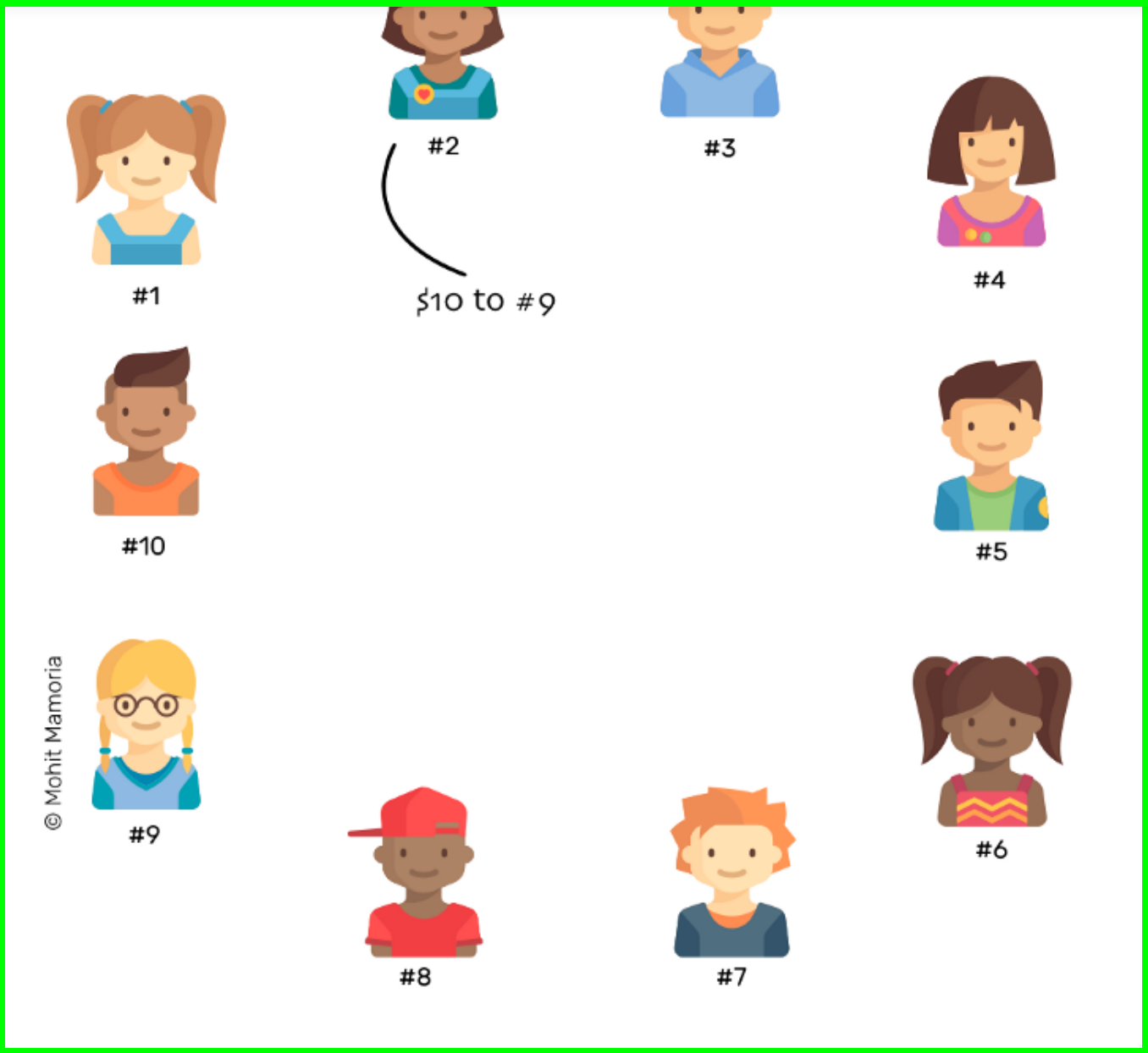
What is a blockchain?

A blockchain, simply put, is a database. It's an ever growing database of certain kind of data and has quite remarkable properties:

1. Once data is stored in the database, it can never be modified or deleted. Every record on a blockchain is permanent for eternity.
2. No single individual or organization maintains the database; several thousand individuals do, and everyone has a copy of the database with themselves.

To understand how several people are able to keep their copies of the database in sync with everyone else, imagine there are ten individuals in a network. Everyone is sitting with an empty file folder and an empty page in front of them. Whenever anyone does something important in the network, like transferring money, they announce it to everyone in the network.

