Understanding of Cryptocurrency creation process

M Tech I (Sem 2)
10 April 2023

Dhiren Patel

News today

- Bitcoin’s Energy Transparency
- Bitcoin mining as a contributor to the climate crisis? EWG - Change the Code, Not the Climate
- We see our energy use, really, as a feature of proof of work
- Regardless, the environmental footprint of Bitcoin mining has been well documented, in part because Bitcoin’s hashrate is public (this competition play out in front of everyone’s eyes creates a degree of transparency innate to Bitcoin mining—one that isn’t shared by the traditional financial system)

EWG Report

- In six case studies, Environment Working Group profiles how a cryptocurrency mining process known as “proof of work” can create air, climate, water, waste and noise pollution issues for those living nearby.
- By Anthony Lacey (EWG) and Jessica Hernandez (EWG)

GEORGIA

Adel

READ HERE

KENTUCKY

Paducah

READ HERE

MONTANA

Big Horn County

READ HERE

NEW YORK

Seneca Lake

READ HERE

NORTH CAROLINA

Cherokee County

READ HERE

PENNSYLVANIA

Venango County

READ HERE

Our take

- Energy costs for producing new Bitcoin are necessary for it to function as money
- Gold is costly to mine analogously, and that's also inherent to hard money
- the fiat currency system is much more harmful
- Miners give what would be wasted energy a new purpose, effectively storing it in cyberspace as Bitcoin!!!

Process

- Creating a cryptocurrency is a complex and multifaceted process that involves a deep understanding of blockchain technology, cryptography, and programming.
- E.g. Bitcoin mining reward (adding new coins in system) is programmed to decrease over time, with a maximum supply of 21 million coins expected to be reached sometime in the year 2140

How? What? Why?

- Determine the purpose and features of your cryptocurrency: Before creating a cryptocurrency, you need to decide on its purpose and the features you want to include. Will it be a medium of exchange or a store of value? What will be its supply limit? Will it be mineable or pre-mined? Will it have privacy features?
- Choose a consensus mechanism: The consensus mechanism determines how transactions are validated and added to the blockchain. The most common consensus mechanisms are Proof of Work (PoW) and Proof of Stake (PoS).

How?

- Develop the codebase: You will need to write the code for your cryptocurrency, including the blockchain, wallet, and any other features you have decided to include. You can choose to develop the codebase from scratch or fork an existing cryptocurrency like Bitcoin or Ethereum.
- Test and launch the network: Once you have developed the codebase, you will need to test it thoroughly to ensure that it works as intended. After testing, you can launch the network and start mining or distributing your cryptocurrency.
- Market your cryptocurrency: Marketing your cryptocurrency is an important step in gaining users and increasing its value. You can use social media, online forums, and other channels to promote your cryptocurrency and attract investors.

Bitcoin

- Receiving, Accumulating, Buying
- Sending, Spending
- A Bitcoin wallet address is a unique identifier that allows you to receive Bitcoin into your wallet.

receiving Bitcoin

- Obtain your Bitcoin address: In order to receive Bitcoin, you need to obtain your Bitcoin address from your Bitcoin wallet. This is a long string of letters and numbers that uniquely identifies your Bitcoin wallet. Most wallets also provide you with a QR-code version of your Bitcoin address
- Share your Bitcoin address: Once you have your Bitcoin address, you can share it with the sender. They can then use this address to send Bitcoin to your wallet.
- Wait for the transaction to confirm: Once the sender sends the Bitcoin to your address, the transaction will need to be confirmed by the Bitcoin network. This typically takes a few minutes to an hour, depending on network congestion.
- Check your wallet balance: Once the transaction is confirmed, the Bitcoin will be added to your wallet balance. You can check your wallet balance to verify that the Bitcoin has been received.

Check bitcoin balance in your wallet

- Find your Bitcoin address: In your Bitcoin wallet, find the Bitcoin address associated with your wallet. This is a long string of letters and numbers that uniquely identifies your Bitcoin wallet.
- Check your balance: Once you have your Bitcoin address, you can check your Bitcoin balance by entering it into a Bitcoin block explorer, such as blockchain.com or blockchair.com. These websites allow you to search for any Bitcoin address and see its transaction history and balance.
- Alternatively, some Bitcoin wallets may have a built-in balance checker that allows you to check your balance without leaving the wallet interface.

Who sums balance?

