

Bitcoin and Crypto Currencies (17 April 2023, 24 April 2023)

- *BTC and Environment
- *Shanghai upgrade (Eth2)
- *Bitcoin, CEX/DEX, Hacks and DeFi
- *Crypto Currency Programs

Dhiren Patel

ETH Holds Steady Post-Shanghai upgrade, Defying (Selling) Expectations

Summary

- ETH's price was remarkably stable in the minutes following Ethereum's historic, successful Shanghai upgrade, which enabled withdrawals of staked ETH.
- The successful implementation of Ethereum's historic Shanghai upgrade, happened on Wednesday evening (April 12, 2023) enabled the withdrawal of staked ETH by the network's participants.

Background

- Staking officially kicked off with the launch of the Beacon Chain in December 2020, which allowed ether, the native token of the Ethereum network, to be staked. To become a validator on Ethereum, users have invested 32 ETH at least each.
- The fact that the upgrade (April 2023) would permit tens of billions of ETH to be withdrawn, sold, and flood the market
- ETH did not drop sharply in price following Shanghai's successful implementation, as was widely expected.
- The price of ETH remained largely unchanged (close to USD 1900).

Background

- In September 2022, the merge event transitioned Ethereum to proof of stake.
- Despite the event's remarkable technical success, ETH plummeted some 8% immediately following the news, as traders offloaded their positions.
- Shanghai, while certainly significant to the Ethereum ecosystem, appears to have avoided making the same impact on ETH.
- The upgrade completed Ethereum's shift to a proof of stake network by enabling the withdrawal of staked ETH from the network. Previously, the \$35 billion worth of ETH deposited with Ethereum had been locked up and inaccessible since May 2021.

May be

- The majority of staked ETH has been deposited with Ethereum via intermediary staking pools and centralized crypto exchanges, many of which issue staking tokens to customers.
- Most people have been able to sell [staked ETH] for quite some time, because the majority of ETH is being staked through platforms with liquid staking programs, like Lido or Rocket Pool.
- In the five days preceding the merge (Sept 2022), ETH's price dropped 10%. It would go on to drop another 15% in the days following. In the five day leading up to Shanghai, however, ETH climbed up 3%.

ETH 2

- Ethereum 2.0 or ETH2 is a multi-phased upgrade that attempts to improve the Ethereum network's scalability and security by making infrastructure modifications, notably switching from a proof-of-work (PoW) to a proof-of-stake (PoS) consensus process.
- Necessity - The Ethereum (ETH) network was overburdened, forcing transaction costs to skyrocket to prohibitively expensive levels for many use cases. This was partly due to the success of DeFi projects, where consumers were willing to pay high transaction fees due to the tremendous financial value of the transactions.

ETH2

- Transaction fees are "gas" costs in Ethereum because they fund actual applications operating on the Ethereum blockchain rather than just transactions.
- Non-finance DApps (decentralized applications developed on top of Ethereum) find it challenging to run on Ethereum due to high gas fees.
- To address these issues, the Ethereum Foundation has been working on a network upgrade (ETH2 – now rebranded as “Consensus Layer”) that attempts to improve the security, speed, efficiency and scalability of the Ethereum network.

PoW (Eth1) to PoS (ETH2)

- On a PoS blockchain, staking is the process of actively participating in transaction validation (similar to mining). Anyone with the minimum necessary cryptocurrency balance can validate transactions and earn staking rewards on these blockchains.
- Eth1 PoW was capable of handling about 15 transactions per second, which is relatively slow in the context of financial transactions.
- Proof-of-stake, on the other hand, is expected to enable the processing of 100,000 transactions per second, considerably expanding the breadth of projects and applications that can be built on the Ethereum blockchain.

Process

- The PoS-powered blockchain bundles 32 blocks of transactions during each round of validation, which lasts on average 6.4 minutes. "Epochs" are the names given to these groups of blocks.
- When the blockchain adds two additional epochs after it, it is considered irreversible i.e., an epoch is considered finalized.
- The Beacon Chain divides stakers into 'committee' of 128 and randomly assigns them to a specific shard block. Each committee is allotted a 'slot' and has a set time to propose a new block and validate the inside transactions. Each epoch has 32 slots, requiring 32 sets of committees to complete the validation process.
- Once a committee has been assigned to a block, one member at random is given the exclusive power to propose a new block of transactions. In contrast, the remaining 127 members vote on the proposal and attest to the transactions.

Sharding

- In Ethereum 2.0 (Eth2), a shard refers to a smaller blockchain network that operates in parallel with the main Ethereum chain, also known as the Beacon Chain. The goal of sharding is to improve the scalability and performance of the Ethereum network by dividing the workload among multiple shards.
- Each shard will be responsible for processing a subset of transactions and smart contracts, reducing the amount of data that needs to be processed by each validator on the network.
- Each shard would have its state, which would include a distinct set of account balances and smart contracts.
- The Beacon Chain collects state information from shards and distributes it to neighbouring shards, keeping the network in sync.
- The validators will be managed by the Beacon Chain, which will handle everything from registering their stake contributions to awarding rewards and punishments.

Bears proved wrong

- Currently up almost 6% over the past 24 hours, with ETH trading hands at around \$1,980
- The successful execution of the Shanghai upgrade finally allowed Ethereum stakers to withdraw their holdings since staking first kicked off in December 2020.
- Prior to Shanghai, however, these validators weren't allowed to withdraw from the network nor collect any accumulated awards. This led to widespread speculation that the ability to finally withdraw funds would incite a bearish impulse on the network.

Eth2

- many validators have indeed made their exit, taking with them their staked Ethereum and rewards as they leave. Over the past 24 hours, there has been a net exit of more than 84,500 ETH
- But based on current price performance, it doesn't appear that the newly-unlocked Ethereum is being sold on the open market

17 April 2023

- BTC price today – 30,000+ USD
- ETH price today – 2100+ USD
- Long Crypto Winter is getting over!!

Bitcoin, Energy consumption and Environment effects

([Talk@IIT](#) Hyd, 13 April 2023)

Dr Dhiren Patel

NIT Surat

Bitcoin - Cryptocurrency

- Bitcoin is a Cryptocurrency.
- It works through a process called crypto mining. Mining is a process of solving a computational puzzle and storing the transactions into a blockchain.
- Bitcoin use a proof-of-work consensus mechanism that needs substantial calculation power, and energy, to obtain the right to update the transaction trail
- Besides the actual mining part, the maintenance and security aspect of crypto also involves a lot of energy.

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) - (March 2023)



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](#)

BTC today (17 April)

30,034.10 USD

+ Follow

+2,648.20 (9.67%) ↑ past month

17 Apr, 5:19 am UTC · [Disclaimer](#)









1D | 5D | 1M | 6M | YTD | 1Y | 5Y | Max



BTC – all time



Crypto currencies – KPI (17 April)

#	Name	Price	1h %	24h %	7d %	Market Cap 	Volume(24h) 	Circulating Supply 
1	 Bitcoin BTC Buy	\$30,013.50	▲0.10%	▼1.04%	▲6.06%	\$580,711,418,018	\$14,719,057,101 491,067 BTC	19,348,343 BTC <div><div></div></div>
2	 Ethereum ETH Buy	\$2,102.43	▲0.18%	▲0.25%	▲12.95%	\$251,102,599,382	\$8,931,500,508 4,259,465 ETH	119,434,715 ETH
3	 Tether USDT	\$1.00	▲0.04%	▼0.02%	▲0.01%	\$80,979,923,798	\$27,578,152,517 27,563,523,148 USDT	80,931,811,952 USDT
4	 BNB BNB Buy	\$347.56	▲0.16%	▲4.13%	▲11.04%	\$54,172,777,742	\$1,034,498,120 2,986,418 BNB	155,865,652 BNB
5	 USD Coin USDC	\$0.9998	▲0.03%	▼0.00%	▼0.01%	\$31,823,761,917	\$4,251,839,275 4,252,929,259 USDC	31,831,484,461 USDC

Energy consumption

- As puzzle difficulty increases, energy consumption will also increase. This makes cryptocurrency bad for long-term sustainability as energy consumed has to keep up with the increasing computing power required, maintaining the solving processes, and security as users also grow in numbers.
- Although cryptocurrency consumes a lot of energy, it has already included the whole currency system with no added real-life energy consumption from physical branches, buildings, bills, and even human resources.

Energy consumption

- As puzzle difficulty increases, energy consumption will also increase. This makes cryptocurrency bad for long-term sustainability as energy consumed has to keep up with the increasing computing power required, maintaining the solving processes, and security as users also grow in numbers.
- Although cryptocurrency consumes a lot of energy, it has already included the whole currency system with no added real-life energy consumption from physical branches, buildings, bills, and even human resources.

Banking system

- Like cryptocurrency, traditional banks also consume energy to run their virtual and physical transactions.
- The virtual transactions include the central server and digital security. Whereas the physical transactions involve branches, ATMs; also consider the requirements for each branch, for example, air conditioning, employee, computers, etc.
- Additionally, traditional banks also use physical currencies such as coins and bills. Many resources are required besides energy, such as metals, ink, cotton, etc.

