Crypto Currenccy UNIT - 2 Notes

Master of Computer Applications (Anna University)

MC4013 CRYTOCURRENCY AND BLOCKCHAIN TECHNOLOGY
UNIT II CRYPTOCURRENCY

What is BITCOIN?

Bitcoin is a decentralized digital currency that operates without the need of financial system or government authorities. **It utilizes peer-to-peer transfers on a digital network that records all cryptocurrency transactions**

How Bitcoin Works

Bitcoin is more than a cryptocurrency used for payments or as an investment. There is an entire ecosystem at work behind a cryptocurrency. In fact, many such ecosystems are at work on the internet today, but because Bitcoin was the first, it's useful to understand how it functions.

The Bitcoin Blockchain

The Bitcoin blockchain is a database of transactions secured by encryption and validated by peers. Here's how it works. The blockchain is not stored in one place; it is distributed across multiple computers and systems within the network. These systems are called nodes. Every node has a copy of the blockchain, and every copy is updated whenever there is a validated change to the blockchain.

The blockchain consists of blocks, which store data about transactions, previous blocks, addresses, and the code that executes the transactions and runs the blockchain. So, to understand the blockchain, it's important first to understand blocks.

Blocks

When a block on the blockchain is opened, the blockchain creates the block hash, a 256-bit number that encodes the following information:

- The block version: the Bitcoin client version
- The previous block's hash: the hash of the block before the current one
- The coinbase transaction: the first transaction in the block, issuing the bitcoin reward
- The block height number: how far away numerically the block is from the first block
- Merkelroot: A 256-bit number that stores the information about all previous blocks
- Timestamp: the time and date the block was opened
- The target in bits: the network target
- The nonce: a randomly-generated 32-bit number

Queued transactions are entered into the block, the block is closed, and the blockchain creates the hash. Each block contains information from the previous blocks, so the blockchain cannot be altered because each block is "chained" to the one before it. Blocks are validated and opened by a process called mining.

BITCOIN MINING

Mining is the process of validating transactions and creating a new block on the blockchain. Mining is conducted by software applications that run on computers or machines designed specifically for mining called Application Specific Integrated Circuits.

The hash is the focus of the mining programs and machines. They are working to generate a number that matches the block hash. The programs randomly generate a hash and try to match the block hash, using the nonce as the variable number, increasing it every time a guess is made. The number of hashes a miner can produce per second is its hash rate.

Mining programs across the network generate hashes. The miners compete to see which one will solve the hash first—the one that does receives the bitcoin reward, a new block is created, and the process repeats for the next group of transactions.

Bitcoin's protocol will require a longer string of zeroes depending on the number of miners, adjusting the difficulty to hit a rate of one new block every 10 minutes. The difficulty—or the average number of tries it takes to verify the hash—has been increasing since Bitcoin was introduced, reaching tens of trillions of average attempts to solve the hash.1 As this suggests, it has become significantly more difficult to mine Bitcoin since the cryptocurrency launched.

Mining is intensive, requiring big, expensive rigs and a lot of electricity to power them. And it's competitive. There's no telling what nonce will work, so the goal is to plow through them as quickly as possible with as many machines working on the hash as possible to get the reward. This is why mining farms and mining pools were created.

KEYS AND WALLETS

A common question from those new to Bitcoin is, "I've purchased a bitcoin, now where is it?" The easiest way to understand this is to think about the Bitcoin blockchain as a community bank that stores everyone's funds. You view your balance using a wallet, which is like your bank's mobile application.

If you're like many people today, you don't use cash very often and never see the money in your checking account. Instead, you use credit and debit cards, which act as tools to access and use your money. You access your bitcoin using a wallet and keys.

KEYS

A bitcoin at its core is data with ownership assigned. Data ownership is transferred when transactions are made, much like using your debit card to transfer money to an online retailer. You use your wallet, the mobile application, to send or receive bitcoin.

When bitcoin is assigned to an owner via a transaction on the blockchain, that owner receives a number, their private key. Your wallet has a public address—called your public

key—that is used when someone sends you a bitcoin, similar to the way they enter your email address in an email.