- Bitcoin balances are not "summed" in the traditional sense. Instead, the balance of a Bitcoin address is determined by the total value of all unspent transaction outputs (UTXOs) associated with that address.
- A UTXO represents the amount of Bitcoin that was received by a particular Bitcoin address earlier and has not yet been spent. When a Bitcoin transaction is sent, it typically consumes one or more UTXOs as inputs and creates one or more new UTXOs as outputs. The total value of the inputs must be greater than or equal to the total value of the outputs, and any excess value is typically paid as a transaction fee to miners.
- To determine the balance of a Bitcoin address, you need to sum the value of all unspent UTXOs associated with that address. This can be done using a Bitcoin block explorer, such as blockchain.com or blockchair.com, which allow you to search for any Bitcoin address and see its transaction history and balance.

Signing Transaction (Spend/Transfer)

- To sign a Bitcoin transaction, you need a Bitcoin wallet that supports transaction signing.
- 1 - Create a new transaction: Start by creating a new transaction with the details of the transaction you want to send. This typically involves specifying the recipient's address, the amount of Bitcoin to send, and any transaction fees.
- 2 - Input selection: The wallet will then select which unspent transaction outputs (UTXOs) to use as inputs for the transaction. These UTXOs represent the Bitcoin you have in your wallet that you can spend.

Signing Transaction

- Transaction fee estimation: The wallet will then estimate the transaction fee based on the current network congestion and the priority of your transaction.
- Review transaction details: Before signing the transaction, you should review the transaction details to ensure that everything is correct.
- Sign the transaction: Once you're satisfied with the transaction details, you can sign the transaction with your private key. The private key is used to prove ownership of the Bitcoin being sent and is required to sign the transaction.
- Broadcast the transaction: Finally, you can broadcast the signed transaction to the Bitcoin network.
- Once it's confirmed by the network, the Bitcoin will be sent to the recipient's address.

spending Bitcoin

- Obtain the recipient's Bitcoin address: To send Bitcoin, you need the recipient's Bitcoin address (wallet address). This is a long string of letters and numbers that uniquely identifies the recipient's Bitcoin wallet.
- Create a new transaction: Once you have the recipient's Bitcoin address, you can create a new transaction in your Bitcoin wallet.
- This typically involves specifying the recipient's address, the amount of Bitcoin to send, and any transaction fees.

Structure of Bitcoin Transaction

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1–9 bytes (VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1–9 bytes (VarInt)	Output Counter	How many outputs are included
Variable	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

Structure of Bitcoin Transaction (Output and Input)

Size	Field	Description
8 bytes	Amount	Bitcoin value in satoshis (10^{-8} bitcoin)
1-9 bytes (VarInt)	Locking-Script Size	Locking-Script length in bytes, to follow
Variable	Locking-Script	A script defining the conditions needed to spend the output

Size	Field	Description
32 bytes	Transaction Hash	Pointer to the transaction containing the UTXO to be spent
4 bytes	Output Index	The index number of the UTXO to be spent; first one is 0
1-9 bytes (VarInt)	Unlocking-Script Size	Unlocking-Script length in bytes, to follow
Variable	Unlocking-Script	A script that fulfills the conditions of the UTXO locking script.
4 bytes	Sequence Number	Currently disabled Tx-replacement feature, set to 0xFFFFFFFF

Fee

- Bitcoin transactions incur a small fee which is paid to the miners that confirm them. Transactions with higher fees attached to them are picked up sooner by miners (who optimize for profitability), so higher-fee transactions are more likely to be included in the next batch.
- Fees are measured in satoshis/byte. A satoshi is the smallest divisible unit of bitcoin, which is 0.00000001 BTC
- Each transaction is made up of data, which is measured in bytes – fee is proportional to length of transaction

Fees

- The default speed (“Fast”) is set to have your transaction confirmed most likely within the next three blocks (so less than 30 minutes).
- If you change it to “Fastest,” you’ll pay a higher fee and likely have your transaction confirmed in the next two blocks (so less than 20 minutes).
- Changing it to “Eco” will save you some money, but still result in your transaction most likely getting confirmed within the next six blocks, so generally less than 60 minutes.
- For advanced users, you also have the option of setting a custom fee.

BTC for high value transactions?

- Transaction fees are often significantly higher, Transaction times are significantly longer (Depending on the fees paid and the current level of network congestion, it takes anywhere from a few minutes to an hour for most Bitcoin transactions to confirm 'on chain')
- Bitcoin's use as a medium of exchange (on layer one) is currently restricted to higher value items where transaction times and costs are less consequential - like buying a car, boat, or house.
- Note that 'layer two' solutions like the Bitcoin Lightning Network solve scalability challenges by enabling 'off chain' transactions.
- This is similar to how the Visa/Mastercard network functions in that millions of small transactions can go through quickly while final settlement occurs in large batches at a later stage.

BTC Transfer

- When someone wants to send Bitcoin to your wallet, they enter your wallet address as the recipient.
- The Bitcoin network then verifies that the address is valid (How?) and that the sender has sufficient funds to send the amount specified.
- If the transaction is valid, the sender's Bitcoin wallet software will broadcast the transaction to the network, where it will be verified and added to the blockchain.

