

5

Bitcoin, Blockchain, and Cryptocurrencies



SUMMARY

- The first cryptocurrency Bitcoin was launched in 2009, providing an innovative solution to the double-spend problem known as hashing.
- Ownership of bitcoins is recorded in an electronic distributed ledger called the blockchain, so-named because transactions are batch processed in blocks and secured using cryptography in an immutable, append-only, public ledger.
- Other developers soon launched alternative cryptocurrencies to Bitcoin (“altcoins”), and later digital tokens. The common feature of these cryptoassets is they are all recorded on separate blockchains.
- Many cryptoassets were pre-mined and sold to the public through initial coin offerings (ICOs), before regulators shut down this market in mid-2018 due to the large number of frauds.
- As the cryptocurrency market has grown, innovations such as cryptowallets for storage and cryptoexchanges for trading of cryptoassets have emerged to address pain points.
- Academic researchers have studied the economics of Bitcoin as a means of payment, the ability to conduct arbitrage across cryptocurrency exchanges, and the returns from investing in cryptocurrencies versus traditional assets.

The previous chapter outlined how angel investors and VCs value a fintech and the methods used to value more mature fintechs and financial intermediaries using market multiples of comparable companies.

Table of Contents

1	Foundations of Fintech	1
2	Fintech Economics, Strategies, and Business Models	33
3	Funding of Early-Stage Fintech Companies	58
4	Valuation of Fintech Companies	90
5	Bitcoin, Blockchain, and Cryptocurrencies	123
6	Ethereum and Decentralized Finance	160
7	Alternative Finance, Online Lending, and Crowdfunding	187
8	Robo-advisors and Digital Wealth Management	220
9	Payments and Insurtech	245
10	Digital Banking and the Response of Incumbents	275
11	Techfins and Bigtech in Financial Services	305

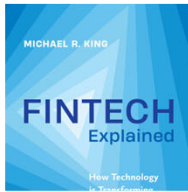
5 Bitcoin, Blockchain, and Cryptocurrencies

- The first cryptocurrency Bitcoin was launched in 2009, providing an innovative solution to the double-spend problem known as hashing.
- Ownership of bitcoins is recorded in an electronic distributed ledger called the blockchain, where transactions are batch processed in blocks and secured using cryptography in an immutable, append-only, public ledger.
- Other developers soon launched alternative cryptocurrencies to Bitcoin (“altcoins”), and later digital tokens. The common feature of these cryptoassets is they are all recorded on separate blockchains.
- Many cryptoassets were pre-mined and sold to the public through initial coin offerings (ICOs), before regulators shut down this market in mid-2018 due to the large number of frauds.
- As the cryptocurrency market has grown, innovations such as cryptowallets for storage and cryptoexchanges for trading of cryptoassets have emerged to address pain points.
- Academic researchers have studied the economics of Bitcoin as a means of payment, the ability to conduct arbitrage across cryptocurrency exchanges, and the returns from investing in cryptocurrencies versus traditional assets

The Rise (and Fall) of Cryptoeconomics

- A **cryptoasset** is a digital asset whose ownership is recorded on an electronic, distributed ledger known as a *blockchain*.
 - A **blockchain** is secured against alteration using cryptography - a mathematical method to encode and protect data (from the Greek word *kryptos* meaning hidden).
- **Bitcoin** was the first cryptocurrency issued in 2009.
 - A cryptocurrency is digital money stored on a blockchain.
 - Other digital coins are known as **Alternatives to Bitcoin** (or altcoins).
 - They were joined by **tokens**: utility tokens, securities tokens, governance tokens, and non-fungible tokens (NFTs).

CoinMarketCap, as of Dec 8, 2023 <https://coinmarketcap.com/>



Cryptos: 2M+ Exchanges: 680 Market Cap: \$1.63T ▲ 2.18% 24h Vol: \$66.43B ▼ 5.20% Dominance: BTC: 52.7% ETH: 17.4% ETH Gas: 44 Gwei ▼ Fear & Greed: 81/100

CoinMarketCap [Cryptocurrencies](#) [Exchanges](#) [Community](#) [Products](#) [Learn](#)

Today's Cryptocurrency Prices by Market Cap

The global crypto market cap is \$1.63T, a ▲ 2.18% increase over the last day. [Read Less](#)

The total crypto market volume over the last 24 hours is \$66.43B, which makes a ▼ 5.20% decrease. The total volume in DeFi is currently \$8.15B, 12.26% of the total crypto market 24-hour volume. The volume of all stable coins is now \$58.81B, which is 88.53% of the total crypto market 24-hour volume.