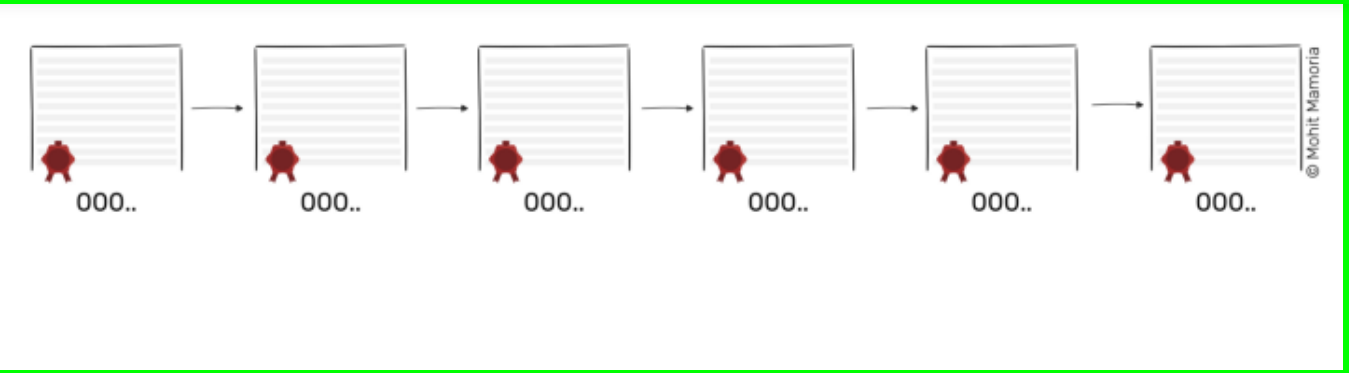




Everyone makes a note of the announcement on their pages until the page is filled. When it does, everyone has to seal the contents of the page by solving a mathematical puzzle. Solving the mathematical puzzle ensures that everyone's page had same contents and that they can never be modified. Whoever does it first, gets rewarded with some amount of cryptocurrency.

Note: Want to know how exactly the process is carried out? Read the ultimate guide to understand blockchain.

Once the page is sealed, the page is added to the file folder, a new page is brought out and the process continues forever.



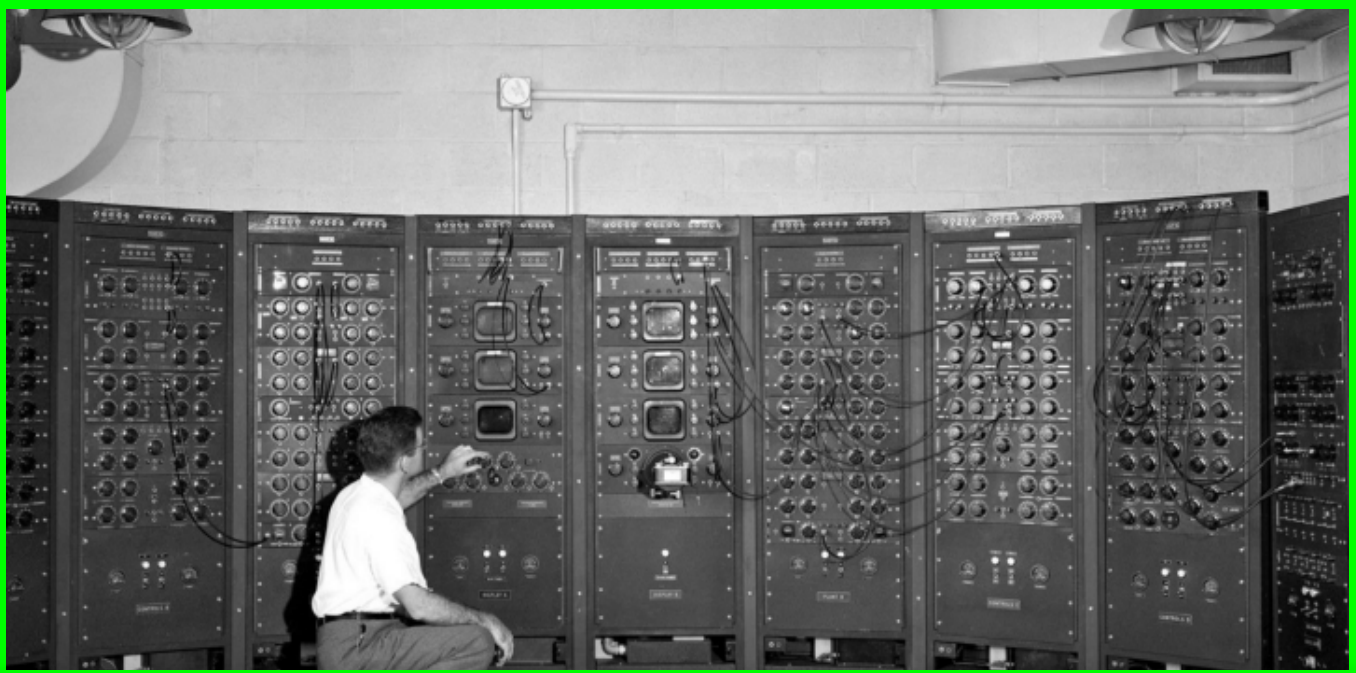
Blockchain

As time passes, these pages (blocks) that contain important records (transactions) are added to the folder (chain), thus forming the database (blockchain).