WALLETS

A wallet is a software application used to view your balance and send or receive bitcoin. The wallet interfaces with the blockchain network and locates your bitcoin for you. The blockchain is a ledger with portions of bitcoin stored on it. Because bitcoin is data inputs and outputs, they are scattered all over the blockchain in pieces because they have been used in previous transactions. Your wallet application finds them all, totals the amount, and displays it.

There are two types of wallets, custodial and noncustodial. A custodial wallet is one where a trusted entity, like an exchange, holds your keys for you. For example, when you sign up for a Coinbase exchange account, you can elect to have them store your keys for you as custodians.

Noncustodial wallets are wallets where the user takes responsibility for securing the keys, such as in your wallet application on your mobile phone. Storing keys in an application connected to the internet is referred to as hot storage. However, hot storage is the vulnerability most often exploited.

BITCOIN TRANSACTIONS

A bitcoin transaction happens when you send or receive a bitcoin. To send a coin, you enter the receiver's address in your wallet application, enter your private key, and agree to the transaction fee. Then, press whichever button corresponds to "send." The receiver must wait for the transaction to be verified by the mining network, which can take up to 30 minutes because transactions wait in a mining queue called the mempool.

BITCOIN SECURITY

There are many parts that make up the Bitcoin blockchain and network, but it is not necessary to understand it all to use this new currency technology. You only need to know that you use a wallet to send, receive, and store your bitcoin keys; you also should use a cold storage method for security because non-custodial wallets can be hacked.

Custodial wallets can also be hacked, but many who offer this service take measures to reduce the chances that hackers can get into the storage systems. Most are turning to enterprise-level cold storage techniques businesses use to store essential data for extended timeframes.

For good reason, many people are concerned about Bitcoin's level of security, especially since it involves exchanging money for encrypted data ownership. However, it's important to note that the Bitcoin blockchain has never been hacked because of the community consensus mechanisms used.

Wallets are the weak spot, so if you're looking to get involved in Bitcoin, it's essential to understand how to utilize cold storage methods and keep your keys out of your hot wallet.

VALUE OF BITCOIN:

Bitcoin Market Cap is at a current level of **386.96B**, down from 395.94B yesterday and down from 1.158T one year ago. This is a change of -2.27% from yesterday and -66.57% from one year ago.

BITCOIN COMMUNITY

Bitcoin community is **an association of people, that own and use bitcoin, are interested in its spread and participate in discussion about its future development**. Bitcoin community consists of regular bitcoin users, crypto enthusiasts, tech developers, media, financial institutions and various startups.

TYPES OF BITCOINS

The four major types include **utility, payment, security, and stablecoins**. There also are DeFi tokens, NFTs, and asset-backed tokens. Of all cryptocurrencies, the most common are utility and payment tokens. These do not have their investment-backed or guaranteed by regulation.

SATOSHI

The satoshi is the smallest unit of the cryptocurrency bitcoin. It is named after Satoshi Nakamoto, the founder(s) of the protocol used in blockchains and the bitcoin cryptocurrency. The satoshi to bitcoin ratio is 100 million satoshis to one bitcoin.

10 BEST CRYPTOCURRENCIES TO INVEST IN 2022

From Bitcoin and Ethereum to Dogecoin and Tether, there are thousands of different cryptocurrencies, which can make it overwhelming when you're first getting started in the world of crypto. To help you get your bearings, these are the top 10 cryptocurrencies based on their market capitalization, or the total value of all of the coins currently in circulation.

1. Bitcoin (BTC)

Created in 2009 by someone under the pseudonym Satoshi Nakamoto, Bitcoin (BTC) is the original cryptocurrency. As with most cryptocurrencies, BTC runs on a blockchain, or a ledger logging transactions distributed across a network of thousands of computers. Because additions to the distributed ledgers must be verified by solving a cryptographic puzzle, a process called proof of work, Bitcoin is kept secure and safe from fraudsters.

2. Ethereum (ETH)

Both a cryptocurrency and a blockchain platform, Ethereum is a favorite of program developers because of its potential applications, like so-called smart contracts that automatically execute when conditions are met and non-fungible tokens (NFTs).

Ethereum has also experienced tremendous growth. From April 2016 to the beginning of March 2022, its price went from about $11 to over $3,000, increasing more than 27,000%.