Bitcoin's dominance is currently 52.73%, a decrease of ▼ 0.29% over the day.

Cryptocurrencies

Categories

AI & Big Data

BRC-20

Gaming

DePin

Show rows 100 ▼

Filters

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply
☆ 1	Bitcoin BTC	\$43,924.83	▲ 0.25%	▲ 1.84%	▲ 13.36%	\$859,359,094,507	\$23,064,832,396 526,170 BTC	19,564,312 BTC
☆ 2	Ethereum ETH	\$2,355.26	▲ 0.19%	▲ 1.06%	▲ 12.86%	\$283,149,441,401	\$13,382,017,777 5,691,609 ETH	120,220,036 ETH
☆ 3	Tether USDt USDT	\$1.00	▲ 0.00%	▲ 0.01%	▲ 0.01%	\$90,284,252,175	\$48,707,838,451 48,694,259,522 USDT	90,255,875,639 USDT
☆ 4	BNB BNB	\$238.13	▲ 0.52%	▲ 3.14%	▲ 4.20%	\$36,123,238,585	\$821,756,126 3,454,798 BNB	151,697,129 BNB
☆ 5	XRP XRP	\$0.669	▲ 0.60%	▲ 4.25%	▲ 9.33%	\$35,962,898,111	\$1,808,506,070 2,707,908,464 XRP	53,757,460,767 XRP

The Rise (and Fall) of Cryptoeconomics

- A **utility (or service) token** records a claim to a product or service.
- A **security token** represents an ownership claim to the cash flows generated by a business or asset (such as real estate).
- A **governance token** provides the holder with the ability to vote.
- A **non-fungible token (NFT)** is a cryptographically secured data file that is non-interchangeable but can be bought or sold, such as a digital piece of art, a photo, a video, or an audio clip.

The Rise (and Fall) of Cryptoeconomics

- Prices of cryptoassets have been volatile, rising and falling through different “**crypto winters.**”
- Like the broader financial markets, the crypto markets have seen their share of **fraud and scams.**
 - **Cybersecurity** is always an issue, particularly with the increase in hacking and emerging technologies such as quantum computing.
 - The bottom line for anyone interested in cryptoassets is ***caveat emptor***, which is Latin for “buyer beware.”
 - We all need to be informed and educated when making investment decisions and avoid behavioral biases such as **FOMO** (fear of missing out)

Bitcoin: The First Cryptocurrency

- In 2008, the anonymous creator(s) Satoshi Nakamoto posted a nine-page working paper on the internet