The Cambridge Bitcoin Electricity Consumption Index (CBECI)

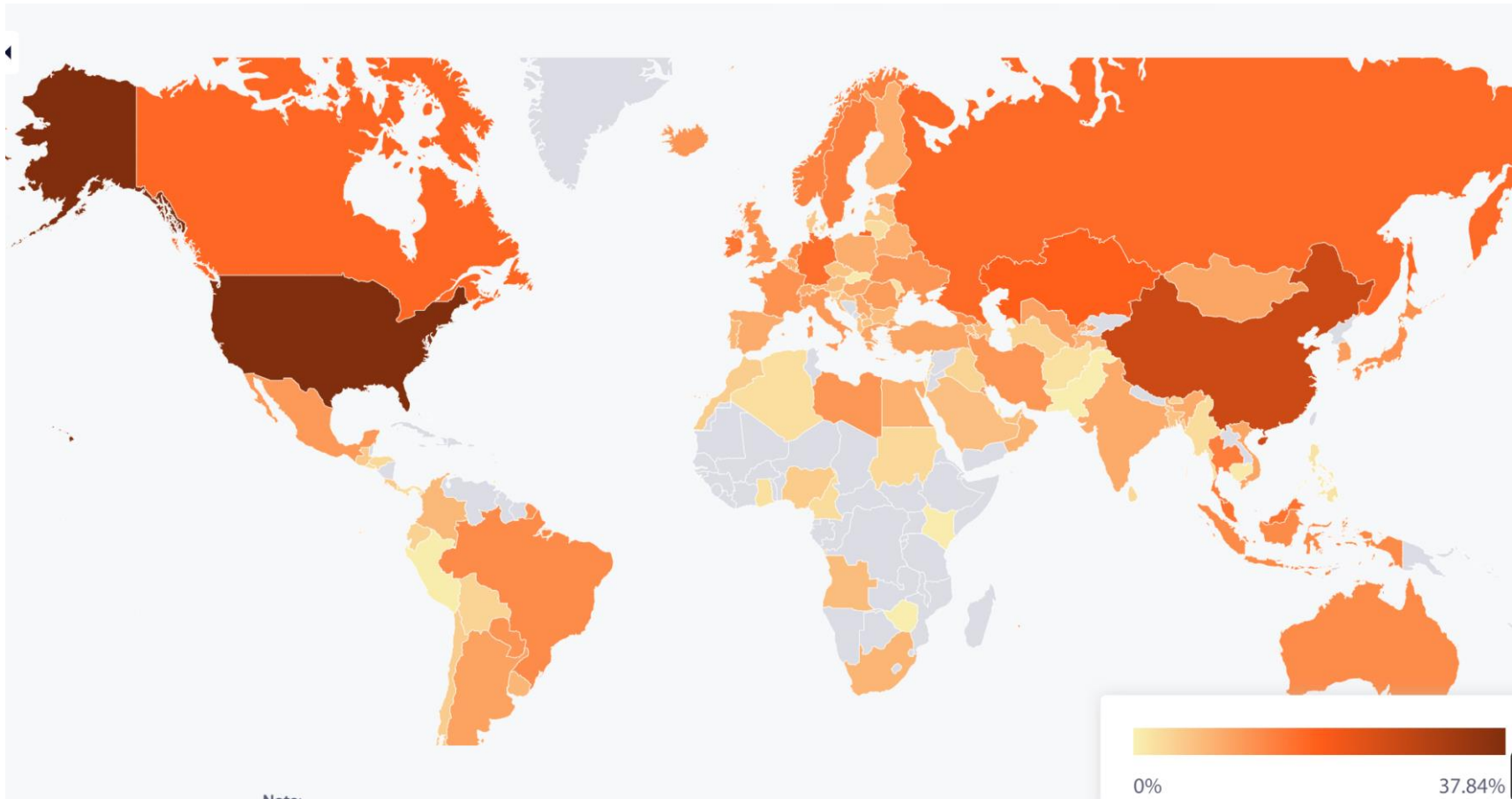
- provides an up-to-date estimate of the Bitcoin network's daily electricity load
- The underlying techno-economic model is based on a bottom-up approach that uses the profitability threshold of different types of mining equipment as the starting point.
- The first number refers to the total **electrical power** consumed by the Bitcoin network and is expressed in gigawatts (GW)
- The second number refers to the total **yearly electricity consumption** of the Bitcoin network and is expressed in terawatt-hours (TWh).

Trivia

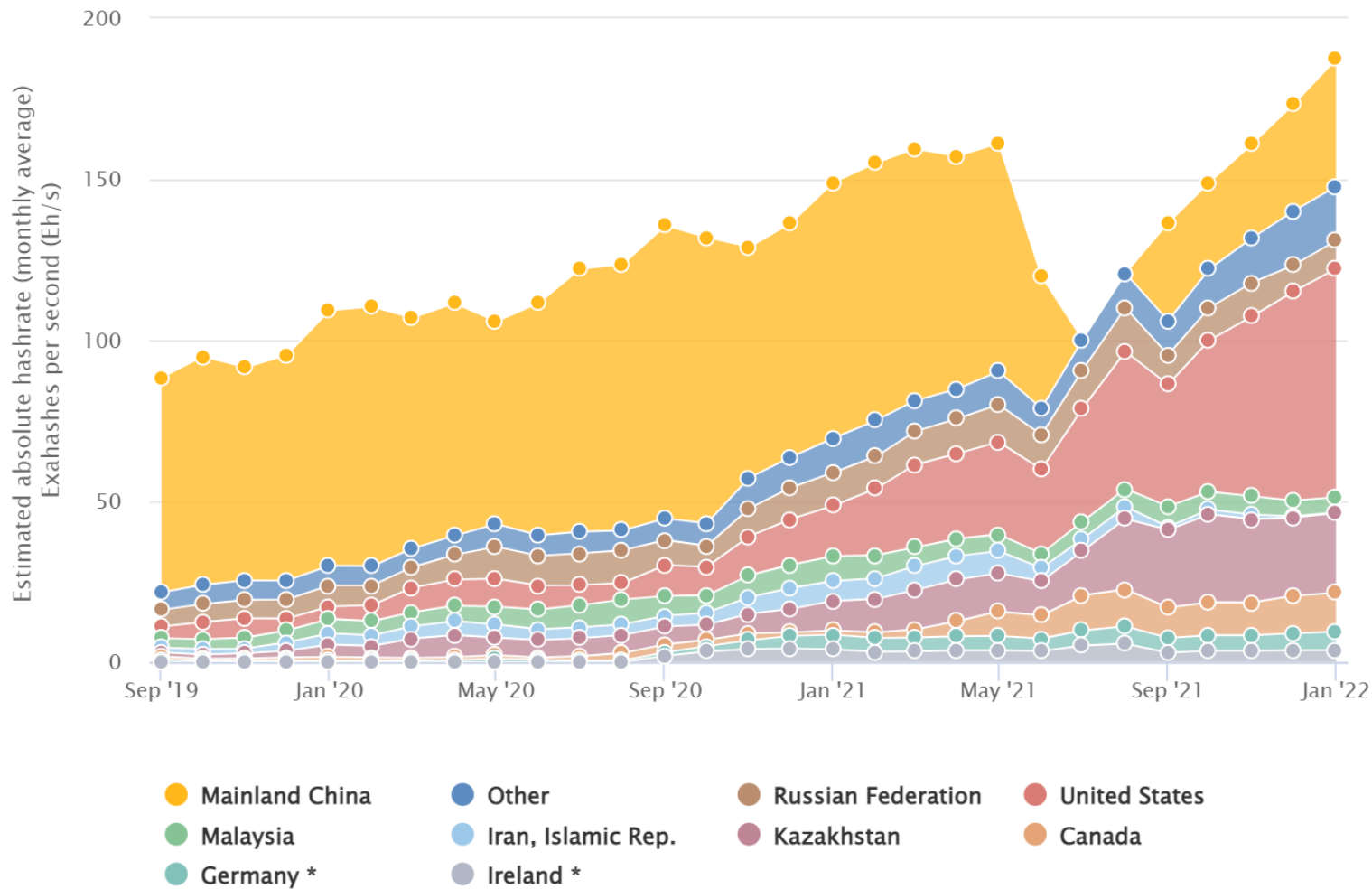
- Miners run the equipment as long as it remains economically profitable in electricity term