Bitcoin private key

- A private key is a secret code that is used to access and spend Bitcoin that is stored in a specific wallet address. It is a 256-bit long number that is randomly generated when you create a Bitcoin wallet.
- When you send Bitcoin to a wallet address, the transaction is recorded on the blockchain and the balance of that address is updated. To spend Bitcoin from that address, you must use the private key associated with that address to sign the transaction and prove that you are the owner of the Bitcoin.

Wallet

- Creating a cryptocurrency wallet involves several steps, depending on the type of wallet you want to create.

Bitcoin wallet address

- A Bitcoin wallet address is a unique identifier used to receive Bitcoin transactions. It is a string of alphanumeric characters that starts with either the number 1 or 3 and is typically 26-35 characters long. For example, a Bitcoin address might look something like this:
- 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Bitcoin wallet address

- There are different types of Bitcoin wallet addresses, including legacy addresses that start with the number 1, and newer Segregated Witness (SegWit) addresses that start with the number 3.
- Some wallets also support Bech32 addresses, which start with the letters "bc1".

Bitcoin wallet addresses

- Legacy addresses: These are the original Bitcoin addresses that start with the number 1. They are the most widely used type of address and are compatible with all Bitcoin wallets and exchanges. Transactions made with legacy addresses are larger in size and may require higher fees.
- Segregated Witness (SegWit) addresses: These addresses were introduced in 2017 to improve the scalability of the Bitcoin network. They start with the number 3 and offer lower transaction fees and faster confirmation times than legacy addresses. SegWit addresses are also compatible with legacy addresses, which means they can be used to send Bitcoin to both SegWit and legacy addresses.

Bitcoin wallet address types

- Bech32 addresses: These are newer Bitcoin addresses that start with "bc1". They are also known as native SegWit addresses and offer the lowest transaction fees and smallest transaction sizes. Bech32 addresses are not yet supported by all Bitcoin wallets and exchanges, but their adoption is increasing.
- In addition to these types of addresses, there are also multi-signature addresses, which require multiple signatures to authorize transactions, and Hierarchical Deterministic (HD) addresses, which allow users to generate an unlimited number of addresses from a single seed phrase.

ENS

- ENS stands for Ethereum Name Service.
- It is a decentralized domain name system built on the Ethereum blockchain that allows users to register human-readable domain names for their Ethereum addresses, smart contracts, and other services on the Ethereum network.
- With ENS, users can register a domain name like "myname.eth" and associate it with their Ethereum address or smart contract.
- This makes it easier for other users to send transactions to them without having to remember long and complicated Ethereum addresses.

ENS

- ENS uses a decentralized system of nodes to manage the registration and resolution of domain names. When a user registers a domain name, they pay a fee in Ether and the registration information is stored on the Ethereum blockchain. Other users can then use the ENS resolver to look up the Ethereum address associated with a domain name and send transactions to it.
- ENS also supports the use of subdomains, which allows users to create hierarchical domain structures for their Ethereum addresses and services. For example, a user could register "myname.eth" and then create subdomains like "wallet.myname.eth" and "dapp.myname.eth" for their Ethereum wallet and decentralized application, respectively.

Secp256k1 in Bitcoin

- SECP-256K1 is an important component of the Bitcoin network and is used extensively in the generation and verification of Bitcoin wallet addresses and transactions.
- In order to generate a Bitcoin address, a private key is first generated using a random number generator. This private key is then used to compute the corresponding public key on the SECP-256K1 curve.

In Bitcoin

- The public key is then hashed using the SHA-256 algorithm and the RIPEMD-160 algorithm to produce a Bitcoin address. This address is what is shared publicly in order to receive payments.
- When a Bitcoin transaction is sent, it is signed using the sender's private key, which is again used in combination with the SECP-256K1 curve to generate a digital signature. The recipient can then use the sender's public key to verify that the transaction was indeed signed by the owner of the sending address.

Secp256k1 – An elliptic curve

- SECP-256K1 is an elliptic curve commonly used in the field of cryptography. It is defined over the finite field of prime order 2^256-2^32-2^9-2^8-2^7-2^6-2^4-1, and it has been selected for use in a number of cryptographic applications, including Bitcoin and other cryptocurrencies.
- The SECP-256K1 curve is particularly well-suited for use in digital signatures, which are used to verify the authenticity and integrity of messages. The curve is also used in key exchange protocols, which are used to establish secure communication channels between parties.
- The "K" in "SECP-256K1" stands for "Koblitz," which refers to the specific type of elliptic curve used in this implementation. This curve was chosen for its efficient implementation and high level of security.