What does a blockchain store?

A blockchain can be used to store any kind of data, and the kind of data a blockchain stores, gives it its value. Bitcoin's blockchain stores the records of financial transactions, therefore, making it analogous to a currency like dollars or pounds. Bitcoins serve no additional purpose than what dollars serve. Ethereum is different.

Ethereum is not merely a currency like dollars, pounds or bitcoin. Ethereum has a purpose higher than just being a currency. Ethereum is this:



'Ethereum computer' has about the same power as one of the rare 90's smartphones; so it can't really do much more than some very trivial things.

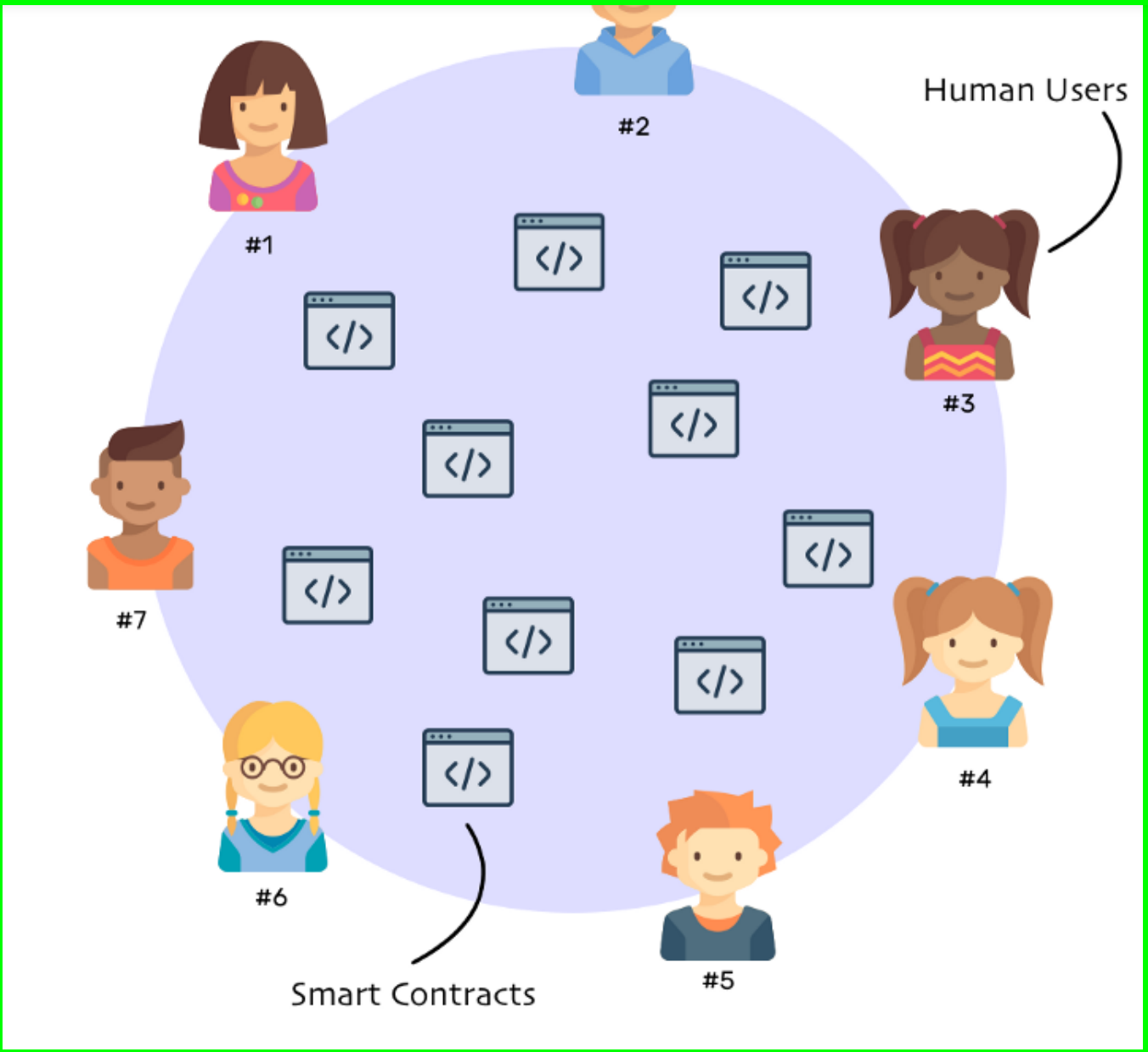
That doesn't really sound so impressive, so why is there so much hype around Ethereum? Well, that's a really good question. Ethereum is taking the world by storm because it's a completely decentralized computer that is distributed across the globe. Understanding how Ethereum's blockchain works will reveal how it acts like a world computer.