Bitcoin Mining Map

- https://ccaf.io/cbeci/mining_map

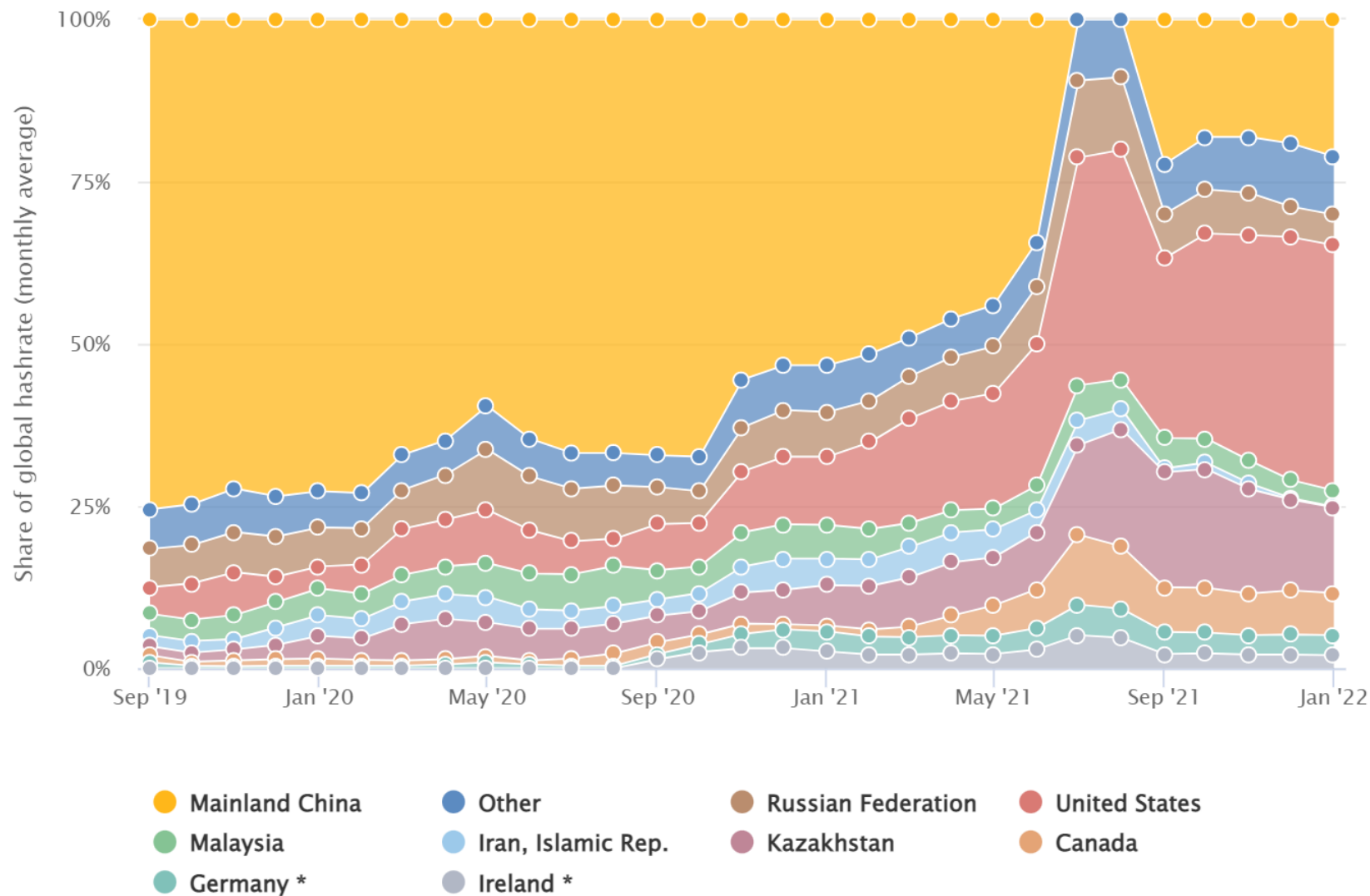


Evolution of Network Hash Rate

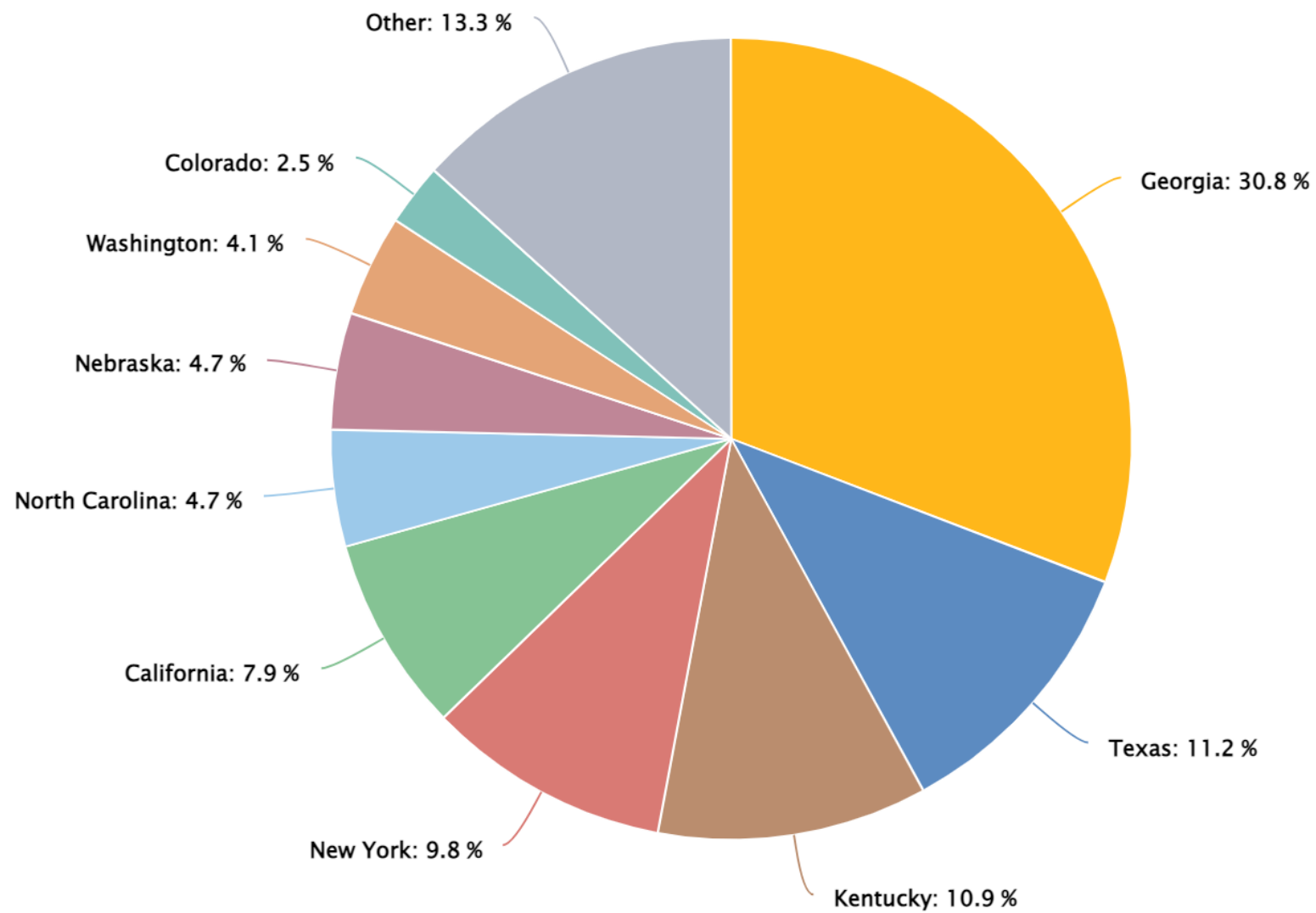


Country Share

Evolution of country share



Hashrate share of United States by states, December 2022



Bitcoin network power demand

🔄 updated every 24 hours

Theoretical lower
bound

7.60

GW

66.63

TWh

Estimated ?

16.21

GW

Annualised
consumption ?