Crypto custodian

- Crypto custodians are companies that provide storage and security services for cryptocurrencies.
- Crypto custodians offer secure storage solutions for individuals and institutional investors who want to hold large amounts of cryptocurrencies but don't want to deal with the technical challenges and security risks associated with self-custody.
- They typically use advanced security measures such as multi-signature wallets, cold storage, and other physical and digital security protocols to protect clients' assets.
- Some popular crypto custodians include Coinbase Custody, BitGo, Gemini Custody, and Anchorage. These custodians typically charge a fee for their services

Wallets

- Choose the type of wallet: There are several types of cryptocurrency wallets, including software wallets, hardware wallets, and paper wallets. Each type has its own advantages and disadvantages, so it's important to choose the one that best suits your needs.
- Download or purchase the wallet software: If you're creating a software wallet, you'll need to download the wallet software from the developer's website. If you're creating a hardware wallet, you'll need to purchase the hardware device and follow the manufacturer's instructions for setting it up.

Wallets

- Install and configure the wallet: Once you have the wallet software or device, you'll need to install and configure it. This typically involves creating a new wallet address and setting a password to protect your funds.
- Backup your wallet: It's important to create a backup of your wallet in case you lose access to it. This can be done by writing down the seed phrase or private key associated with your wallet and storing it in a safe place.
- Fund your wallet: Once your wallet is set up and backed up, you can fund it by transferring cryptocurrency from an exchange or another wallet. To receive funds, you'll need to share your wallet address with the sender.

Hardware wallets

- Hardware wallets are designed to be secure against hacking and malware attacks, and can be disconnected from the internet when not in use to prevent remote access.
- Self-custody can be achieved through the use of a hardware wallet, which is a physical device that stores the private keys needed to access a cryptocurrency wallet.
- It requires keeping backup copies of private keys in a safe place, using strong passwords and two-factor authentication, and regularly updating security software

Cold wallet

- A cold wallet is a type of cryptocurrency wallet that is designed to store cryptocurrency offline, typically on a hardware device that is not connected to the internet. Cold wallets are also known as cold storage or offline wallets, and are considered to be the most secure way to store cryptocurrencies.
- The key advantage of a cold wallet is that it is not connected to the internet, which means that it is not vulnerable to online hacking or malware attacks. Instead, the wallet is typically a physical device that can be plugged into a computer or mobile device when needed to perform transactions.

Cold wallet examples

- Ledger Nano S: The Ledger Nano S is a popular hardware wallet that supports a variety of cryptocurrencies, including Bitcoin, Ethereum, and more. It is a small USB device that can be plugged into a computer or mobile device when needed to perform transactions.
- Trezor: Trezor is another popular hardware wallet that supports a variety of cryptocurrencies, including Bitcoin, Ethereum, Litecoin, and more. It is a small, key-shaped device that can be plugged into a computer or mobile device when needed.
- KeepKey: KeepKey is a hardware wallet that supports a variety of cryptocurrencies, including Bitcoin, Ethereum, Litecoin, and more. It has a large, easy-to-read screen and is designed to be user-friendly and intuitive.
- Coldcard: Coldcard is a hardware wallet specifically designed for Bitcoin and other cryptocurrencies. It is an open-source device that offers advanced security features, including multi-signature support and air-gapped transactions.

ColdCardMK4, Ledger Nano X, Trezor, KeepKey

Hot wallet

- A hot wallet is a type of cryptocurrency wallet that is designed to be connected to the internet, typically through a computer or mobile device. Hot wallets are also known as online wallets, and they are the most convenient way to store and access cryptocurrencies.
- There are several types of hot wallets available, including desktop wallets, mobile wallets, and web wallets.
- However, because hot wallets are connected to the internet, they are more vulnerable to hacking and other types of security breaches.

Hot wallet examples

- MetaMask: MetaMask is a web-based wallet that allows users to store and manage Ethereum and other ERC-20 tokens directly from their web browser.
- Coinbase Wallet: Coinbase Wallet is a popular mobile wallet app that allows users to store and manage a variety of cryptocurrencies, including Bitcoin, Ethereum, Litecoin, and more.
- Exodus: Exodus is a desktop wallet application that supports a variety of cryptocurrencies, including Bitcoin, Ethereum, Litecoin, and more.
- MyEtherWallet: MyEtherWallet is a web-based wallet that allows users to store and manage Ethereum and other ERC-20 tokens.