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

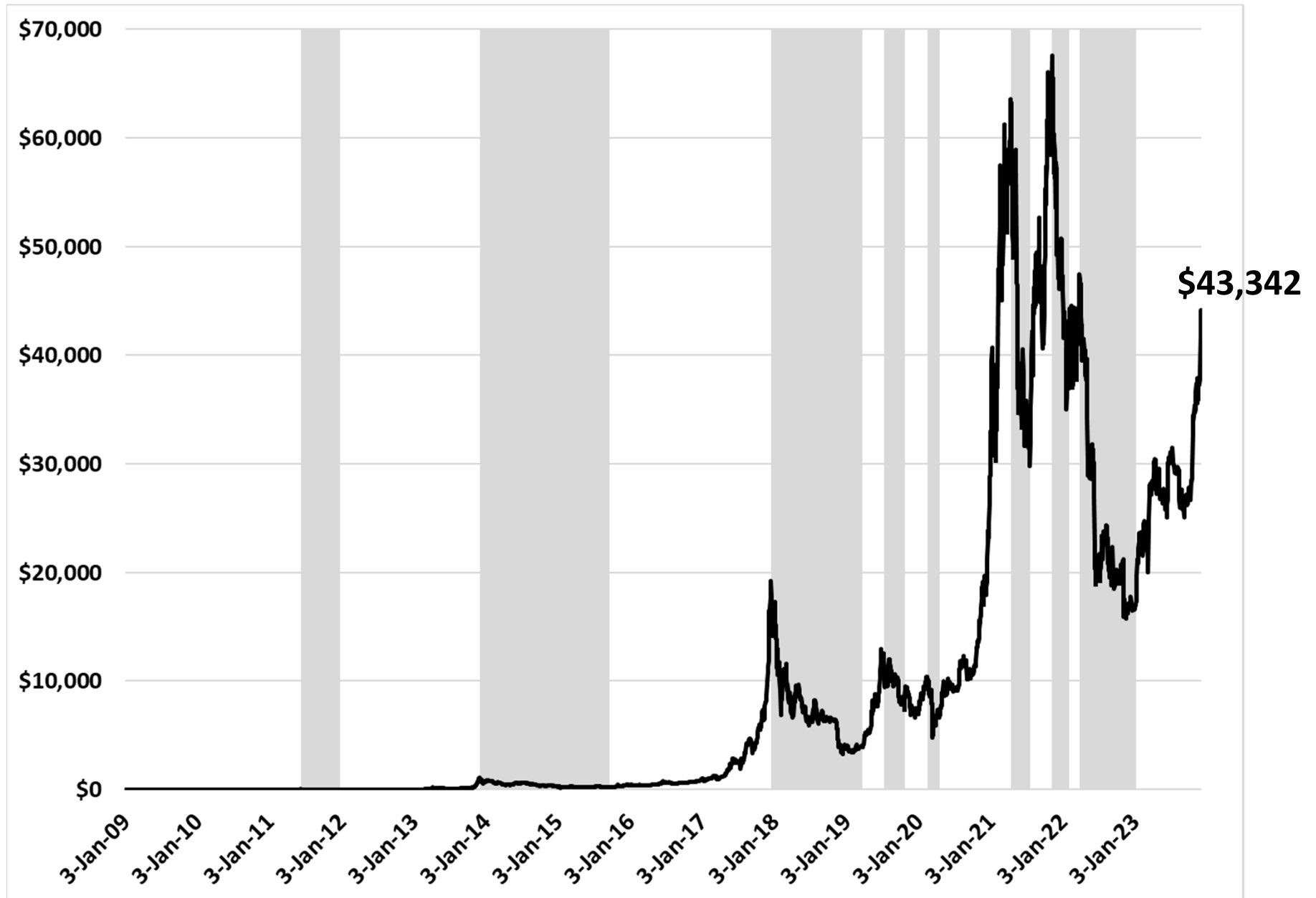
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin: The First Cryptocurrency

- Satoshi's motivation was to create a currency not controlled by a central authority.
 - A peer-to-peer (P2P) version of electronic cash would allow online payments to be sent directly from one party to another without going through a central intermediary, such as a central bank.
 - The Bitcoin network was launched over the internet in 2009, with Satoshi mining the first coins.
- Is it spelt Bitcoin or bitcoin? Satoshi used both.
 - Use uppercase "B" in Bitcoin to refer to the concept of Bitcoin or the network for transacting in this digital coin.
 - Individual coins and the currency unit are spelled with a lowercase "b" as bitcoins. The symbols are ₿ or BTC.
- Bitcoin has gone through many boom-bust cycles

Bitcoin: The First Cryptocurrency

Figure 5.1. Bitcoin Price and Crypto Winters



Bitcoin: The First Cryptocurrency

- Here is a snapshot of the ups and downs, daily return, and bitcoin in circulation.

Table 5.1. Bitcoin Statistics

Year	Average Price (USD)	Min Price (USD)	Max Price (USD)	St. Dev. Price (USD)	Average Daily Return (%)	Bitcoin in Circulation
2010	0.17	0.06	0.37	0	4.81	4,378,243
2011	6.05	0.30	35.00	6	2.45	6,604,402
2012	8.47	4.33	15.40	3	0.68	9,371,011
2013	189	13	1,151	242	2.86	11,380,586
2014	525	314	896	145	-0.33	12,960,176
2015	272	177	459	58	0.31	14,342,474
2016	566	373	967	137	0.50	15,641,818
2017	4,018	785	19,290	4,078	1.74	16,425,120
2018	7,561	3,271	17,319	2,436	-0.53	17,125,076
2019	7,383	3,395	12,933	2,642	0.24	17,796,539
2020	11,057	4,830	28,857	4,213	0.46	18,399,414
2021	47,386	28,983	67,562	9,827	0.22	18,750,821
2022	28,387	15,787	47,466	10,165	-0.23	19,242,081

Source: CoinMarketCap, author's calculations.