How does Ethereum work?

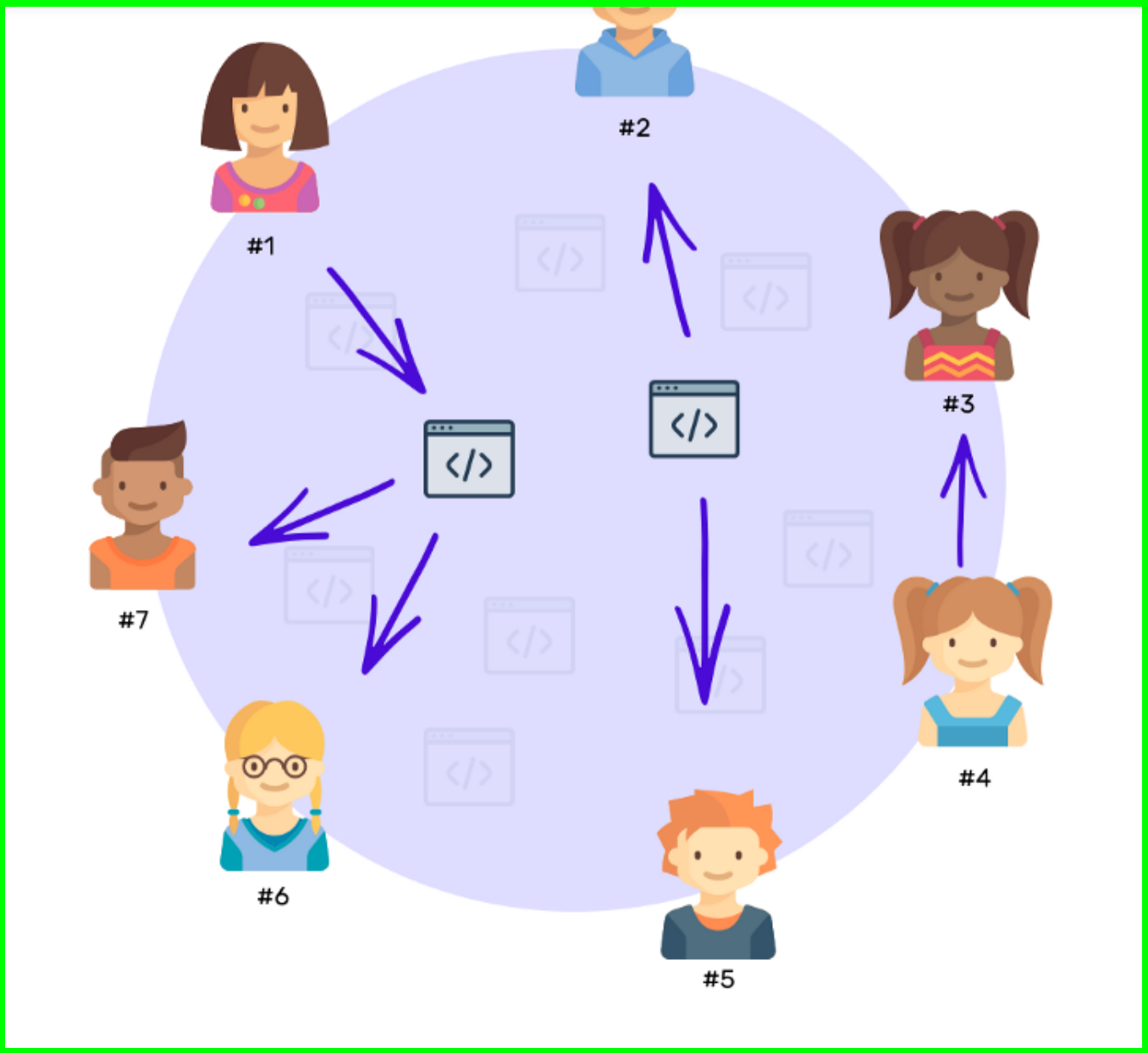
Like any other blockchain, Ethereum needs several thousand people running a software on their computers to power the network. Every node (computer) in the network runs something called Ethereum Virtual Machine (EVM). Think of EVM as a operating system that understands and executes the software written in Ethereum specific programming language. The software/apps executed by Ethereum Virtual Machine are called 'smart contracts.'

To get anything done on this world computer, you need to pay a price. However, you don't pay it in regular currency like dollars or pounds. Instead, everything has to be paid with a cryptocurrency native to the network, called ether. Ether is exactly like bitcoin except that it can also be used to pay for executing smart contracts on Ethereum.

