Write up on Blockchain and Ethereum

By Chandrashekar Dasari

What is blockchain?

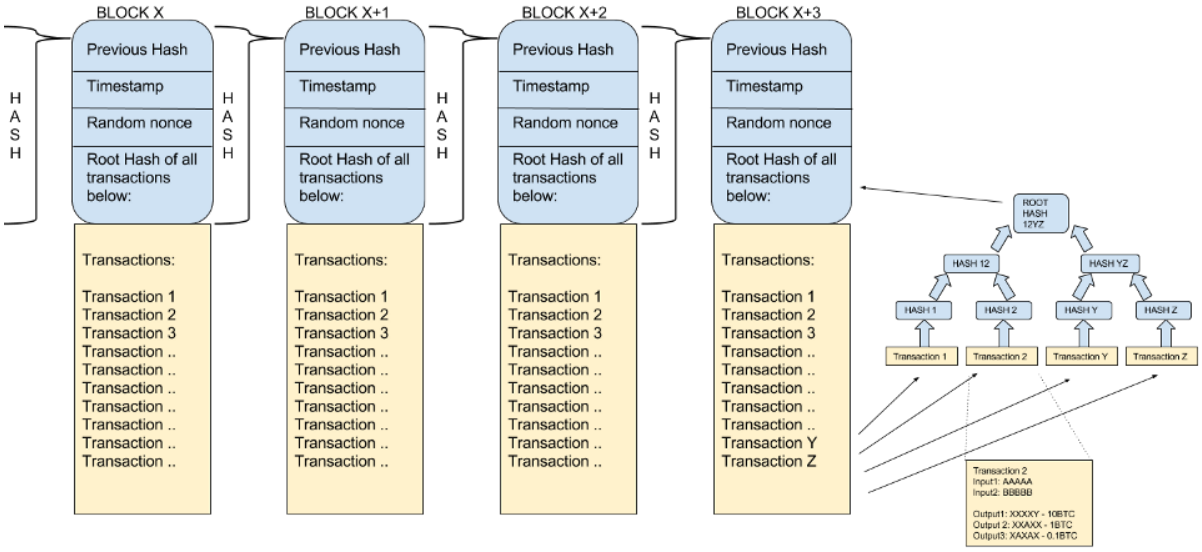
Blockchain technology was first outlined in 1991 by Stuart Haber and W. Scott Stornetta, two researchers who wanted to implement a system where document timestamps could not be tampered with. But it wasn't until almost two decades later, with the launch of Bitcoin in January 2009, that blockchain had its first real-world application.
The Bitcoin protocol is built on blockchain. In a research paper introducing the digital currency, Bitcoin's pseudonymous creator Satoshi Nakamoto referred to it as "a new electronic cash system that's fully peer-to-peer, with no trusted third party."

If this technology is so complex, why call it "blockchain?" At its most basic level, blockchain is literally just a chain of blocks, but not in the traditional sense of those words. When we say the words "block" and "chain" in this context, we are actually talking about digital information (the "block") stored in a public database (the "chain"). **Essentially blocks in a blockchain are digital pieces of information.** As shown in the figure.

Which consists of three main parts within the block. blocks store information about transactions, say the date, time, and amount (can be any currency) of your most recent transaction for another user. Blocks store information about who is participating in transactions such as the sender and receiver nodes in the blockchain. Instead of using your actual name, your purchase is recorded without any **identifying information using a unique "digital signature,"** sort of like a username. Blocks store information that distinguishes them from other blocks. Much like you and I have names to distinguish us from one another, each block stores a unique code called a "hash" that allows us to tell it apart from every other block. Even though the

details of your new transaction would look nearly identical to your earlier purchase, we can still tell the blocks apart because of their unique codes.

A single block on the blockchain can actually store up to 1 MB of data. Depending on the size of the transactions, that means a single block can house a few thousand transactions under one roof. best way to understand blockchains is to understand how cryptocurrencies such as bitcoin work. Blockchains are most recognized with respect to the Cryptocurrencies. Digital currencies backed by cryptography (a.k.a cryptocurrencies) make such trust-less systems possible.