Bitcoin: The First Cryptocurrency

- **The Double-Spend Problem**

- Earlier digital currencies failed as no one could solve the “double-spend” problem: how to allow for the electronic exchange of money without a trusted intermediary to verify that the money had not be spent twice.
- Satoshi’s solution was to use a **time-stamped** electronic record-keeping system to record transfers of bitcoins.
- This electronic ledger, called the **blockchain**, was **secured** against alterations using cryptography.
- The blockchain would remain **public and transparent**, with multiple copies widely available on a **P2P network** run on independent computers (called **nodes**).
- Bitcoin transactions were collected in **blocks** and **hashed** to make these records **immutable** through a process called “**mining**”.

Bitcoin: The First Cryptocurrency

- **Blockchain**

- Originally, "blockchain" referred to the **electronic distributed ledger** that records ownership of bitcoins.
- Bitcoin transactions are **batch processed in blocks**. A block is like a page of transactions in a book.
- Each block is **appended to the digital ledger** like adding pages in a book.
- The **blocks are chained together** and secured using a **cryptographic hash**, like binding a book.
- This book is **public, permissionless** & fully transparent.
- Anyone can download the blockchain from the internet, view the contents, and confirm new transactions.
- The owners of bitcoins are listed using the digital address associated with their public key, which is a hash (or hexadecimal number) so **pseudo-anonymous**.

Bitcoin: The First Cryptocurrency

- **Blockchain**

- The first public key recorded in the genesis block of the Bitcoin blockchain belongs to Satoshi Nakamoto, the inventor:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

- This address is associated with 1,125,150 bitcoins worth \$48 billion (at \$43,340 per BTC).

- **Hashing and SHA-256**

- A cryptographic hash function, or simply “hash,” is a mathematical algorithm that maps data of arbitrary size to a string of a fixed size.
 - A hash is a one-way function – it cannot be decrypted or inverted to reveal the source data.
- Satoshi chose Secure Hash Algorithm 256-bit (SHA-256), which converts any text into a 256-bit representation

Bitcoin: The First Cryptocurrency

- **Satoshi decided the rules, or protocols, for Bitcoin.**
 - A maximum of 21 million bitcoins will be created
 - The maximum size of a block is 1-megabyte (MB)
 - The average block in 2018 contained around 1,500 transactions, creating an upper limit on processing speed of 2.5 transactions per second (vs VISA at 24,000 per second).
 - Transactions would be batched processed with 1 block added about every 9-10 minutes.
 - The hashing algorithm for encryption of blocks is SHA-246.
 - Computers on the Bitcoin network (called nodes) race to find a hash that meets a specific level of difficulty. This level adjusts to ensure the targeted pace of block creation.
 - Verification of transactions is by mining using Proof-of-Work (PoW).
 - The block reward is halved every 210,000 blocks (roughly every 4 years), starting from 50 BTC in 2009. As of 2022, it was 6.25.

Bitcoin: The First Cryptocurrency

- **Proof-of-Work and Mining**

- PoW is a mechanism for reaching consensus on the truth, namely confirming Bitcoin transactions have taken place.
- Nodes are chosen at random to verify blocks and receive the reward through a process called **mining**.
- Miners run Bitcoin software that searches for a random number called the **nonce**.
 - When the nonce is hashed with Bitcoin transactions waiting to be verified, it generates a hexadecimal number.
 - The goal is to generate a hash beginning with a specific number of zeros (e.g., **00000000**839a8e6886ab...).
- A miner with this hash sends it over the Bitcoin network for verification.
 - Once other nodes confirm it works, the block is added to the blockchain and the miner is credited with the reward.
 - Mining can be described as *random number guessing*

Bitcoin Block 820,310 (Dec 8, 2023 12:28:09)