Wallet types - more

- Software wallets: These are applications that you install on your computer or mobile device to store your Bitcoin. Examples of popular software wallets include Electrum, Exodus, and Mycelium.
- Web wallets: These are online services that allow you to create and manage a Bitcoin wallet through a web browser. Examples of popular web wallets include Coinbase, Blockchain.com, and BitGo.
- Hardware wallets: These are physical devices that store your Bitcoin offline and are considered one of the most secure ways to store Bitcoin. Examples of popular hardware wallets include Ledger, Trezor, and KeepKey.
- Paper wallets: These are physical printouts that contain your Bitcoin address and private key. They are considered a more secure way to store Bitcoin compared to software wallets, as they are not susceptible to hacking or malware attacks. However, they are also less convenient to use and require more care to ensure their security.

steps to get a Bitcoin wallet address

- Choose a type of wallet: There are several types of Bitcoin wallets, including software wallets, web wallets, hardware wallets, and paper wallets. Each type has its own pros and cons, so it's important to choose one that fits your needs and priorities.
- Set up your wallet: Once you have chosen a wallet, follow the instructions provided by the wallet provider to set up your wallet account. This typically involves creating a username and password and providing basic personal information.
- Generate a new Bitcoin address: Once your wallet account is set up, you can generate a new Bitcoin address by clicking on the "Receive" or "Deposit" button in your wallet. This will generate a unique Bitcoin address that you can use to receive Bitcoin from others.
- Share your Bitcoin address: To receive Bitcoin from others, simply share your Bitcoin address with them. You can do this by copying and pasting the address, or by scanning a QR code if your wallet supports it.
- Keep your private key secure: Remember that your private key is what allows you to access and spend your Bitcoin, so it's important to keep it secure and never share it with anyone else.

steps to generate a Bitcoin wallet using a software wallet

- Choose a software wallet: There are several software wallets available, such as Electrum, Exodus, and Mycelium. Choose one that is compatible with your device and suits your needs.
- Download and install the software: Once you have chosen a software wallet, download and install it on your computer or mobile device.
- Create a new wallet: Once the software is installed, open the application and follow the instructions to create a new wallet. This typically involves choosing a username and password and setting up your security preferences.
- Generate a new Bitcoin address: Once your wallet is set up, you can generate a new Bitcoin address by clicking on the "Receive" or "Deposit" button in your wallet. This will generate a unique Bitcoin address that you can use to receive Bitcoin from others.
- Backup your wallet: To protect your Bitcoin and ensure that you can access it even if you lose your device, it's important to backup your wallet. Follow the instructions provided by your wallet provider to backup your wallet and keep the backup in a secure location.
- Keep your private key secure: Remember that your private key is what allows you to access and spend your Bitcoin, so it's important to keep it secure and never share it with anyone else.

a Bitcoin wallet using an online wallet generator

- Go to the Bitaddress.org website.
- Move your mouse around the screen to generate randomness for the wallet generation process.
- Click on the "Paper Wallet" tab.
- Choose the number of addresses you want to generate.
- Choose the "BIP38 Encrypt" option if you want to password protect your private key. This is optional, but highly recommended.
- Click the "Generate" button.
- Print out your paper wallet, making sure to keep it in a secure location where no one else can access it.
- You can also save a digital copy of the wallet by clicking on the "paper wallet" button and saving it as a PDF.

More – paper wallet

- Generate a new Bitcoin address and private key: You can use a service like bitaddress.org to generate a new Bitcoin address and private key pair. Make sure to do this on an offline computer to ensure that your private key remains secure.
- Print out the address and private key: Once you have generated a new Bitcoin address and private key pair, print them out on a piece of paper. Make sure to print multiple copies and store them in separate locations to ensure that you have backups in case one is lost or damaged.
- Transfer Bitcoin to your paper wallet: To transfer Bitcoin to your paper wallet, simply send it to the public address listed on the printout. Keep in mind that paper wallets are not as convenient as other forms of wallets, as you will need to manually enter your private key to spend your Bitcoin.
- Keep your paper wallet secure: Make sure to keep your paper wallet in a secure location and protect it from damage, theft, or unauthorized access. It's also a good idea to periodically transfer your Bitcoin to a more secure type of wallet, such as a hardware wallet.

Bitcoin forks

- Bitcoin forks are changes to the Bitcoin network that create a new blockchain with a different set of rules from the original Bitcoin blockchain.
- Soft forks: A soft fork is a backward-compatible upgrade to the Bitcoin network that does not result in a new cryptocurrency being created. Soft forks occur when the majority of the Bitcoin network's hash power and nodes adopt a new set of rules, such as a change in the block size limit or the introduction of a new transaction type.

Hard forks

- Hard forks: A hard fork is a permanent divergence from the original Bitcoin blockchain that creates a new cryptocurrency. Hard forks occur when a group of developers and miners decide to create a new blockchain with different rules from the original Bitcoin blockchain, often as a result of disagreements over the direction of the Bitcoin network.
- It's important to note that when a hard fork occurs, Bitcoin holders are typically given an equal amount of the new cryptocurrency associated with the fork.