How does blockchain work?

When a block stores new data it is added to the blockchain. Blockchain, as its name suggests, consists of multiple blocks strung together. In order for a block to be added to the blockchain, however, four things must happen:

1. A transaction must occur. Let's continue with the example of your impulsive Amazon purchase. After hastily clicking through multiple checkout prompts, you go against your better judgment and make a purchase.

2. That transaction must be verified. After making that purchase, your transaction must be verified. In blockchain the job to verify the records is left up to a network

of computers. These networks often consist of thousands more more incase of cryptocurrencies. These are associated for all the computers over the globe. When the transaction occurs the network of computers rushes to check that your transaction happened in the way you said it did. That is, they confirm the details of the purchase, including the transaction's time, dollar amount, and participants. This is the stand out point of blockchain that makes it very almost impenetrable in terms of security.

3. That transaction must be stored in a block. After your transaction has been verified as accurate, it gets the green light. The transaction's currency amount, your digital signature, and sender's digital signature are all stored in a block. There, the transaction will likely join hundreds, or thousands, of others like it.

4. That block must be given a hash. Not unlike an angel earning its wings, once all of a block's transactions have been verified, it must be given a unique, identifying code called a hash. The block is also given the hash of the most recent block added to the blockchain. Once hashed, the block can be added to the blockchain.
When that new block is added to the blockchain, it becomes publicly available for anyone to view you will see that you have access to transaction data, along with information about when ("Time"), where ("Height"), and by who ("Relayed By") the block was added to the blockchain.

Security and Privacy for Blockchain

With regards to privacy aspect of blockchain, Anyone can view the contents of the blockchain, but users can also opt to connect their computers to the blockchain network. In doing so, their computer receives a copy of the blockchain that is updated automatically whenever a new block is added. This means that as transactions are happening, anyone can see what has happened in the past transactions.

Each computer in the blockchain network has its own copy of the blockchain, which means that there are thousands, or in the case of Bitcoin, millions of copies of the same blockchain. Although each copy of the blockchain is identical,

spreading that information across a network of computers makes the information more difficult to manipulate. With blockchain, there isn't a single, definitive account of events that can be manipulated. Instead, **a hacker would need to manipulate 51% of copies of the blockchain on the network.**
Looking over the Bitcoin blockchain, however, you will notice that you do not have access to identifying information about the users making transactions. Although transactions on blockchain are not completely anonymous, personal information about users is limited to their digital signature, or username.

When it comes to security aspect of blockchain, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the blockchain. If you take a look at Bitcoin's blockchain, you'll see that each block has a position on the chain, called a "height."

After a block has been added to the end of the blockchain, it is very difficult to go back and alter the contents of the block. That's because each block contains its own hash, along with the hash of the block before it. Hash codes are created by a math function that turns digital information into a string of numbers and letters. If that information is edited in any way, the hash code changes as well.

If a hacker tries to change the change the hash value of transaction then the next block in the chain will still contain the old hash, and the hacker would need to update that block in order to cover their tracks. However, doing so would change that block's hash. And the next, and so on. Thus making it not worth the effort to try and manipulate the blockchain network. This only gets more difficult as the network gets bigger adding more nodes to the network, It increases the number of nodes the hacker must try to manipulate.
To address the issue of trust, blockchain networks have implemented tests for computers that want to join and add blocks to the chain. The tests, called "consensus models," require users to "prove" themselves before they can participate in a blockchain network. One of the most common examples employed by Bitcoin is called "proof of work."

In the proof of work system, **computers must "prove" that they have done "work" by solving a complex computational math problem**. If a computer solves one of these problems, they become eligible to add a block to the

blockchain. But the process of adding blocks to the blockchain, what the cryptocurrency world calls “mining,” is not easy. In fact, according to the blockchain news site BlockExplorer, the odds of solving one of these problems on the Bitcoin network are about 1 in 7 trillion at the time of writing. To solve complex math problems at those odds, computers must run programs that cost them significant amounts of power and energy

As the network size keeps on increasing, Proof of work does not make attacks by hackers impossible, but it does make them somewhat useless. If a hacker wanted to coordinate an attack on the blockchain, they would need to solve complex computational math problems at 1 in 7 trillion odds just like everyone else. The cost of organizing such an attack would almost certainly outweigh the benefits.