3. Tether (USDT)

Unlike some other forms of cryptocurrency, Tether is a stablecoin, meaning it's backed by fiat currencies like U.S. dollars and the Euro and hypothetically keeps a value equal to one of those denominations. In theory, this means Tether's value is supposed to be more consistent than other cryptocurrencies, and it's favored by investors who are wary of the extreme volatility of other coins.

4. Binance Coin (BNB)

The Binance Coin is a form of cryptocurrency that you can use to trade and pay fees on Binance, one of the largest crypto exchanges in the world.

Since its launch in 2017, Binance Coin has expanded past merely facilitating trades on Binance's exchange platform. Now, it can be used for trading, payment processing or even booking travel arrangements. It can also be traded or exchanged for other forms of cryptocurrency, such as Ethereum or Bitcoin.

BNB's price in 2017 was just $0.10. By the beginning of March 2022, its price had risen to around $413, a gain of approximately 410,000%.

5. XRP (XRP)

Created by some of the same founders as Ripple, a digital technology and payment processing company, XRP can be used on that network to facilitate exchanges of different currency types, including fiat currencies and other major cryptocurrencies.

At the beginning of 2017, the price of XRP was $0.006. As of March, 2022, its price reached $0.80, equal to a rise of more than 12,600%.

6. Terra (LUNA)

Terra is a blockchain payment platform for stablecoins that relies on keeping a balance between two types of cryptocurrencies. Terra-backed stablecoins, such as TerraUSD, are tied to the value of physical currencies. Their counterweight, Luna, powers the Terra platform and is used to mint more Terra stablecoins.

Terra stablecoins and Luna work in concert according to supply and demand: When a stablecoin's price rises above its tied currency's value, users are incentivized to burn their Luna to create more of that Terra stablecoin. Likewise, when its value falls compared to its base currency, this encourages users to burn their Terra stablecoins to mint more Luna. As adoption of the Terra platforms grows, so too does the value of Luna.

From Jan. 3, 2021, when its price was $0.64, to the beginning of March 2022, Luna has risen over 14,200% to $92.

7. Cardano (ADA)

Somewhat later to the crypto scene, Cardano is notable for its early embrace of proof-of-stake validation. This method expedites transaction time and decreases energy usage and environmental impact by removing the competitive, problem-solving aspect of transaction verification present in platforms like Bitcoin. Cardano also works like Ethereum to enable smart contracts and decentralized applications, which are powered by ADA, its native coin.

Cardano's ADA token has had relatively modest growth compared to other major crypto coins. In 2017, ADA's price was $0.02. As of March 1, 2022, its price was at $0.99. This is an increase of 4,850%.

8. Solana (SOL)

Developed to help power decentralized finance (DeFi) uses, decentralized apps (DApps) and smart contracts, Solana runs on a unique hybrid proof-of-stake and proof-of-history mechanisms that help it process transactions quickly and securely. SOL, Solana's native token, powers the platform.

When it launched in 2020, SOL's price started at $0.77. By March 1, 2022, its price was around $101, a gain of nearly 13,000%.

9. Polkadot (DOT)

Polkadot (DOT), founded in the year 2016, is a unique blockchain interoperability protocol designed to connect different chains together. It also allows exchanging data and processing transactions for parachains, or parallel blockchains without compromising their security. Developers can create their own blockchains while using the Polkadot security.

The core founder of Ethereum, Gavin Wood created Polkadot. The exciting feature of DOT is that it has no hard limit on its total supply. Rather, a new token is constantly in circulation.

Polkadot's price reached its heights in May 2020 at $6.30 and later in May 2021, the price hit its all-time high of $55.11.

10. Litecoin (LTC)

Litecoin (LTC), an open-source blockchain project launched in 2011, was created by former crypto exchange Coinbase software engineer Charlie Lee. It was one of the initial cryptocurrencies whose code is imitated from Bitcoin's. Despite the fact that it has similarities with Bitcoin, it is developed to have a faster transaction confirmation time. It can be used as an avenue for paying people around the world without a mediator. LTC is frequently considered as "silver to Bitcoin's gold."