142.05

TWh

Theoretical upper
bound

26.58

GW

232.96

TWh

Comparison – Annual Electricity Consumption



Pakistan

132.3

TWh per
year



Ukraine

134.3

TWh per
year



Bitcoin

142.1

TWh per
year



Malaysia

150.8

TWh per
year

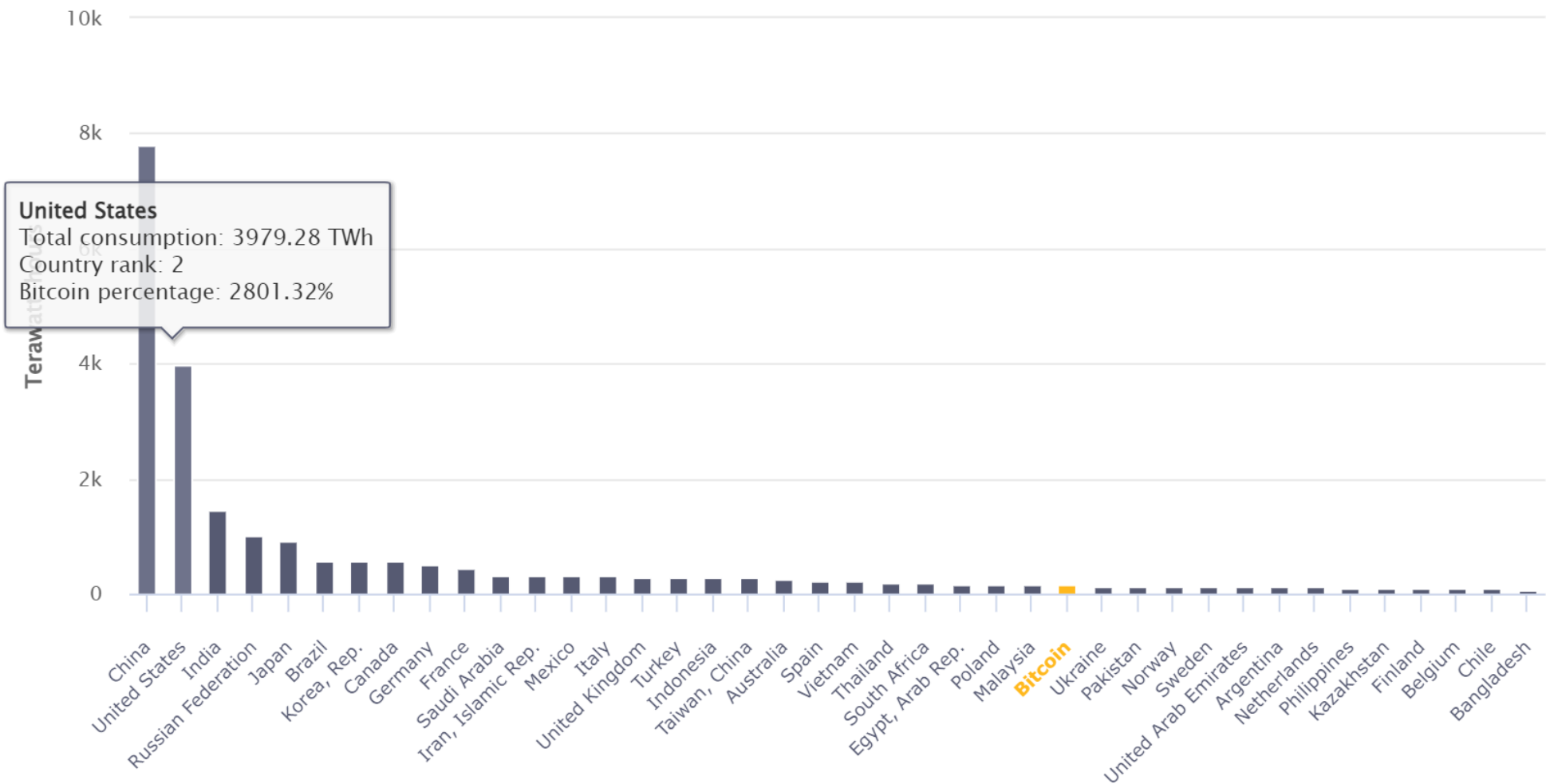


Poland

158.2

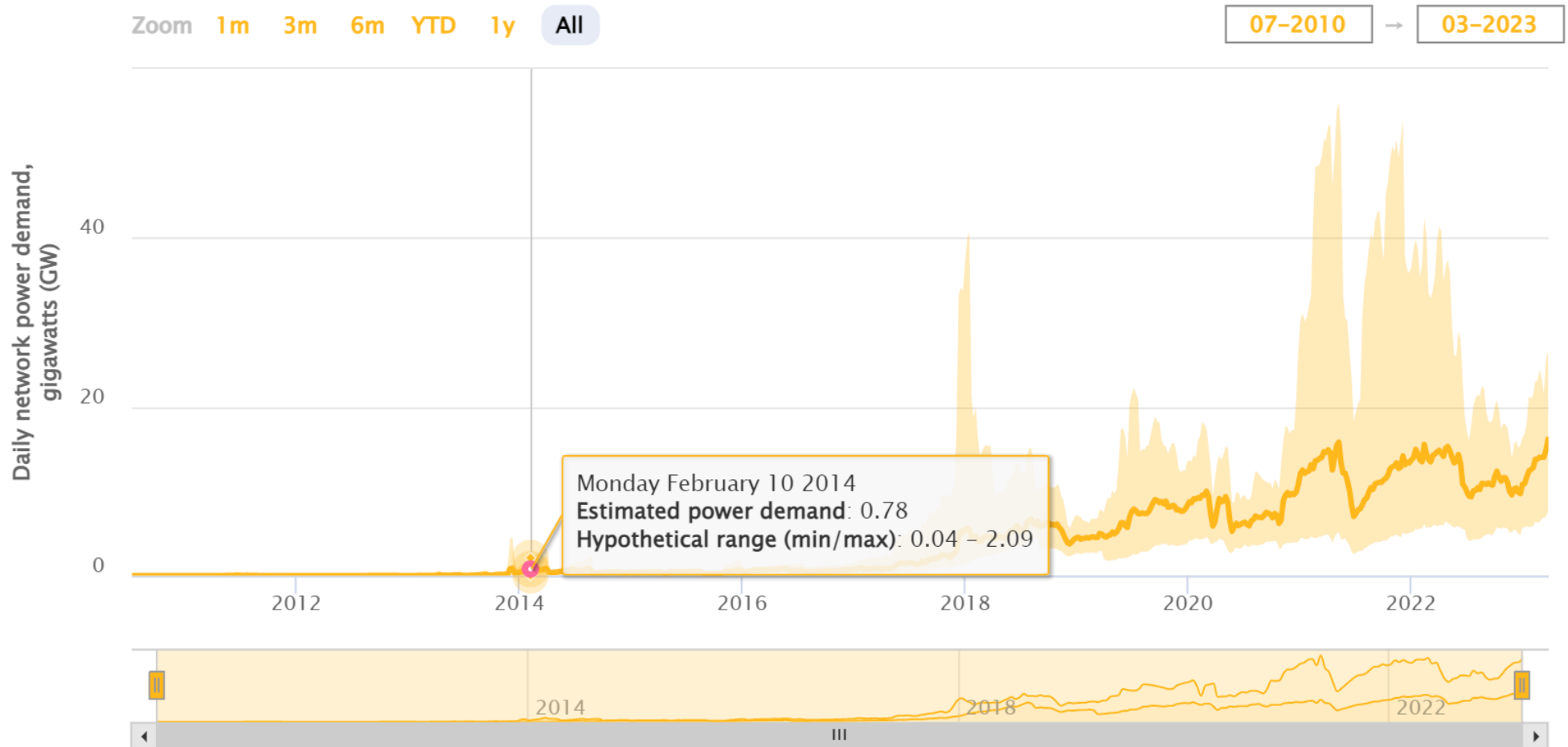
TWh per
year

Country ranking, annual electricity consumption



Historical Bitcoin network power demand

Select an area by dragging across the lower chart



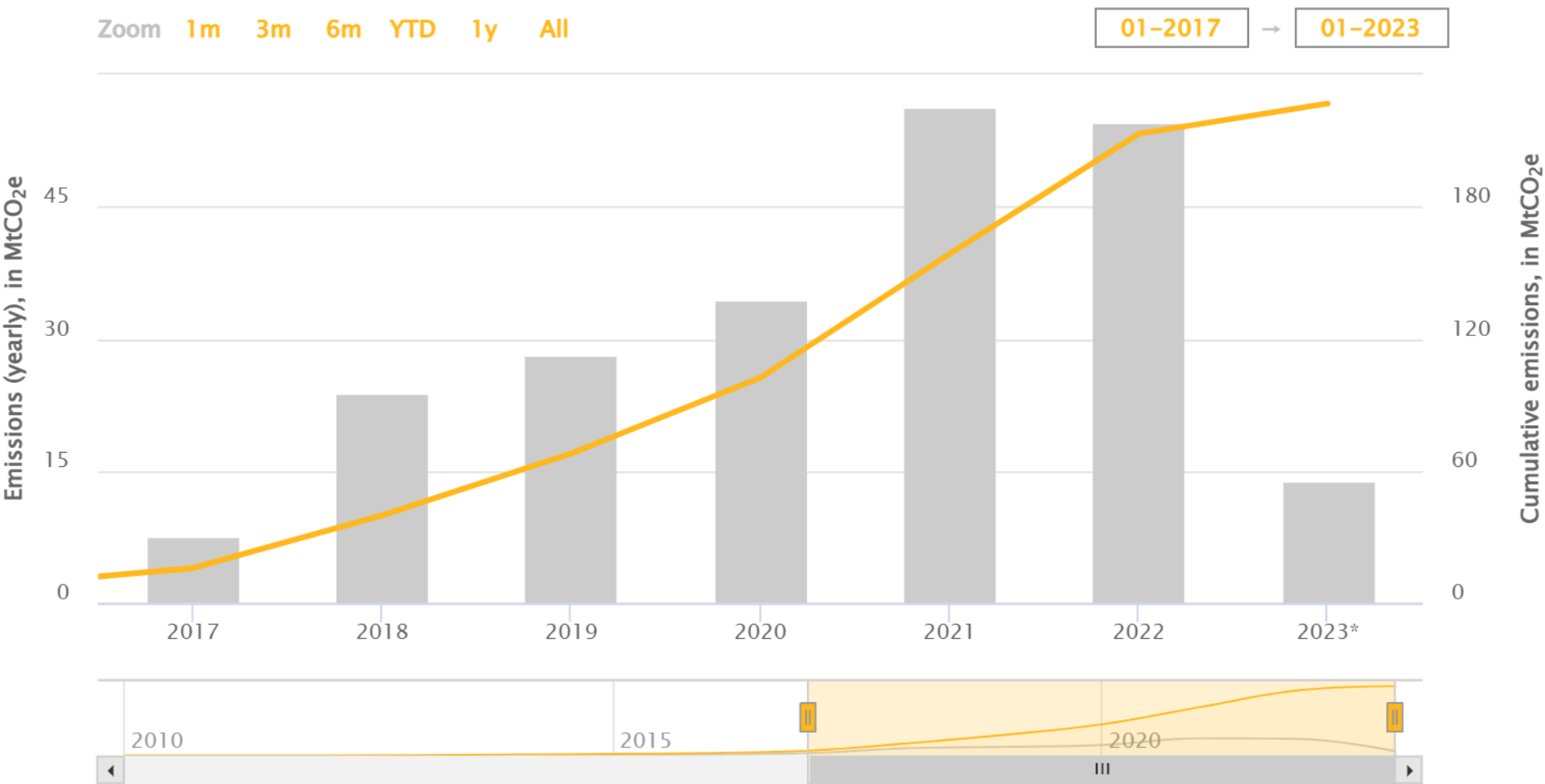
Historical Bitcoin greenhouse gas emissions

Select an area by dragging across the lower chart



Total Bitcoin greenhouse gas emissions

Select an area by dragging across the lower chart



Total World Production & Consumption

- Electricity is generated by transforming primary energy sources into electrical power.
- A significant share of the input energy is lost during this conversion process, with the exact proportion depending on fuel type and power plant efficiency