Blockchain in Real World

Blocks on the blockchain store data about monetary transactions. But it turns out that blockchain is actually a pretty reliable way of storing data about other types of transactions, as well. In fact, blockchain technology can be used to store data about property exchanges, stops in a supply chain, and even votes for a candidate.

Financial institutions only operate during business hours, five days a week. if you do make your deposit during business hours, the transaction can still take 1-3 days to verify due to the sheer volume of transactions that banks need to settle. Blockchain, on the other hand, never sleeps. By integrating blockchain into banks, consumers can see their transactions processed in as little as 10 minutes, basically the time it takes to add a block to the blockchain, regardless of the time or day of the week. With blockchain, banks also have the opportunity to exchange funds between institutions more quickly and securely. In the stock trading business, for example, the settlement and clearing process can take up to three days

Blockchain forms the bedrock for cryptocurrencies like Bitcoin. As we explored earlier, currencies like the U.S. dollar are regulated and verified by a central

authority, usually a bank or government. Under the central authority system, a user's data and currency are technically at the whim of their bank or government. If a user's bank collapses or they live in a country with an unstable government, the value of their currency may be at risk. These are the worries out of which Bitcoin was borne. By spreading its operations across a network of computers, blockchain allows Bitcoin and other cryptocurrencies to operate without the need for a central authority. This not only reduces risk but also eliminates many of the processing and transaction fees. It also gives those in countries with unstable currencies a more stable currency with more applications and a wider network of individuals and institutions they can do business with, both domestically and internationally. Now there are over 1000 types of cryptocurrencies.

Health care providers can leverage blockchain to securely store their patients' medical records. When a medical record is generated and signed, it can be written into the blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy

Mining cryptocurrencies

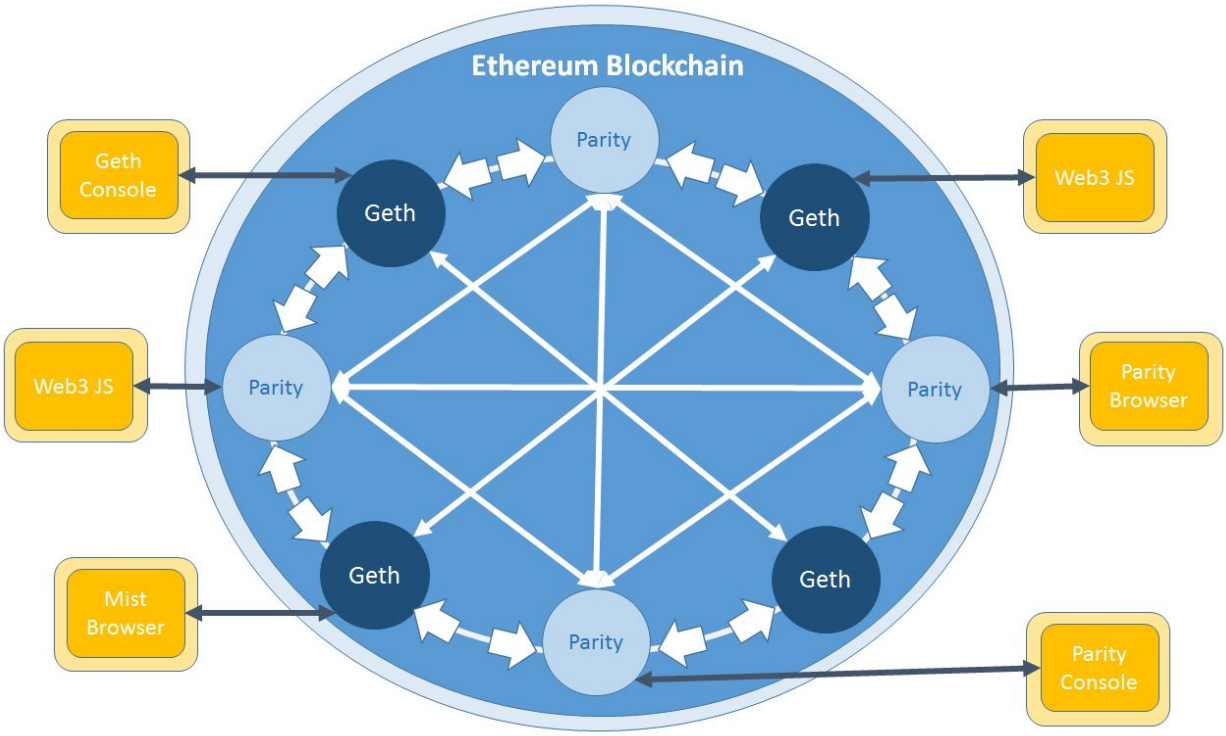
At a high level, each participating node or "miner" on a bitcoin network is running special software and hardware to solve for the nonce to verify that a block of transactions is valid. This takes a lot of computing resources, and so whoever cracks the problem is rewarded with new bitcoins from the network as well as any transaction fees that Alice included with the 1 bitcoin transfer. The successful miner announces the new blockchain (=old blockchain + the new block) to the rest of the network , the network checks the validity of this claim, arrives at a consensus and accepts the proposed blockchain as the new source of truth.