Litecoin has a total round-off supply of 84 million tokens. In May 2021, it recorded its lifetime high of $413.47 but it dropped by over 50%. There are a growing number of merchants that undertake Litecoin. It has a per token value of around $106, the 21st-largest cryptocurrency in the world.

ADVANTAGES AND DISADVANTAGES OF BITCOIN

The advantages of cryptocurrencies include **cheaper and faster money transfers and decentralized systems that do not collapse at a single point of failure**. The disadvantages of cryptocurrencies include their price volatility, high energy consumption for mining activities, and use in criminal activities.

Bitcoin is **fast and easy to use**

Since Bitcoin is a digital peer-to-peer currency as outlined in the original Satoshi Nakamoto whitepaper, transactions are near-instant. They're very low-cost too, much less than central payment networks such as PayPal, Visa or Mastercard.

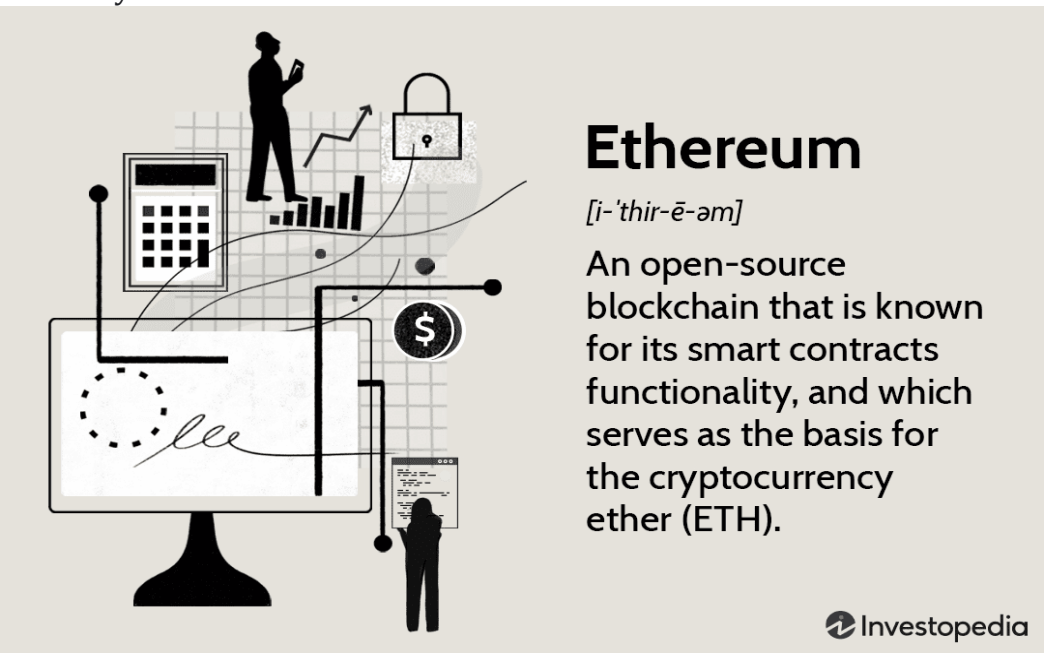
5 disadvantages of cryptocurrency

- Understanding cryptocurrency takes time and effort. ...
- Cryptocurrencies can be an extremely volatile investment. ...
- Cryptocurrencies haven't proven themselves as a long-term investment—yet. ...
- Crypto has serious scalability issues. ...

- Crypto newbies are vulnerable to security risks.

ETHEREUM

Ethereum is **a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code, called smart contracts**. Smart contracts allow participants to transact with each other without a trusted central authority.



ETHEREUM BENEFITS

It has a large and committed global community and the largest ecosystem in blockchain and cryptocurrency. Wide range of functions. Besides being used as a digital currency, Ethereum can also process other financial transactions, execute smart contracts and store data for third-party applications.

A decentralized application (dapp) is **an application built on a decentralized network that combines a smart contract and a frontend user interface**. On Ethereum, smart contracts are accessible and transparent – like open APIs – so your dapp can even include a smart contract that someone else has written.