Electricity



Production

26 730 TWh

Consumption

22 315 TWh

Bitcoin share

 **0.64%**

Energy



Production

167 716 TWh

Bitcoin share*

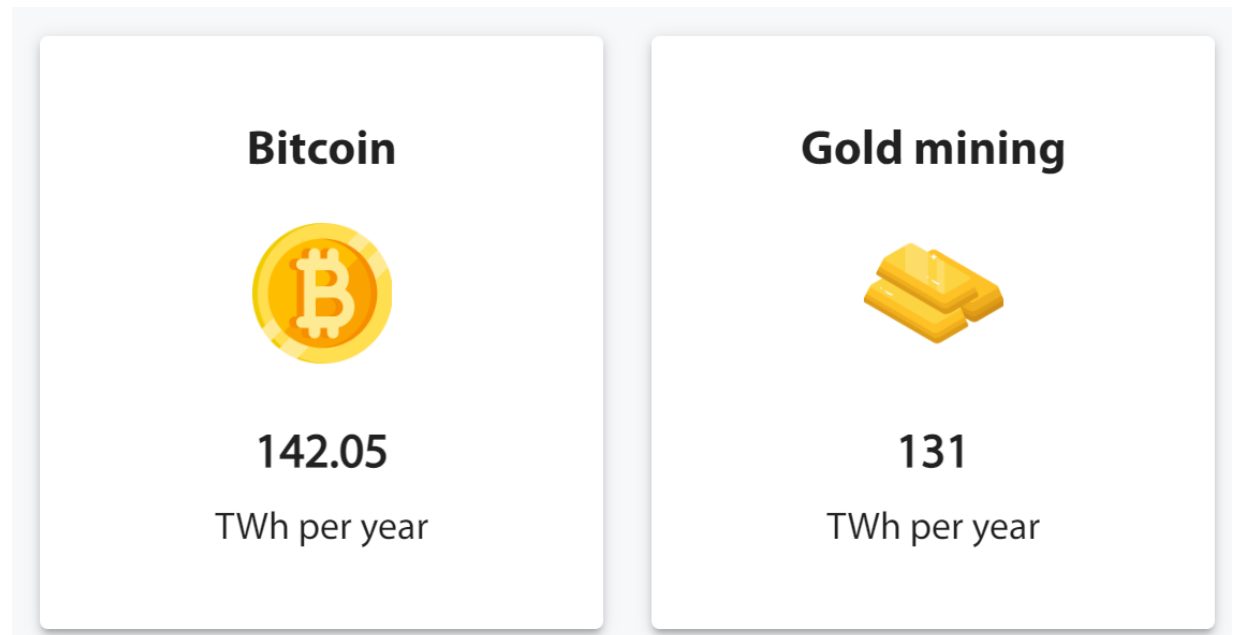
 **0.22%**

Comparisons

- Bitcoin is many things to many people:
- some consider it a new store of value in the form of a synthetic, counterparty-free commodity;
- others prize the underlying value transfer system that enables both payment and settlement functions in a permissionless and censorship-resistant fashion;
- and still others are primarily drawn to the incorruptible notary function enabled by its tamper-resistant public ledger.
- As a result, direct comparisons to other activities that appear similar on the surface can only provide a partial – and thus necessarily incomplete – picture.

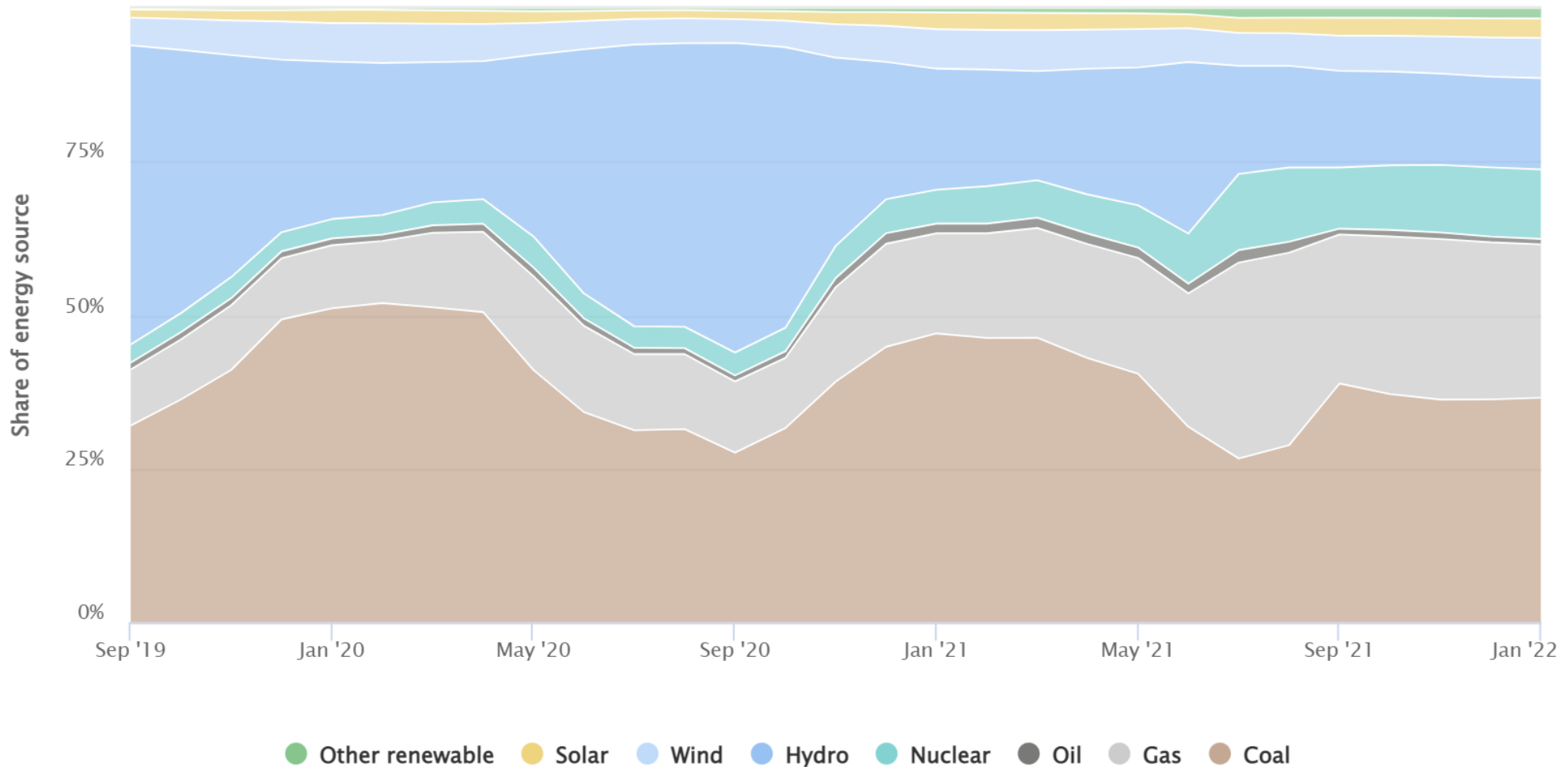
??

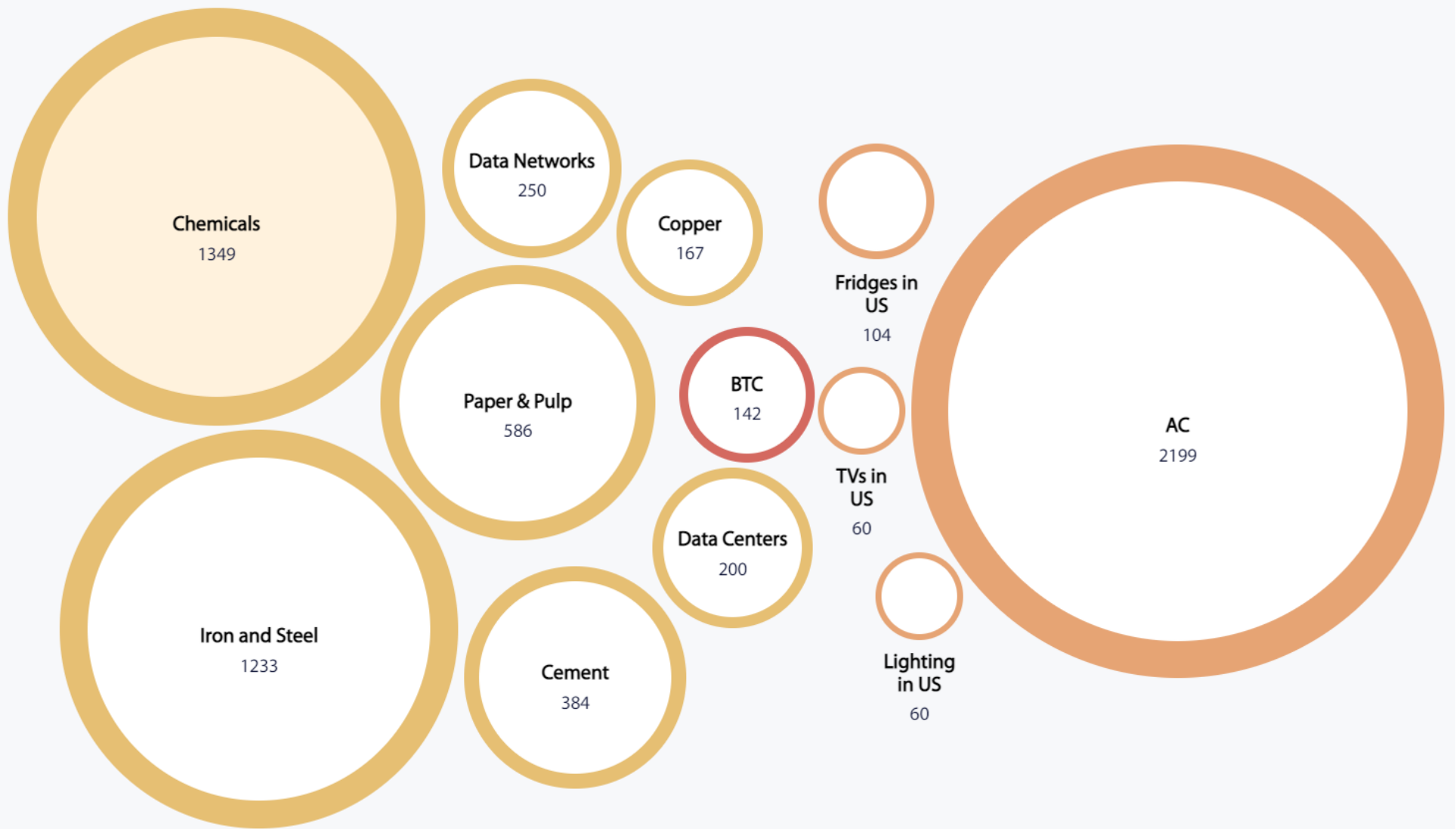
- Presenter Bias - Comparisons tend to be subjective – one can make a number appear small or large depending on what it is compared to.
- Bitcoin's closest and most referenced real-world analogue is gold. While they arguably share utilitarian similarities as stores of value



37% – Coal, 25% – gas, 11% – N, 14% – Hydro, 6% – Wind, 3% – Solar, 2% - other renewable

Bitcoin electricity consumption by source (monthly)





Residential (TWh)



Industrial (TWh)

Loss & Waste

- Unlike other industries, Bitcoin mining is relatively mobile. In their quest for cheap and abundant energy sources, miners can set up new facilities fairly quickly all over the world, including the most remote areas
- As a result, Bitcoin miners can tap into so-called ‘stranded’ energy assets that cannot easily be put to productive use by other industries. In those cases, Bitcoin miners are not competing with other industries or residential users for the same resources, but instead soaking up surplus energy that would otherwise have been lost or wasted.