Bitcoin hardforks

- Bitcoin Cash (BCH): A hard fork of Bitcoin that occurred in August 2017, with a larger block size limit of 8 MB compared to Bitcoin's 1 MB limit.
- Bitcoin Gold (BTG): A hard fork of Bitcoin that occurred in October 2017, with a different mining algorithm designed to be more ASIC-resistant and accessible to more people.
- Bitcoin SV (BSV): A hard fork of Bitcoin Cash that occurred in November 2018, with a larger block size limit of 128 MB and a focus on scaling and enterprise use cases.

Ethereum Forks

- Ethereum Classic (ETC): The first and most well-known Ethereum fork occurred in 2016 after the DAO hack, which resulted in the theft of millions of dollars worth of Ether. To fix the problem, a hard fork was implemented that returned the stolen funds to their owners. However, some members of the Ethereum community disagreed with this decision and continued to use the original Ethereum blockchain, which became Ethereum Classic.
- Byzantium and Constantinople: These were two separate upgrades to the Ethereum network that were implemented through soft forks in 2017 and 2019, respectively. They introduced several improvements to the network, including lower transaction fees and faster block confirmation times.

Ethereum forks

- Ethereum 2.0: This is a major upgrade to the Ethereum network that is currently underway. It aims to improve the network's scalability, security, and sustainability by transitioning from a proof-of-work consensus algorithm to a proof-of-stake algorithm. Ethereum 2.0 is being implemented through a series of hard forks, with the first one, known as the Beacon Chain, launching in December 2020.

EIP

- EIP stands for Ethereum Improvement Proposal. An EIP is a proposal for changes or improvements to the Ethereum network's protocol or its underlying technologies.
- EIPs are used to propose new features, standards, or protocols that can be implemented in the Ethereum network.
- EIPs can be submitted by anyone, including developers, users, and other stakeholders in the Ethereum community. EIPs go through a rigorous review process before being accepted and implemented on the Ethereum network.

Important EIPs

- EIP-20 (ERC-20) (2015): This EIP introduced the standard for creating tokens on the Ethereum network. The ERC-20 standard has become the most widely used token standard in the Ethereum ecosystem and has enabled the creation of countless new tokens.
- EIP-1559 (2021): This EIP introduced a new fee structure for Ethereum transactions that aims to make the network more efficient and user-friendly. The new fee structure includes a base fee that is burned (destroyed) instead of going to miners as a transaction fee, which helps to reduce the overall supply of Ethereum and potentially increase its value.

Important EIPs

- EIP-721 (ERC-721) (2018): This EIP introduced the standard for non-fungible tokens (NFTs) on the Ethereum network. NFTs have become increasingly popular and are used to represent unique digital assets such as artwork, collectibles, and in-game items.
- EIP-155 (2016): This EIP introduced a standardized way to encode transaction data on the Ethereum network, which helps to prevent replay attacks and other security vulnerabilities.
- EIP-196 and EIP-197 (2017): These EIPs introduced precompiled contracts for modular exponentiation and elliptic curve operations, respectively. These precompiled contracts help to improve the efficiency of certain types of transactions on the Ethereum network.

Ethereum Difficulty Bomb

EIP-3554 (2021), which proposes to delay the "difficulty bomb" on the Ethereum network for another 12 months. The difficulty bomb is a mechanism that increases the difficulty level of mining on the Ethereum network over time, eventually making it so difficult that mining becomes impossible. The purpose of the difficulty bomb is to incentivize the network to transition from proof-of-work to proof-of-stake consensus algorithm. EIP-3554 delays the difficulty bomb to December 2022 to allow more time for the transition to proof-of-stake.

EIP

- EIP-1551 (2022): This introduced a new mechanism for compensating miners for the gas fees they collect. Instead of receiving the full amount of gas fees, miners receive a portion of the fees as a "base reward," which is paid out of the network's inflationary block rewards.
- Each EIP has contributed to the evolution of the Ethereum ecosystem in its own way, and the process continues to evolve as new challenges and opportunities arise

timeline of the EIP process

- Proposal: Anyone can submit an EIP proposal on the Ethereum GitHub page. The proposal should include a description of the proposed change, its rationale, and any relevant technical details.
- Draft: The proposal is reviewed and discussed by the Ethereum community on GitHub and other forums. The proposal may be revised based on feedback from the community.
- Accepted: If the proposal gains enough support from the community, it may be accepted as an official EIP. The proposal will be assigned a number and added to the official EIP repository.
- Finalized: Once an EIP has been accepted, it will go through a final review and testing process to ensure that it is safe and effective. The EIP may be revised again based on the results of this testing.
- Implemented: If the EIP passes the final review and testing process, it may be implemented on the Ethereum network as part of a software upgrade or hard fork.