Components of Ethereum Network

Overview :

- Vitalik Buterin, a programmer, proposed Ethereum in 2013. The network went live in 2015, with an initial supply of 72 million coins, after being crowdfunded in 2014.
- The Ethereum Virtual Machine (EVM) can run decentralized programs and execute scripts. Ethereum is used for decentralized banking, the production and distribution of non-fungible tokens (NFTs), and many ICOs.
- After Bitcoin, Ethereum is quoted as the second most prevalent crypto-currency. Unlike Bitcoin, Ethereum is proposed to be much more than simply a means of exchange or a store of value.
- Ethereum, on the other hand, refers to itself as a decentralized computer network based on blockchain technologies. Ethereum is built on top of a blockchain network. A blockchain is a transparent, distributed public ledger that verifies and records all

transactions. Everyone on the Ethereum network has an exact copy of this ledger, which allows them to view all previous transactions.

- The Ethereum network allows users to build and run apps, smart contracts, and other transactions. These features are not available in Bitcoin.
- It is only used as a medium of exchange and a store of cash. There is no boundary on how much Ether tokens can be produced while Bitcoin can only deliver 21 million coins.
- All, regardless of context or location, have access to digital money and data-friendly resources thanks to Ethereum. It's the technology that powers the ether (ETH) and thousands of other apps available today.
- The Ethereum Virtual Machine (EVM) is run by Ethereum clients, which may be built in any popular programming language.

Benefits of Ethereum client implementations :

There are several benefits to having so many Ethereum client implementations, including the following as follows.

1. It strengthens the network's bug resistance.
2. It keeps development resources from being centralized.
3. In general, team contests aid in the discovery of the best solutions to common and difficult problems.
4. In mining, prototyping, DApp development, and other areas, each customer may have a distinctive emphasis, strength, and weakness. DApp developers and private Ethereum blockchain operators may pick and choose which ones best suit their purposes.

Components of Ethereum Network :

Component-1:

Nodes –

There are two types of nodes in an Ethereum network. They are as follows.

1. **Mining Node –**
   These nodes are responsible for writing all the transactions that have occurred in the Ethereum network in the block.

2. **Ethereum Virtual Machine Node –**
   These are the nodes in the Ethereum network in which Smart Contracts (it is a type of contract between supporter and developer in which there are a set of rules based on which both the parties agree to interact with each other. The agreement will be automatically executed when the pre-defined rules are met.) are implemented. By default, this node utilizes a 30303 port number for the purpose of communication among themselves.

Component-2 :

Ether –

- Ether is a type of cryptocurrency used in the Ethereum network just like a bitcoin is used in a blockchain network. It is a peer-to-peer currency, similar to Bitcoin. It tracks and promotes each transaction in the network.
- It is the second-largest cryptocurrency in the world. The first one is Bitcoin. Other cryptocurrencies can be used to get ether tokens, but vice versa is not true.
- It means that ether tokens can't be interchanged by other cryptocurrencies to render computing power for Ethereum transactions. Ether is paid as a commission for any execution that affects the state in Ethereum.

- It is used in the Ethereum algorithm as an incentive for miners who connect blocks to the blockchain using a proof-of-work method.
- It is the only currency that can be used to pay transaction costs, which go to miners as well. The block reward, as well as transaction fees, provide miners with an opportunity to keep the blockchain rising.
- Aside from paying for transactions, ether is often used to purchase gas, which is used to pay for the computation of any transaction on the Ethereum network.

Component-3:

Gas –

- Gas is an internal currency of the Ethereum network. We need gas to run applications on the Ethereum network, much as we need gas to run a vehicle.
- To complete every transaction on the Ethereum network, a consumer must first make a payment—send out ethers—and the intermediate monetary value is known as gas.
- Gas is a unit of measurement on the Ethereum network for the computing power used to execute a smart contract or a transaction.
- The price of gas is very low compared to Ether. The execution and resource utilization costs are predetermined in Ethereum in terms of Gas units, called **gwei.**

Component-4:

Ethereum Accounts –

There are two types of Ethereum accounts. They are as follows.

1. **Externally owned account –**
   These accounts are used to store transactions.

2. **Contract account –**
   As the name itself suggests, these accounts store the details of Smart Contracts.

Component-5:

Nonce –

For externally owned accounts, nonce means the number of transactions via this account. For a contract account, nonce means the number of contracts generated via this account.