Environment Effect – GHG emissions

Gold mining



100.4

MtCO₂e per year

Bitcoin

Estimated



71.98

MtCO₂e

World

2019



49 758.23

MtCO₂e

Bitcoin share*

 0.14%



Kenya

73.4

MtCO₂e per year



New Zealand

72.6

MtCO₂e per year



Bitcoin

72.0

MtCO₂e per year



Cambodia

71.8

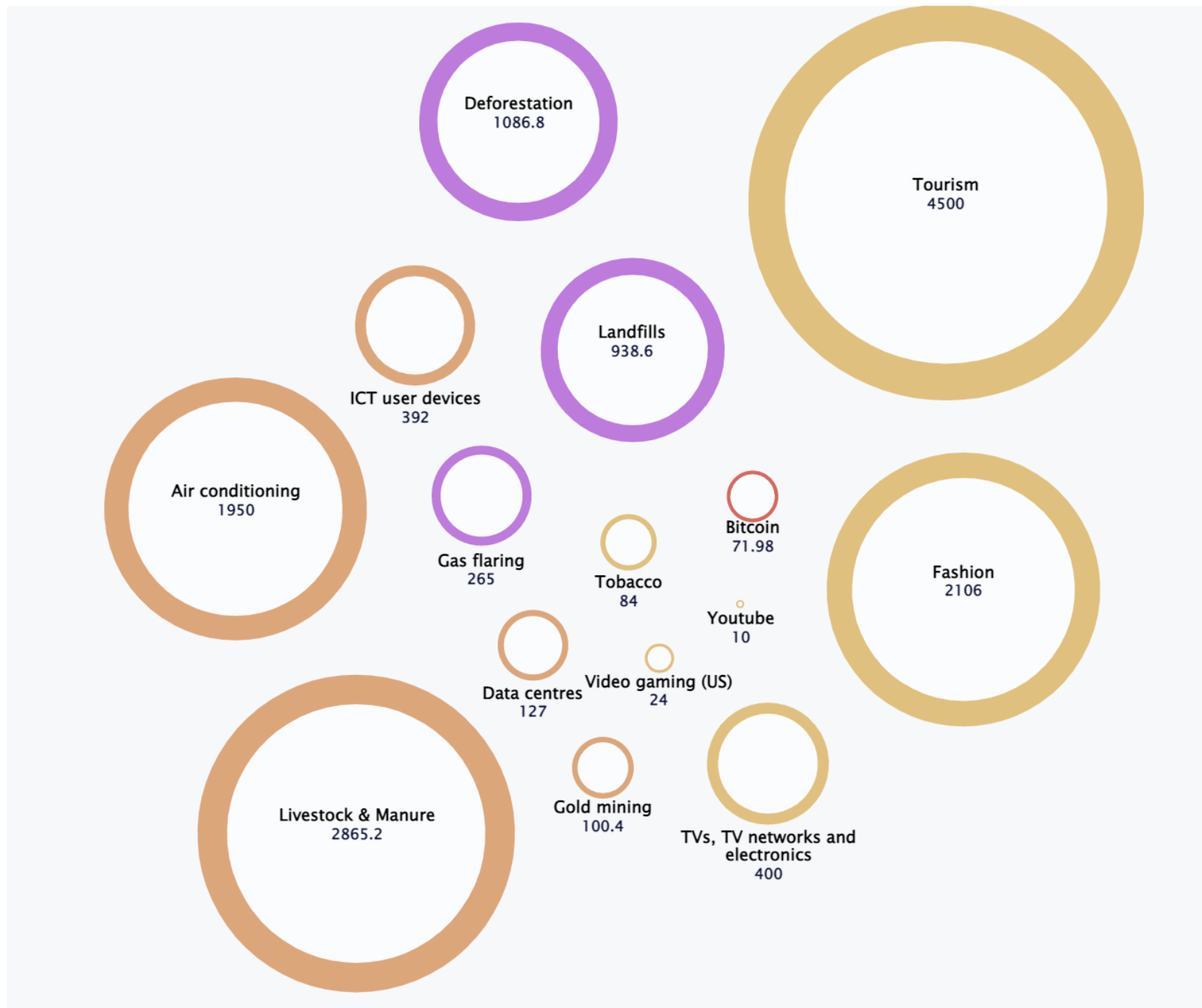
MtCO₂e per year



Austria

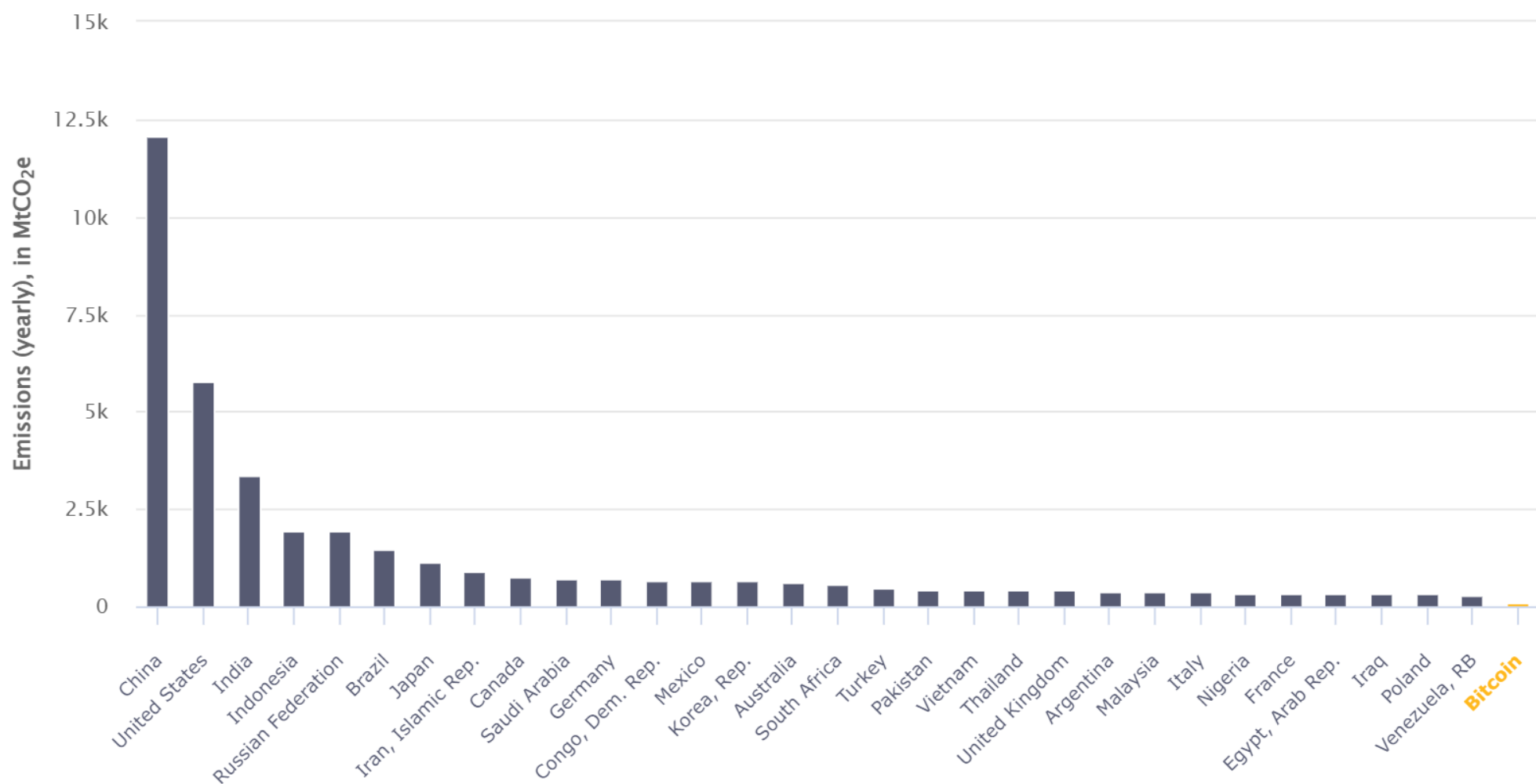
69.8

MtCO₂e per year



GHG Emissions

Greenhouse gas emissions: Bitcoin compared to the 30 most polluting countries



Waste!!!!!!

T&D electricity losses in the USA



206 TWh

Could power the entire Bitcoin network

 **1.5 times**

Global gas flaring recovery potential



688 TWh

Could power the entire Bitcoin network

 **4.8 times**

Renewables curtailment in China



105 TWh

Could power the entire Bitcoin network

 **0.7 times**

Energy sink

- Bitcoin mining the ideal energy sink: anyone, anywhere, can monetize excess energy by plugging in equipment and switching it off at their convenience.
- One example of where Bitcoin mining acts as an energy sink is in oil fields, resulting in a direct reduction in methane emissions
- oil fields currently generate about 40 percent of the world's energy. However, they also frequently produce methane as a by-product, whose greenhouse effects are 25 times as environmentally damaging as those of an equivalent quantity of carbon dioxide!!! (Bitcoin mining offers a solution)

Other Examples

- Iran – Trade sanctions
- Bitcoin Mining
- El Salvador - Volcano's energy use

NFT Power Consumption

- Each NFT sale involves a single transaction on the blockchain.
- **In 2022 there were more than 10.4 million NFT sales.** That yields a total of **about 500 GWh** (Gigawatt hours) for all transactions in the year.
- **the 500 GWh used for NFT transactions in 2022 drove a total of roughly \$6 billion in sales.**
Purchasing 500 GWh for generic use would cost, on average, about \$75 million USD.