Block Hash

00000000000000000000000034fa3d3034746e3c17eb569ee7cfba278ec62367a2222

Relayed By	 AntPool
Difficulty	85.01 T / 67.96 T
Block Reward	6.25000000 BTC
Fee Reward	0.95550104 BTC
Tx Count	3,380
Tx Volume	8,946.94541681 BTC

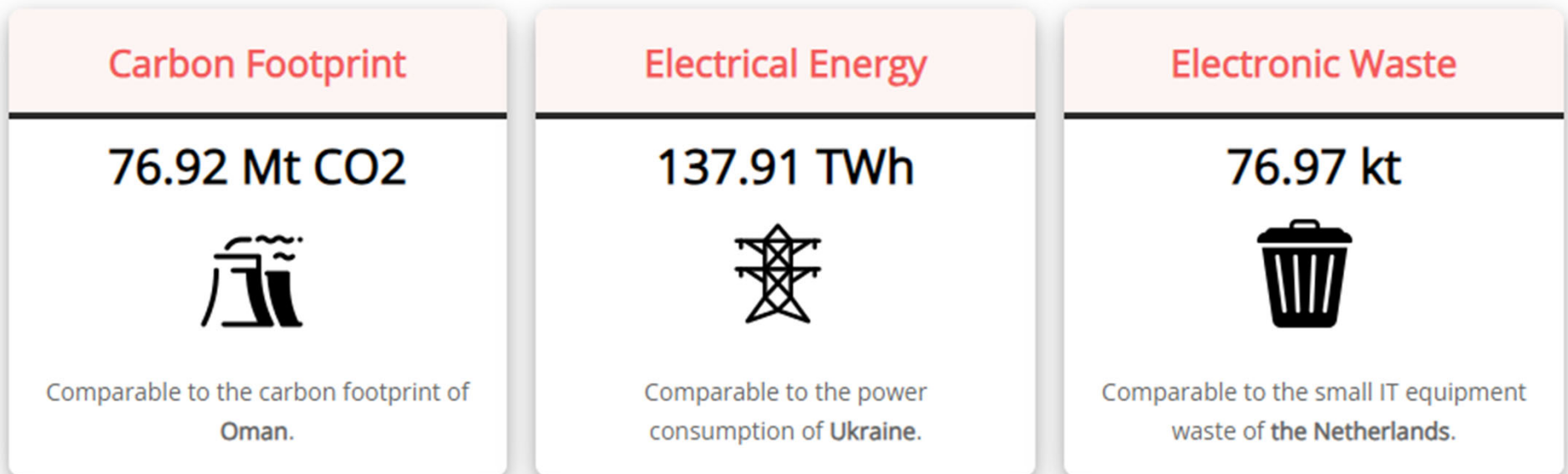
2401f2c6de463b1851501e7d0d2295b868c7349c42151a20d79d9ddd8e08427	Merkle Root
0x2e94c000	Version
0x58184c22	Nonce
0x17042450	Bits

<https://explorer.btc.com/en/btc/block/820310>

Bitcoin: The First Cryptocurrency

- PoW mining is a wasteful activity, as the many nodes searching for the hash consume electricity.
 - At year-end 2022 was estimated at 73 terawatt-hours, or the equivalent annual electricity usage of Austria.
 - At year-end 2023, it was 138 TWh equivalent to Ukraine.

Annualized Total Bitcoin Footprints



Bitcoin: The First Cryptocurrency

- **Proof of Stake (PoS)** consensus mechanism
 - There are many alternative to reach consensus on blocks
 - PoS does not require mining to verify transactions.
 - Instead, a holder of a given cryptocurrency must deposit or “stake” cryptocurrency with the network to be entered into a pool of validators.
 - Validators are randomly chosen to verify transactions and receive the block reward, with the probability linked to the amount of cryptocurrency they have staked.
 - A validator that verifies (or attests) malicious blocks loses their stake as a penalty.
 - In September 2022, the Ethereum network completed its transition from PoW to PoS, reducing its energy consumption by 99.95% (see Chapter 6).