Component-6:

Storage Root –

It is the main root node of a Merkle tree. Hash of all details of the account is stored here. The root of the Merkle tree is the verification of all transactions.

Component-7:

Ethash –

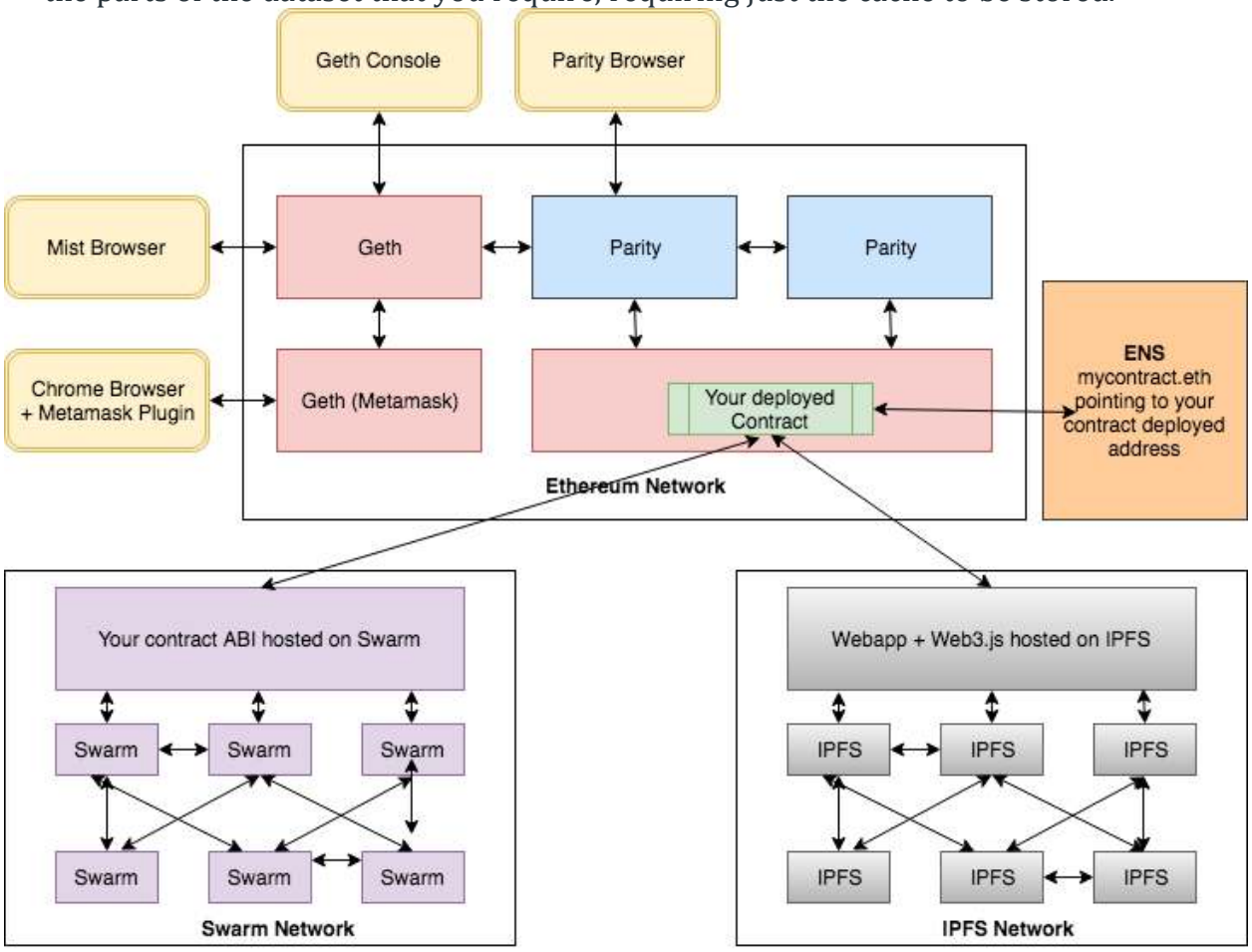
The intended PoW algorithm for Ethereum 1.0 is Ethash. It's the most recent version of Dagger-Hashimoto, however, it's no longer proper to call it that because many of the algorithms' initial characteristics have been dramatically altered in the previous month of study and development. The original version may be found here.