A human being and a smart contract are both seen as users on Ethereum. Whatever a human user can do, a smart contract can do too, and then some.



Smart contracts act exactly like any other human user in the network. Both of them can send and receive ether just like any other currency.



But unlike human users, smart contracts can also execute a predefined computer program to perform various actions when triggered. To understand the power of a smart contract, let's consider an example.

Power of smart contracts

Imagine you and I place a bet about tomorrow's weather. I bet that it'll be sunny tomorrow while you bet it'll be rainy. We agree that the loser has to give the winner $100. How can we do this and ensure that the loser will keep his promise? I can think of three distinct ways:

1. Trust each other

know all kinds of embarrassing stuff about me. But things get more difficult if we're complete strangers. You have no reason to trust me and I have no reason to trust you.

2. Sign a legal agreement

Another plausible way is to formulate our bet as a legal agreement. We'll both sign an agreement that defines all the terms of our bet in detail — including what happens if the loser violates the agreement.

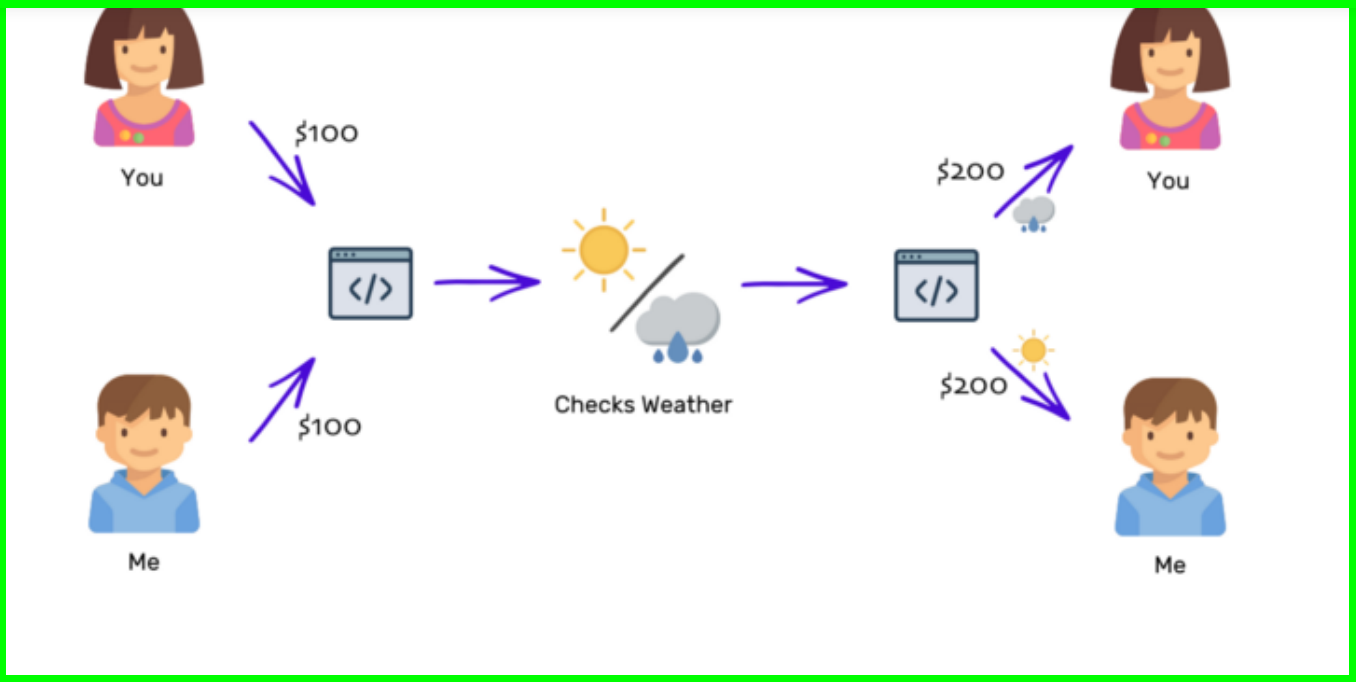
The agreement would makes us legally obligated to pay the winner, but it wouldn't serve any practical purpose because forcing the agreement through the legal route would be more expensive than what the bet was worth.

3. Get help from a mutual friend

We could find a mutual friend who we both trust and we'd both give him/her $100 each for safekeeping. The nextday, he/she would check the weather and give the total $200 to whoever won the bet. Simple and easy, except that it isn't: What if the trusted friend runs away with $200?

Now we have three different ways of doing the bet but each option has its shortcomings. Because we are strangers, we cannot trust each other. Forcing a legal agreement will be so expensive that it wouldn't be practically feasible. Getting help from a mutual friend brings up the question of trust again.