BIP

- BIP stands for Bitcoin Improvement Proposal. It is a standard process used by the Bitcoin community to propose and implement changes to the Bitcoin protocol or network. The BIP process is used to ensure that proposed changes are well-documented, well-understood, and well-supported by the Bitcoin community before they are implemented.
- Standards Track BIPs: These propose changes to the Bitcoin protocol, such as changes to the consensus rules, transaction format, or block size limit.
- Informational BIPs: These provide information or guidelines for the Bitcoin community, such as best practices for wallet development or recommendations for network security.
- Process BIPs: These propose changes to the BIP process itself, such as updates to the BIP format or changes to the way BIPs are reviewed and accepted.

Important BIPs examples

- BIP 32: Hierarchical Deterministic Wallets - This proposal introduced a standard for creating deterministic wallets, which allows for the creation of child keys from a single master key.
- BIP 39: Mnemonic code for generating deterministic keys - This proposal introduced a standard for generating a mnemonic phrase (a sequence of words) from a random set of numbers, which can be used to generate a set of deterministic keys.
- BIP 44: Multi-Account Hierarchy for Deterministic Wallets - This proposal introduced a standard for organizing multiple cryptocurrency accounts within a single deterministic wallet.
- BIP 141: Segregated Witness - This proposal introduced a way to separate the signature data from transaction data, which increases the efficiency of Bitcoin's block size limit.

Important BIPs

- BIP 148: User Activated Soft Fork - This proposal was created to address concerns around the centralization of Bitcoin mining and the potential for a hard fork. It proposed a mechanism for users to activate a soft fork, which would require a supermajority of miners to support it.
- BIP 174: Partially Signed Bitcoin Transactions (PSBT) - This proposal introduced a standard for creating partially signed transactions, which allows multiple parties to collaboratively create and sign a single transaction.
- BIP 340, BIP 341, and BIP 342: Schnorr Signatures, Taproot, and Tapscript - These three proposals are part of a larger upgrade to Bitcoin known as the Taproot/Schnorr upgrade. They introduce new cryptographic tools to improve privacy, security, and efficiency on the Bitcoin network.

Taproot (2021)

- Taproot is a proposed Bitcoin protocol upgrade that aims to improve privacy, security, and efficiency on the network. It is a combination of three Bitcoin Improvement Proposals (BIPs): BIP 340, BIP 341, and BIP 342.
- The main feature of Taproot is the introduction of Schnorr signatures, a new cryptographic tool that allows for more efficient transaction signing and greater privacy.
- Schnorr signatures are more compact than the current signature algorithm (ECDSA), which reduces the size of transactions and the fees needed to broadcast them.

Taproot

- Tapscript allows for more complex smart contracts to be created on the Bitcoin network while maintaining privacy and scalability.
- Taproot introduces a new output type called the "pay-to-taproot" (P2TR) output. P2TR outputs are a form of Bitcoin address that allows users to hide the complexity of their transactions while maintaining privacy. They also allow for more efficient use of block space and reduce the fees associated with broadcasting transactions.

Bitcoin private key and public key

- Bitcoin private keys and public keys are two critical components of the Bitcoin cryptographic system that allow users to securely store and transfer their Bitcoin.
- A Bitcoin private key is a 256-bit number that is generated by a Bitcoin wallet when a user creates a new account. This private key is used to sign transactions and prove ownership of Bitcoin associated with that account.
- The public key is often represented as a Bitcoin address, which is a shorter and more user-friendly string of characters that is derived from the public key. Bitcoin addresses typically start with a "1" or "3" and are used as the destination for Bitcoin transactions.

generating a private key

- The process of generating a private key involves the following mathematical operations:
- Choose a random number as the private key. The private key is a 256-bit number, which means that there are 2^256 possible private keys.
- Use the private key to calculate the corresponding public key using the secp256k1 elliptic curve algorithm. This algorithm involves multiplying a point on the curve by the private key, resulting in a point on the curve that represents the public key.
- Use a one-way cryptographic hash function, such as SHA-256 or RIPEMD160, to convert the public key into a Bitcoin address.
- Bitcoin wallets use a process called hierarchical deterministic (HD) key generation to generate a sequence of private keys from a single "seed" value.