A nonce is an integer which will be incremented during the mining process.Without a nonce, the data of a block is constant, and thus the hash function always returns the same result. If your hash consists of hexadecimal characters, and you want to have a hash starting with 5 zeros you will have a

probability of 1/1048576 to produce a hash verifying this condition with a random nonce. Each time you fail to get a hash verifying the condition, you can update the nonce and try again. This assures that the miners of the network will have to work to add a block to the blockchain and that's why this algorithm is called proof of work.

Ethereum

Like Bitcoin, Ethereum is a distributed public blockchain network. Although there are some significant technical differences between the two, the most important distinction to note is that Bitcoin and Ethereum differ substantially in purpose and capability. Bitcoin offers one particular application of blockchain technology, a peer to peer electronic cash system that enables online Bitcoin payments.

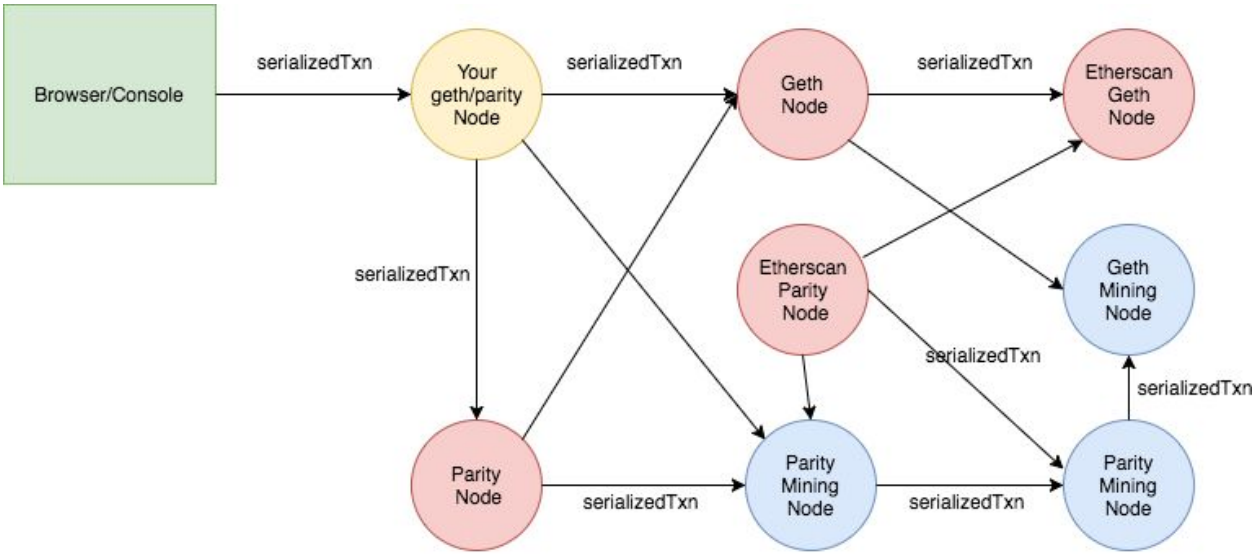


While the Bitcoin blockchain is used to track ownership of digital currency (bitcoins), the Ethereum blockchain focuses on running the programming code of any decentralized application.
In the Ethereum blockchain, instead of mining for bitcoin, miners work to earn Ether, a type of crypto token that fuels the network. Beyond a tradeable cryptocurrency, Ether is also used by application developers to pay for transaction fees and services on the Ethereum network.

There is a second type of token that is used to pay miners fees for including transactions in their block, it is called gas, and every smart contract execution requires a certain amount of gas to be sent along with it to entice miners to put it in the blockchain.

Ethereum Network

Ethereum's core innovation, the Ethereum Virtual Machine (EVM) is a Turing complete software that runs on the Ethereum network. It enables anyone to run any program, regardless of the programming language given enough time and memory. The Ethereum Virtual Machine makes the process of creating blockchain applications much easier and efficient than ever before.



Signed Transaction Propogates to the network

Instead of having to build an entirely original blockchain for each new application, Ethereum enables the development of potentially thousands of different applications all on one platform.

The underlying network consists of nodes or computers connected in a decentralized , peer to peer network. Each node runs an EVM, and processes the same instructions to ensure that consensus is achieved on any particular transaction.

A Contract Account contains code to execute a particular function that it was designed for, and this code 'lives' on the Ethereum blockchain . Once a contract account is triggered either by an Externally Owned Account or by another contract account the code inside is executed by the Ethereum Virtual Machine(EVM) on each participating node. These accounts also enable "Smart Contracts".