Ethereum's smart contract can save the day in such a situation. A smart contract is like the trusted mutual friend but written in code. Ethereum allows us to write a software that accepts ether worth $100 from both of us, and then the next day, uses the open weather API to check the weather and transfer the total ether worth of $200 to the winner.

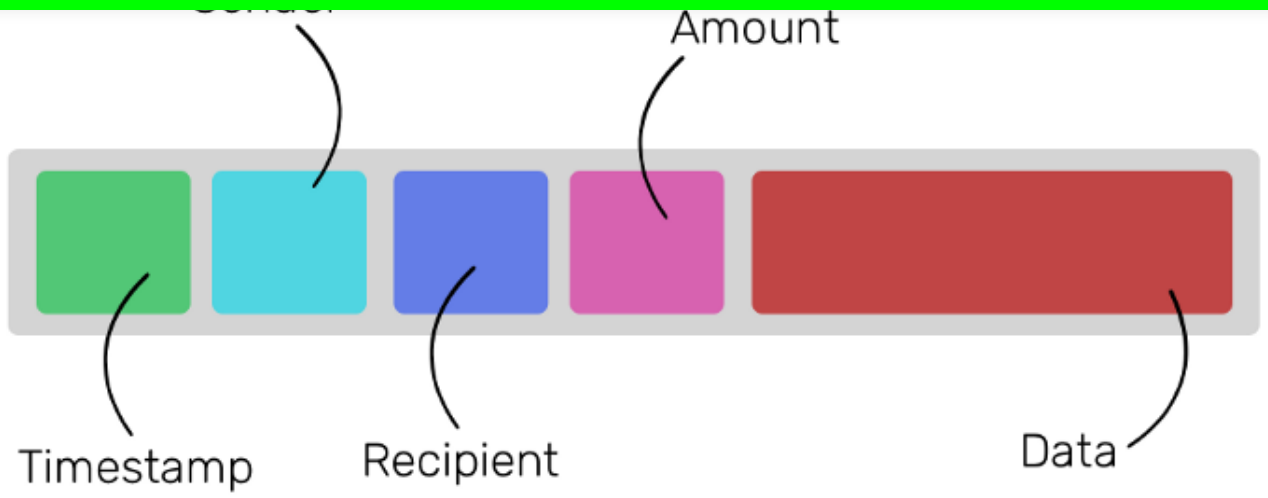


Once a smart contract has been written it cannot be edited or altered in any way. Therefore, you can be sure that whatever the contract dictates, it will be executed no matter what.

But how is a smart contract executed? And how does it relate to blockchain?

How does smart contract relate to blockchain?

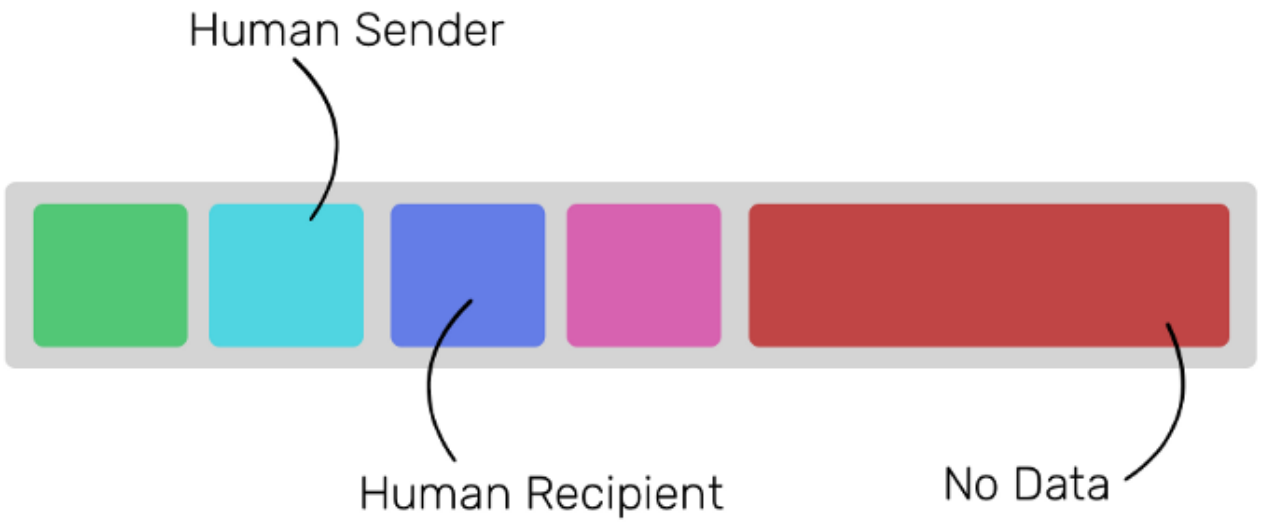
Whenever a smart contract is executed, it records the information about the execution on a block as a transaction. On a very high level, a transaction on Ethereum blockchain looks like this:



The fields are self explanatory except the last one. The ‘data’ field is what gives Ethereum its unique power. The ‘data’ field is used to record creation and execution of smart contracts as a transaction. Any given block on the Ethereum blockchain can contain three kind of transactions:

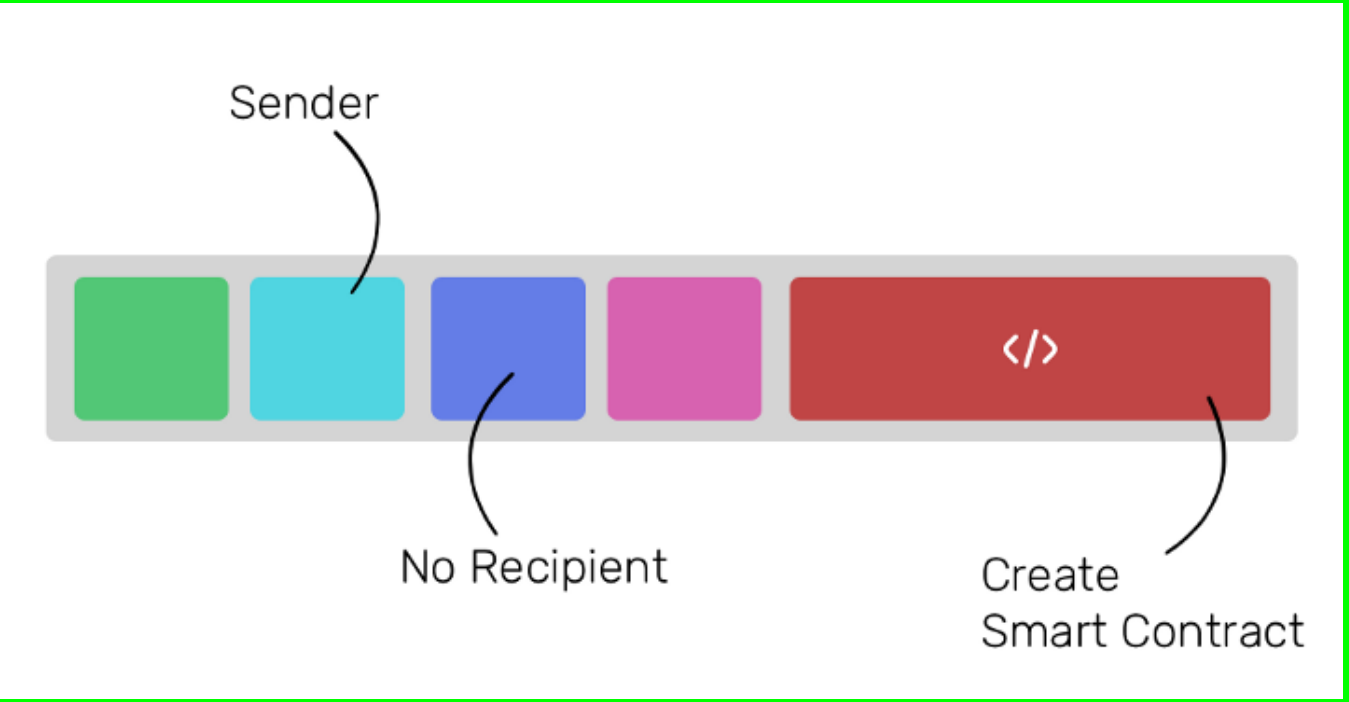
1. Regular transfers of ether from one user to a human user

These are the regular bitcoin-like transactions in the network. If you send ether directly to your friend the data field will be left empty.