Public key in Bitcoin

- In Bitcoin, a public key is a unique identifier that is derived from a private key using elliptic curve cryptography
- To spend Bitcoin, the owner of the public key must use their associated private key to sign the transaction and prove ownership of the Bitcoin.
- A Bitcoin address is a shorter version of the public key that is easier for humans to read and share. It is derived from the public key using a process called Base58Check encoding.

generating a Bitcoin wallet address

- Generate a public key using the private key and the secp256k1 elliptic curve algorithm. This results in a point on the curve that represents the public key.
- Apply a one-way hash function, such as SHA-256 or RIPEMD160, to the public key. This generates a unique hash value that is used to create the Bitcoin address.
- Apply a checksum to the hash value to ensure that the address is valid and has not been modified or corrupted.
- Encode the checksum and hash value into a Bitcoin address format using base58 encoding, which is a modified version of the Base64 encoding scheme.

Base 58 - a binary-to-text encoding scheme

- Base58 encoding works by first converting the binary data into a large integer. The integer is then converted into a Base58 string by repeatedly dividing it by 58 and appending the remainder to the output string. The process continues until the integer is reduced to zero.
- The characters used in Base58 encoding are typically chosen to avoid ambiguous characters like 0 (zero), O (capital letter o), l (lowercase L), and I (capital letter i) that can be easily confused with each other. In addition, some characters like + (plus) and / (slash) that are used in Base64 encoding are also excluded to further improve readability and avoid confusion with special characters in URLs.
- Overall, Base58 encoding provides a reliable and efficient way to represent binary data as a human-readable string, making it an important tool in the world of cryptocurrencies
- When a wallet address is encoded in Base58, it is shortened and made more readable for humans. E.g. 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

Algorithms used in Bitcoin

- ECC - secp256k1 elliptic curve algorithm
- Hash - SHA-256
- Hash – RIPEMD-160 (Short)
- Base58 (Short)
- HD (Hierarchical Deterministic) (Wallets) - HD wallets use a deterministic algorithm to generate a sequence of private and public keys from a single seed value. The seed value is typically a randomly generated 128-256 bit number that is converted into a mnemonic phrase for easier backup and restoration.
- Merkle Trees: In Bitcoin, Merkle trees are used to create a hash of all the transactions in a block, which is included in the block header.

Bitcoin block

- A Bitcoin block is a collection of transactions that have been validated by miners and added to the Bitcoin blockchain.
- When a block is added to the blockchain, it serves as a permanent record of all the transactions that occurred within it.
- The block is also linked to the previous block in the blockchain, creating an unbreakable chain of blocks that form the backbone of the Bitcoin network.
- In addition to containing transaction data, Bitcoin blocks also contain a nonce value that is used in the proof-of-work algorithm to validate the block.

Bitcoin mining

- The mathematical computations involved in Bitcoin mining are designed to be computationally difficult and energy-intensive to prevent malicious actors from gaining control of the network.
- The difficulty level and nonce value are adjusted regularly to ensure that new blocks are generated at a consistent rate and that the network remains secure.
- The proof of work system ensures that miners must invest significant computational power and energy consumption to validate transactions and generate new blocks, providing a secure and decentralized system for managing the Bitcoin network.

Bitcoin Mining

- 1 - Hashing: Bitcoin mining begins with the creation of a block header, which contains information about the previous block, the timestamp of the current block, and a list of transactions. This block header is then hashed using the SHA-256 algorithm to create a 256-bit hash value.
- 2 - Difficulty: The hash value generated in step 1 must meet a certain difficulty level to be considered valid. The difficulty level is adjusted every 2016 blocks to ensure that blocks are generated at a consistent rate.
- 3 - Nonce: To find a valid hash value, miners change a small piece of data in the block header called the nonce. The nonce is a 32-bit integer that is incremented with each attempt to find a valid hash value.

Bitcoin Mining

- Brute Force: Miners use a brute force approach to find a valid hash value. They repeatedly hash the block header with different nonce values until a valid hash value is found. This process requires significant computational power and energy consumption.
- Proof of Work: When a valid hash value is found, it is broadcast to the network as a proof of work. Other nodes on the network can easily verify the proof of work by hashing the block header with the same nonce value and checking that the resulting hash value meets the difficulty level.
- Summary - Bitcoin mining involves complex mathematical computations that are used to validate transactions, secure the network, and generate new blocks of transactions.

Mining difficulty

- Bitcoin mining difficulty is a measure of how difficult it is to find a valid block hash that meets the network's target difficulty. The target difficulty is adjusted every 2016 blocks, or approximately every two weeks, to maintain an average block time of 10 minutes.
- The difficulty adjustment is based on the total computational power, or hash rate, of the Bitcoin network. If the hash rate increases, the network will adjust the target difficulty upwards to maintain an average block time of 10 minutes. Conversely, if the hash rate decreases, the network will adjust the target difficulty downwards to maintain an average block time of 10 minutes.
- The Bitcoin mining difficulty is measured in hashes per second, or the number of calculations that a miner can perform in one second. As the difficulty increases, miners need to invest more computational power and energy consumption to find a valid block hash, which can make mining less profitable.