TX SB1751 | 2023-2024 | 88th Legislature

- the legislation would curb benefits offered to Bitcoin miners in the state to reduce their power usage during times of high demand. In exchange for cutting their power usage to help the grid prioritize residential customers, Bitcoin miners have been among the commercial clients eligible to receive credits they can use toward their power bills.
- Bitcoin miners consume roughly 2,100 megawatts—up 75% over the past year—and amount to roughly 3.7% of Texas state's peak load
- //Bitcoin mining industry be restricted more than other industries that use as much energy - If this bill passes the BTC miners will just go somewhere else...That state or country will benefit in the future from accepting them

TX SB1751 | 2023-2024 | 88th Legislature

- Marathon, hosts the majority of its rigs—10 exahash of its total installed 14 EH—in several Texas facilities.
- artificial intelligence and machine learning to manage energy use and maintenance for individual rigs
- Marathon can set up very small Bitcoin mining operations “at the edge,” or at the source of where renewable energy can be generated

Bitcoin's Energy Transparency

- Bitcoin mining as a contributor to the climate crisis? EWG - Change the Code, Not the Climate
- In BTC 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)

Our take

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

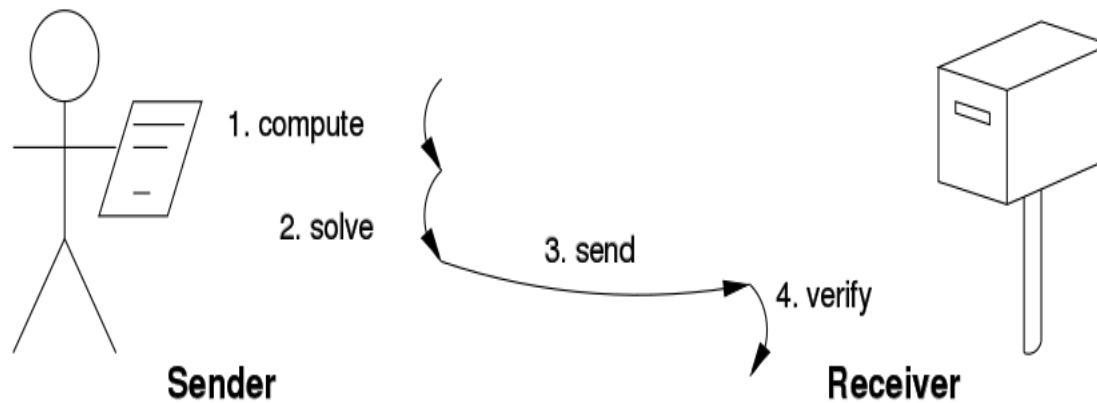
Bitcoin mining puzzle

- also known as the proof-of-work puzzle
- one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended
- Hashcash -The computational work involves finding a partial hash collision, which means finding a hash value that meets a certain difficulty level.
- To solve the puzzle, miners must repeatedly hash the block header with different nonce values until they find a hash that meets the target difficulty level.

PoW – Challenge Response



PoW – Solution Verification (Hashcash)



steps to validate a Bitcoin address

1. Check that the address is in the correct format: A Bitcoin address should start with a "1", "3", or "bc1" and be composed of 26-35 alphanumeric characters.
2. Verify the checksum: Bitcoin addresses contain a built-in checksum that ensures the address is valid. To verify the checksum, the address is decoded from base58 and the last four bytes of the decoded string are the checksum. The checksum is then recalculated, and if it matches the original checksum, the address is valid.
3. Check the address against known address types: Some addresses are reserved for specific purposes, such as multi-signature addresses, pay-to-script-hash (P2SH) addresses, and bech32 addresses. Verifying that the address matches the intended address type ensures that the funds are sent to the correct type of address.

steps to validate a Bitcoin address

Check the address on a blockchain explorer: A blockchain explorer is a tool that allows you to search for information about Bitcoin transactions and addresses on the blockchain. By searching for the address on a blockchain explorer, you can confirm that the address has a transaction history and that the transactions are legitimate.

Spending Bitcoin

- When a user wants to spend Bitcoin from their wallet, they create a transaction and sign it with their private key to prove that they are the legitimate owner of the Bitcoin.
- When a transaction is verified, the signature is checked against the public key of the sender to ensure that it was signed using the correct private key.
- The signature is generated using a process called Elliptic Curve Digital Signature Algorithm (ECDSA), which is a cryptographic algorithm used to create digital signatures.

SegWit

- Segregated Witness (SegWit) is a Bitcoin improvement proposal that was activated on the Bitcoin network in 2017.
- To optimize the use of limited space, it was introduced; which separates the signature data from the rest of the transaction data, allowing for more transactions to be included in each block.
- This has helped to reduce the size of Bitcoin signatures and improve the scalability of the Bitcoin network.

SHA 256 in Bitcoin

- SHA-256 is used to:
- Generate unique identifiers (hashes) for each block on the blockchain, as well as for each transaction within a block.
- Verify the integrity and authenticity of data by generating a hash for the data and comparing it to the expected hash value.
- Securely sign transactions using digital signatures, which rely on the SHA-256 algorithm to ensure the signature is valid and unforgeable.
- Generate the target value for the proof-of-work consensus mechanism used in Bitcoin mining.

Merkle tree in bitcoin blockchain

- To construct a Merkle tree, the transactions in a block are first hashed individually using the SHA-256 algorithm. The resulting hashes are then paired and hashed again to produce a new set of hashes.
- This process continues until there is only a single hash remaining, known as the Merkle root.
- The Merkle root is then included in the block header along with other information such as the previous block hash and the target difficulty.

Wallet creation

- Use your wallet: You can use your wallet to send and receive cryptocurrency, view your transaction history, and manage your funds.
- It's important to note that cryptocurrency wallets are not insured by the government, so it's important to take steps to protect your funds, such as keeping your backup phrase secure and using strong passwords.
- wallet creation program
- To create a cryptocurrency wallet program, you would need to have a good understanding of programming languages like Java, Python, or C++. Here are the general steps to create a wallet program:
- Choose the cryptocurrency: Decide which cryptocurrency your wallet program will support.
- Choose the platform: Decide which platform your wallet program will run on, such as desktop or mobile.
- Choose the type of wallet: Decide which type of wallet your program will be, such as software, hardware, or paper wallet.

Wallet creation

- Set up the development environment: Set up your development environment with the necessary tools and libraries.
- Develop the wallet software: Write the code for your wallet software, including features like creating new wallet addresses, generating private keys, sending and receiving transactions, and viewing transaction history.
- Implement security features: Implement security features like password protection, encryption, and two-factor authentication to ensure the safety of users' funds.
- Test the wallet program: Test the program thoroughly to ensure that it works as intended and is free of bugs.
- Launch the wallet program: Launch the wallet program and make it available for download.
- Provide support and updates: Provide support to users and release updates to the wallet program as needed to fix bugs and add new features.

Bitcoin Hacks

- Bitcoin hacks refer to the various incidents where hackers have stolen Bitcoin or gained unauthorized access to Bitcoin wallets, exchanges, or other digital platforms.
- Some of the notable Bitcoin hacks and thefts in recent years include:
- Mt. Gox hack: In 2014, Mt. Gox, one of the largest Bitcoin exchanges at the time, suffered a massive security breach resulting in the loss of around 850,000 bitcoins, worth over \$460 million at the time.
- Bitfinex hack: In 2016, Bitfinex, a major Bitcoin exchange, was hacked, resulting in the loss of around 120,000 bitcoins, worth around \$72 million at the time.

Bitcoin hacks

- NiceHash hack: In 2017, NiceHash, a popular Bitcoin mining marketplace, was hacked, resulting in the theft of around 4,700 bitcoins, worth around \$64 million at the time.
- Coincheck hack: In 2018, Coincheck, a Japanese cryptocurrency exchange, was hacked, resulting in the theft of around 500 million NEM coins, worth around \$530 million at the time.
- Binance hack: In 2019, Binance, one of the largest cryptocurrency exchanges, suffered a security breach that resulted in the loss of around 7,000 bitcoins, worth around \$40 million at the time.

Ethereum hacks

- Some of the notable Ethereum hacks and thefts include
- DAO hack: In 2016, a smart contract on the Ethereum blockchain called The DAO was hacked, resulting in the theft of around 3.6 million ETH, worth around \$50 million at the time. The incident led to a hard fork of the Ethereum blockchain, resulting in the creation of Ethereum (ETH) and Ethereum Classic (ETC).
- Parity wallet hack: In 2017, a vulnerability in a popular Ethereum wallet called Parity Multi-Sig Wallet was exploited, resulting in the theft of around 150,000 ETH, worth around \$30 million at the time.
- Bancor hack: In 2018, Bancor, a decentralized exchange built on the Ethereum blockchain, suffered a security breach, resulting in the theft of around \$23.5 million worth of ETH and other cryptocurrencies.
- Upbit hack: In 2019, Upbit, a South Korean cryptocurrency exchange, was hacked, resulting in the theft of around 342,000 ETH, worth around \$50 million at the time.

Other hacks

- In addition to Bitcoin and Ethereum, other cryptocurrencies have also been subject to various hacks and security breaches. Here are some examples:
- BitGrail hack: In 2018, BitGrail, an Italian cryptocurrency exchange, was hacked, resulting in the loss of around \$170 million worth of Nano (NANO) cryptocurrency.
- Coinrail hack: In 2018, Coinrail, a South Korean cryptocurrency exchange, was hacked, resulting in the loss of around \$40 million worth of various cryptocurrencies.