Algorithm:

The algorithm follows the following general path as follows.

1. There is a seed for each block that may be determined by reading over the block headers till that point.
2. A 16 MB pseudo-random cache may be computed from the seed. The cache is saved by light clients.
3. We can construct a 1 GB dataset from the cache, with the condition that each item in the dataset is dependent on just a few cache items. The dataset is stored by full clients and miners. The dataset expands linearly over time.

4. Taking random slices of the dataset and hashing them together is what mining is all about. Verification may be done with little memory by utilizing the cache to renew just the parts of the dataset that you require, requiring just the cache to be stored.



Ethereum Ecosystem

INTRODUCTION TO SMART CONTRACTS

WHAT IS A SMART CONTRACT?

A "smart contract" is simply a program that runs on the Ethereum blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the Ethereum blockchain.

Smart contracts are a type of Ethereum account. This means they have a balance and can be the target of transactions. However they're not controlled by a user, instead they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via the code. Smart contracts cannot be deleted by default, and interactions with them are irreversible.

Smart contracts are the fundamental building blocks of Ethereum applications. They are computer programs stored on the blockchain that allow converting traditional contracts into digital parallels.
Contracts are just agreements. That is, any form of agreement can be encapsulated within the conditions of a contract. Verbal agreements or pen-and-paper contracts are acceptable for many things, but they aren't without flaws.

Trust and contracts

One of the biggest problems with a traditional contract is the need for trusted individuals to follow through with the contract's outcomes.
Here is an example:
Alice and Bob are having a bicycle race. Let's say Alice bets Bob $10 that she will win the race. Bob is confident he'll be the winner and agrees to the bet. In the end, Alice finishes the race well ahead of Bob and is the clear winner. But Bob refuses to pay out on the bet, claiming Alice must have cheated.
This silly example illustrates the problem with any non-smart agreement. Even if the conditions of the agreement get met (i.e. you are the winner of the race), you must still trust another person to fulfill the agreement (i.e. payout on the bet).

Smart contracts

Smart contracts digitize agreements by turning the terms of an agreement into computer code that automatically executes when the contract terms are met.

A digital vending machine

A simple metaphor for a smart contract is a vending machine, which works somewhat similarly to a smart contract - specific inputs guarantee predetermined outputs.

- You select a product
- The vending machine returns the amount required to purchase the product
- You insert the correct amount
- The vending machine verifies you have inserted the correct amount
- The vending machine dispenses the product of choice

The vending machine will only dispense your desired product after all requirements are met. If you don't select a product or insert enough money, the vending machine won't give out your product.

Automatic execution

One of the most significant benefits smart contracts have over regular contracts is that the outcome is automatically executed when the contract conditions are realized. There is no need to wait for a human to execute the result. In other words: smart contracts remove the need for trust.

For example, you could write a smart contract that holds funds in escrow for a child, allowing them to withdraw funds after a specific date. If they try to withdraw the funds before the specified date, the smart contract won't execute. Or, you could write a contract that automatically gives you a digital version of a car's title when you pay the dealer.

Predictable outcomes

The human factor is one of the biggest points of failure with traditional contracts. For example, two individual judges may interpret a traditional contract in different ways. Their interpretations could lead to different decisions getting made and disparate outcomes. Smart contracts remove the possibility of different interpretations. Instead, smart contracts execute precisely based on the conditions written within the contract's code. This precision means that given the same circumstances, the smart contract will produce the same result.

Public record

Smart contracts are also useful for audits and tracking. Since Ethereum smart contracts are on a public blockchain, anyone can instantly track asset transfers and other related information. You can check to see that someone sent money to your address, for example.

Privacy protection

Smart contracts can also protect your privacy. Since Ethereum is a pseudonymous network (your transactions are tied publicly to a unique cryptographic address, not your identity), you can protect your privacy from observers.

Visible terms

Finally, like contracts, you can check what's in a smart contract before you sign it (or otherwise interact with it). Better yet, public transparency of the terms in the contract means that anyone can scrutinize it.