Smart contracts are contract accounts that facilitate exchange of value in a transparent and trustless way without the need for middlemen. Here are the high level steps to create a Smart Contract:

A contract account with rules (and specified actions based on those rules) is created. e.g. "If this is true, then do that"

This **contract is then coded in a Ethereum high level language such as Solidity** (syntax is similar to Javascript) and then "deployed" on the Ethereum Blockchain.

Once deployed, the contract gets a public key address, that can be used to reach the contract and trigger its code execution.

Also, once a smart contract is deployed to the Ethereum blockchain, it cannot be changed even by the EOA that created it.

Geth: if you have experience with web development and are interested in building frontends for dapps, you should experiment with Geth.

Eth : If you want added security by running two different implementations in parallel or are serious about GPU mining, then the C++ Eth client is for you.

Pyethapp: If you are a Python developer that wants to build decentralized apps or are interested in Ethereum for research or an academic purpose, this is a great client.

We used Geth for the prototype in the other folder. Ethereum's Go implementation is called Geth**.** Geth is a command line interface (CLI) tool that communicates with the Ethereum Network and acts as the a link between your computer, its hardware and the rest of the ethereum nodes or network computers.

If a block is mined by another node, your Geth program will pick it up and then pass on the new information onto your GPU or CPU to update the blockchain.

To create our private blockchain then, we will create a genesis block. To do this, we will create a custom Genesis file, and ask Geth to use that genesis file to create our own genesis block , which in turn will be the start of our custom private blockchain.

```
{
    "config": {
        "chainId": 987,
        "homesteadBlock": 0,
        "eip155Block": 0,
        "eip158Block": 0
    },
    "difficulty": "0x400",
    "gasLimit": "0x8000000",  //set this really high for testing
    "alloc": {}

}
}
```

Once you run this snippet on your terminal window, you should see Geth connect to the genesis file and provide confirmation of the same.

We use miner.start() and miner.stop() for mining in our private ethereum network. In public ethereum networks it's a lot more difficult to mine and requires large about of GPU usage. Whereas in out private ethereum network set the **difficulty to low in the Genesis.json file.** Thus we can mine easily with those commands.

In the prototype, I already prepared 10 nodes in the ethereum network along with making it a docker container. All the instructions for installing and interacting with geth are provided in the README.md file of the repository.