Bitcoin hacks

- Cryptopia hack: In 2019, Cryptopia, a New Zealand-based cryptocurrency exchange, suffered a security breach, resulting in the theft of around \$16 million worth of various cryptocurrencies.
- KuCoin hack: In 2020, KuCoin, a Singapore-based cryptocurrency exchange, was hacked, resulting in the loss of around \$280 million worth of various cryptocurrencies.
- These incidents demonstrate the importance of implementing proper security measures and protocols for cryptocurrencies, as well as staying vigilant and aware of potential vulnerabilities and threats.

DeFi

- DeFi, or Decentralized Finance, refers to a set of financial applications built on top of decentralized blockchain networks, such as Ethereum.
- DeFi applications aim to create a more open, transparent, and accessible financial system that operates without intermediaries or central authorities.

DeFi features

- Some of the key features of DeFi include:
- Open access: Anyone with an internet connection can access DeFi applications, regardless of their location, nationality, or financial status.
- Decentralization: DeFi applications are built on top of decentralized blockchain networks, meaning they are not controlled by any central authority or intermediary.
- Transparency: All transactions on DeFi networks are publicly visible on the blockchain, allowing for greater transparency and accountability.
- Programmability: DeFi applications are built using smart contracts, which are self-executing computer programs that automatically execute when certain conditions are met.

DeFi applications

- Some of the most popular DeFi applications include decentralized exchanges (DEXs), lending and borrowing platforms, stablecoins, and prediction markets.

DEX

- A DEX, or decentralized exchange, is a type of cryptocurrency exchange that operates in a decentralized manner, meaning it does not rely on a central authority or intermediary to manage and facilitate trades.
- Instead, DEXs operate on a decentralized blockchain network, typically using smart contracts to automate the exchange of cryptocurrencies between users.
- Some of the most popular DEXs include Uniswap, PancakeSwap, SushiSwap, and Curve.

DEX features

- Some of the key features of DEXs include:
- Decentralization: DEXs are built on top of decentralized blockchain networks, meaning they are not controlled by any central authority or intermediary.
- Transparency: All transactions on DEXs are publicly visible on the blockchain, allowing for greater transparency and accountability.
- Security: Because DEXs do not rely on a central authority or intermediary, they are generally considered to be more secure and less susceptible to hacking or theft.
- Control: Users of DEXs have full control over their funds and can trade cryptocurrencies without the need for a third party.

CEX

- Centralized exchanges (CEXs) are traditional cryptocurrency exchanges that operate in a centralized manner, meaning they rely on a central authority or intermediary to manage and facilitate trades.
- In contrast to decentralized exchanges (DEXs), CEXs typically operate on a centralized server or database, with a central team of administrators responsible for managing the exchange.
- Some of the most popular CEXs include Binance, Coinbase, Kraken, and Bitfinex.

CEX features

- Some of the key features of CEXs include:
- User-friendly interface: CEXs often have a more user-friendly interface than DEXs, making it easier for users to navigate and trade cryptocurrencies.
- High liquidity: Because CEXs operate on a centralized server, they can offer high levels of liquidity, making it easier for users to buy and sell cryptocurrencies.
- Faster trades: CEXs can often process trades faster than DEXs, as they do not rely on blockchain transactions to settle trades.
- Regulation: CEXs are often subject to regulation and compliance requirements, which can offer users a greater sense of security and protection.

Meltdown (of CEX)

- A CEX meltdown could refer to a number of scenarios that could cause disruption or even the collapse of a centralized cryptocurrency exchange (CEX). Such a meltdown could be caused by a number of factors, including:
- Security breaches: CEXs are often targeted by hackers who attempt to steal funds or personal information from users. A major security breach could cause significant damage to the reputation and finances of an exchange.
- Operational failures: Technical glitches or operational failures could lead to trading disruptions, delays, or even losses of funds. If such problems are not addressed promptly, they could lead to a loss of user confidence in the exchange.

Cont. (CEX meltdown)

- Regulatory crackdowns: CEXs are often subject to regulatory scrutiny, and a major regulatory crackdown could lead to the closure of an exchange or severe restrictions on its operations.
- Market volatility: The cryptocurrency market is highly volatile, and a sudden drop in prices could lead to a rush of users trying to sell their assets on the exchange. If the exchange is unable to handle the volume of trades, it could cause the exchange to shut down or suffer losses.
- In the event of a CEX meltdown, users could lose access to their funds or suffer losses, and the exchange could face legal action, bankruptcy, or closure.

DEX meltdown

- Smart contract vulnerabilities: DEXs are built on top of smart contracts that automate the exchange of cryptocurrencies between users. If there are vulnerabilities in the code or if the code is not audited properly, it could lead to the loss of funds or the manipulation of trades.
- Liquidity issues: DEXs rely on a network of users to provide liquidity, and if there is not enough demand or supply for a particular token, it could lead to significant price slippage or even a lack of trades.
- Network congestion: DEXs operate on a decentralized blockchain network, and if the network becomes congested with high transaction volumes or high gas fees, it could lead to delays or even the inability to execute trades.
- Market volatility: The cryptocurrency market is highly volatile, and sudden price movements could lead to a rush of users trying to sell their assets on the DEX. If the DEX is unable to handle the volume of trades, it could cause the DEX to shut down or suffer losses.

A crypto derivative exchange

- A crypto derivative exchange is a type of cryptocurrency exchange that allows traders to buy and sell derivatives contracts based on the price of cryptocurrencies.
- The most common types of cryptocurrency derivatives offered by these exchanges are futures and options.
- Some popular crypto derivative exchanges include BitMEX, Deribit, FTX, and Binance Futures.

Future and Option

- Futures contracts are agreements to buy or sell a cryptocurrency at a predetermined price and date in the future, while options contracts give the holder the right, but not the obligation, to buy or sell a cryptocurrency at a predetermined price and date in the future.
- A call option gives the holder the right to buy an underlying asset, while a put option gives the holder the right to sell an underlying asset.

DAO

- DAO, stands for Decentralized Autonomous Organization. A DAO is an organization that operates through rules encoded as computer programs called smart contracts, which run on a decentralized blockchain network. In a DAO, decision-making and operations are decentralized, meaning that members can vote on proposals and make decisions without the need for a central authority or intermediary. The rules of a DAO are enforced through smart contracts, which ensure that all transactions are transparent and cannot be changed without consensus from the members.

DAO

- DAOs can be used for a variety of purposes, such as managing decentralized finance (DeFi) protocols, creating decentralized social networks, or organizing online communities. DAOs can also provide a more democratic and transparent way of managing organizations, as decision-making is open to all members and the rules are transparent and immutable. However, DAOs are still a relatively new concept, and there are challenges to overcome in terms of governance, security, and scalability.

MakerDAO

- MakerDAO is a decentralized autonomous organization (DAO) that operates on the Ethereum blockchain. Its primary goal is to provide a stablecoin called DAI, which is pegged to the value of the US dollar.
- Unlike other stablecoins that are backed by fiat currency or other assets, DAI is backed by collateral held in smart contracts on the Ethereum blockchain.
- To generate DAI, users can deposit Ethereum or other Ethereum-based assets as collateral and borrow DAI against that collateral. The collateral is held in a smart contract called a Collateralized Debt Position (CDP), which automatically liquidates the collateral if its value falls below a certain threshold to maintain the stability of DAI.

MakerDAO hacks

- MakerDAO's stablecoin, DAI, has become popular in the decentralized finance (DeFi) ecosystem as it provides a way for users to access stable value without relying on centralized institutions.
- Black Thursday: On March 12, 2020, the value of Ethereum dropped sharply, causing a liquidation cascade in MakerDAO's system. This event, known as Black Thursday, led to approximately \$8.32 million worth of DAI being undercollateralized, which led to a debt auction and a significant loss for some users.
- Oracle Attacks: In April 2020, MakerDAO suffered two separate oracle attacks, in which attackers were able to manipulate the price of certain assets used as collateral in the system. This led to a loss of approximately \$12.5 million in ETH from the system's liquidation mechanism.

MakerDAO hacks

- Flash Loan Exploit: In November 2020, a user was able to exploit a vulnerability in the system to create an undercollateralized loan of over \$88 million worth of DAI. The exploit involved using flash loans to manipulate the price of certain assets and create an artificially high collateralization ratio.
- February 2021 Incident: In February 2021, MakerDAO disclosed that it had discovered a vulnerability in its Liquidations 2.0 code, which could have allowed attackers to manipulate the liquidation process and steal funds from users. The vulnerability was quickly patched, and no funds were reported stolen.

DeFi and TradFi

- Decentralized finance (DeFi) may represent the financial “pipes” of the future, but it is the old world of traditional finance (TradFi) that still holds all the water.
- To date, adoption has been hindered by regulatory uncertainty, market volatility and the risks inherent in diving in to provable digital scarcity as an early entrant.
- But lying behind these immediate roadblocks, the way forward becomes somehow even less clear.
- Perhaps the most fundamental issue of all is sheer size. Consider the just market for foreign currency. JPMorgan settles forex trades with the combined value of the entire cryptocurrency sector every day.

DeFi and TradFi

- Blockchain technology has much value to bring to this market, particularly through the novel capabilities of stablecoins. Their potential for instant settlement and close-to-zero marginal costs – which could unlock dramatically lower foreign exchange (FX) rates – is tantalizingly real, but the infrastructure needed to support adoption at scale is critically missing.
- Scale matters because almost all present-day crypto settlement products were built under retail-sized premises. Namely, low marginal cost settlement has been made possible by the remarkable maturation of “automated market makers,” also known as AMMs

Programs

- To generate a wallet
- To generate ERC 20 token
- To generate ERC 721 token
- To create a DAO