Ethereum Clients

An Ethereum client is **a software application that implements the Ethereum specification and communicates over the peer-to-peer network with other Ethereum clients**. Different Ethereum clients interoperate if they comply with the reference specification and the standardized communications protocols.

- Pantheon — Java client by PegaSys.
- Geth — Go client.
- Parity — Rust client.
- Aleth — C++ client.
- Pyethapp — Python client using pyethereum.
- Trinity — Python client using py-evm.
- Ethereumjs — JS client using ethereumjs-vm.
- Ethereumj — Java client by the Ethereum Foundation.

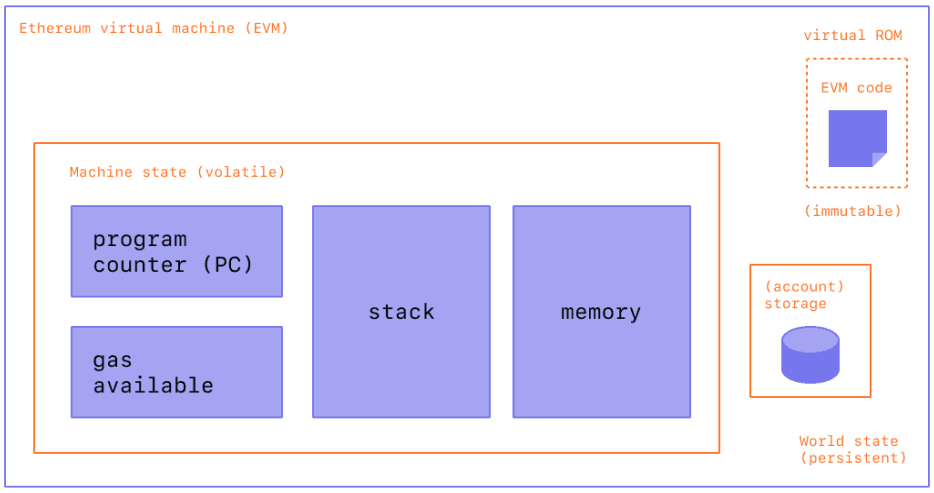
Geth is currently the most popular Ethereum client. It has the largest user base and offers a vast range of tools, written in Go, for both consumers and developers. Geth is open source and is licensed under the GNU LGPL v3.

J.P. Morgan and more than 300 banks use a version of Enterprise Ethereum to run an inter-bank payment network. The Covantis initiative, set up by a group of institutions in the commodity industry, uses Enterprise Ethereum to run a post-trade execution platform for agricultural shipping transactions.

ETHEREUM VIRTUAL MACHINE (EVM)

The EVM's physical instantiation can't be described in the same way that one might point to a cloud or an ocean wave, but it does *exist* as one single entity maintained by thousands of connected computers running an Ethereum client.

The Ethereum protocol itself exists solely for the purpose of keeping the continuous, uninterrupted, and immutable operation of this special state machine. It's the environment in which all Ethereum accounts and smart contracts live. At any given block in the chain, Ethereum has one and only one 'canonical' state, and the EVM is what defines the rules for computing a new valid state from block to block.



The analogy of a 'distributed ledger' is often used to describe blockchains like Bitcoin, which enable a decentralized currency using fundamental tools of cryptography. The ledger maintains a record of activity which must adhere to a set of rules that govern what someone can and cannot do to modify the ledger. For example, a Bitcoin address cannot spend more Bitcoin than it has previously received. These rules underpin all transactions on Bitcoin and many other blockchains.

While Ethereum has its own native cryptocurrency (Ether) that follows almost exactly the same intuitive rules, it also enables a much more powerful function: smart contracts. For this more complex feature, a more sophisticated analogy is required. Instead of a distributed ledger, Ethereum is a distributed state machine. Ethereum's state is a large data structure which holds not only all accounts and balances, but a *machine state*, which can change from block to block according to a pre-defined set of rules, and which can execute arbitrary machine code. The specific rules of changing state from block to block are defined by the EVM

Introducing Ethereum Script 2.0

Solidity programming

Solidity programming stands apart from the other programming languages and is the programming language of choice in Ethereum. Solidity is a brand-new programming

language developed by Ethereum, the second-largest cryptocurrency market by capitalization.