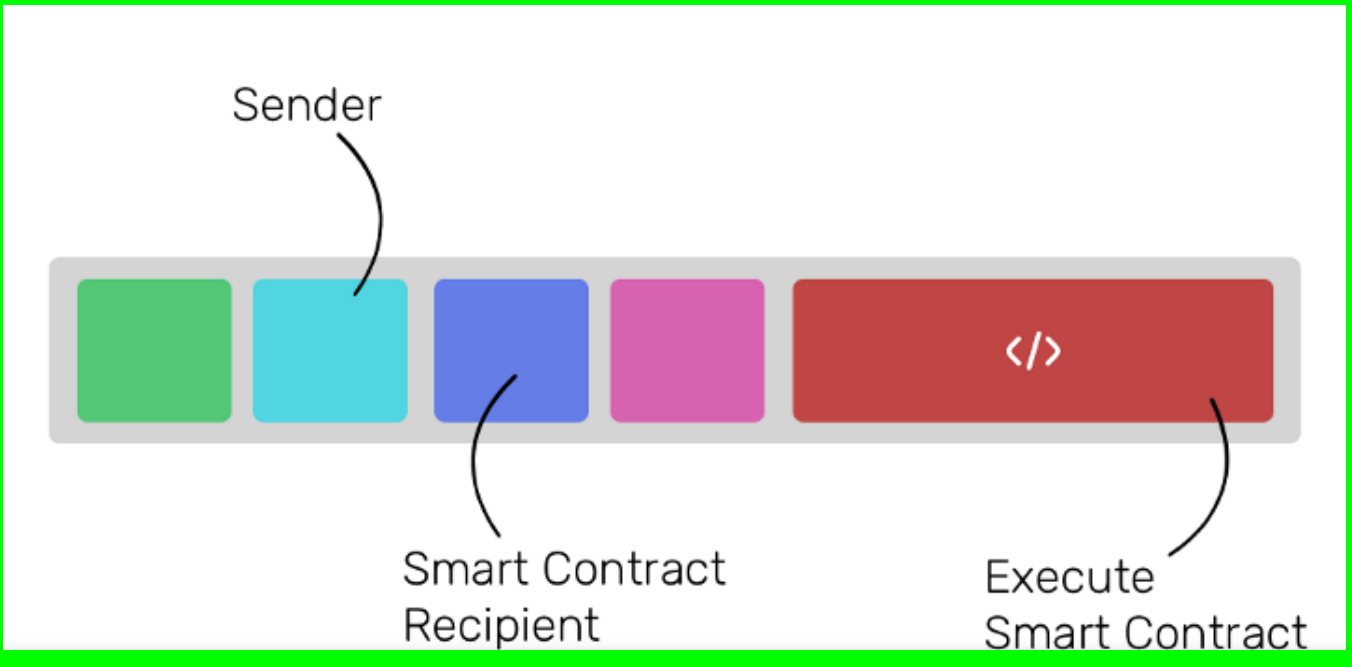
2. Transfers of ether from one user to no one

in the ‘data’ field. The ‘data’ field contains the software code that will be made to act like any other user in the network.



3. Transfers of ether from a user to a smart contract

Whenever a user (or a smart contract) wants to execute a smart contract, he/she/it is required to make a transaction to the smart contract and put the instructions for the execution in the ‘data’ field.



addition to making note of it, each node also executes the instructed smart contract to bring the state of their EVM in sync with the rest of the network.

Each node executes a piece of software, thus, making the whole network act as a giant (but slow) distributed computer. Every tiny execution is then stored on the blockchain to make it permanent.

Wait, I've heard about something called Gas — what's that?

I told you that the user using a smart contract must pay a certain price to execute it. This price is paid to the node that actually spends memory, storage, computation and electricity to execute the smart contract.

To calculate the prices of smart contracts, every statement has an assigned cost to it. For example, if you execute a statement that uses the node's memory, those type of statements have a specific cost. If you execute a statement that uses the node's disk storage, those kind of statements have a specific cost attached to them. The unit in which the cost is defined is called Gas. Eventually, Gas is converted to ether using an exchange rate.

Whenever you execute a smart contract, you have to define the maximum Gas to be consumed. The execution will stop either when the execution is completed or when the Gas Limit is reached. This is done to avoid infinite loops in smart contracts, preventing the program getting stuck executing a set of statements repeatedly without proceeding further.

Such situations occur because of programmer's carelessness. With every repetition, some of the assigned Gas will be used, thus making any infinite loop a finite one. It doesn't make any sense for a node to be stuck in execution because of a programmer's mistake. The concept of Gas solves this problem.

And that, ladies and gentleman, is Ethereum

Ethereum isn't just a cryptocurrency to be traded; its real value lies in its purpose. Ethereum's purpose is to allow the owner to use the distributed world computer that several thousand nodes are powering.



slow compared to what? The faster but centrally controlled servers.

To enjoy the lower costs of using a centralized computer, we give them the power to control us. If the central computer (server) goes down or gets hacked, it takes down with it all the clients attached to it. A decentralized computer will only go down if every single node goes down, making it a computer that will always be available. Wherever there's internet, there's Ethereum.

—

About the author

Mohit Mamoria is the CEO of godtoken.org and editor of a weekly newsletter, Unmade, which delivers one startup idea from the future to your inboxes.

Have feedback? I am available on Twitter.

The story first appeared on The Next Web.

Thanks for reading! :) If you liked it, please support by hitting that heart button below. 💚

. . .

You might also like —

Bartering to Blockchain — History Of Money

What is money anyway?

hackernoon.com

Sign up for Get Better Tech Emails via HackerNoon.com

By HackerNoon.com

how hackers start their afternoons. the real shit is on hackernoon.com. Take a look.

Your email

Get this newsletter

Get started