Bitcoin: The First Cryptocurrency

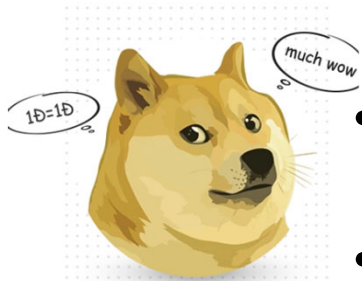
- **Transaction Fees**

- The Bitcoin network does not impose any official transaction fees to process transactions. Unverified transactions wait their turn to be processed in the memory pool or “**mempool.**”
- Senders wanting quicker confirmation can pay a **voluntary fee** to incentivize miners to pick them first.
 - Miners choose transactions offering the highest fee-to-size ratio to maximize the fee for each block.
 - This fee is known as the “**feerate**” and is measured in Satoshi-per-byte, where 1 bitcoin is divisible into 100,000 Satoshis.
- A significant portion of Bitcoin blocks are not filled to capacity, suggesting miners collude to extract higher fees from Bitcoin users.
 - In Dec 2023, 5 mining pools controlled 87% of Bitcoin hashrate (62% in China): <https://hashrateindex.com/hashrate/pools>

Cryptocurrencies










• Alternatives to Bitcoin

- At year-end 2023, Bitcoin was one of 23,000+ coins, tokens, and other cryptoassets with a total market capitalization around US\$ 1.65 trillion.
- Coders altered the Bitcoin source code on GitHub to create altcoins with different features and governance.
 - Litecoin & Namecoin (2011); Peercoin (2012); Gridcoin, Primecoin, NXT and Ripple XRP (2013)...
 - Dogecoin (2013) was introduced as a joke currency that featured the dog from the “Doge” internet meme as its logo.
 - Many were pre-mined and sold to the public through initial coin offerings (ICOs) until they were shut down by regulators in mid-2018
- In mid-2022, the top 10 cryptocurrencies had a market capitalization of \$1.5 trillion, representing 79% of total cryptocurrency market cap, with Bitcoin making up 41%.



Cryptocurrencies <https://coinmarketcap.com/>



#	Name	Price	1h %	24h %	7d %	Market Cap ⓘ
1	 Bitcoin BTC	\$44,518.50	▲ 0.09%	▲ 2.61%	▲ 14.60%	\$870,982,516,232
2	 Ethereum ETH	\$2,370.47	▲ 0.10%	▼ 0.01%	▲ 13.26%	\$284,978,497,810
3	 Tether USDt USDT	\$1.00	▲ 0.00%	▼ 0.02%	▼ 0.02%	\$90,277,823,605
4	 BNB BNB	\$239.72	▲ 0.27%	▲ 2.95%	▲ 4.79%	\$36,364,413,863
5	 XRP XRP	\$0.6682	▼ 0.61%	▲ 3.62%	▲ 8.97%	\$36,053,310,170
6	 Solana SOL	\$73.07	▲ 0.17%	▲ 5.98%	▲ 21.45%	\$31,124,844,159
7	 USDC USDC	\$0.9999	▼ 0.01%	▼ 0.02%	▼ 0.01%	\$24,465,771,742
8	 Cardano ADA	\$0.5484	▲ 1.21%	▲ 19.79%	▲ 42.80%	\$19,368,601,641
9	 Dogecoin DOGE	\$0.1021	▼ 0.81%	▲ 7.69%	▲ 21.94%	\$14,520,734,601

Cryptocurrencies

- **Alternatives to Bitcoin**

- **Ether (ETH)** is the most innovative and transformational cryptocurrency. It is the token used to run decentralized applications (dapps) on the Ethereum blockchain.
 - Ether was launched through a crowdsale in mid-2014 -- the first ICO.
- **Stablecoins** are tokens backed by fiat currencies (e.g. U.S. dollar), commodities (gold, oil), other cryptocurrencies, or nothing at all (algo stables).
- Cryptocurrencies have become a major asset class traded 24 hours per day, 7 days per week on over 400 unregulated exchanges globally
 - Leading cryptoexchanges are Binance, Coinbase, and Kraken.

<https://www.economist.com/finance-and-economics/2023/11/22/another-crypto-boss-falls>

Another crypto boss falls

Changpeng Zhao may face jail, while his firm pays a \$4.3bn fine

Cryptocurrencies

• Trading and HODLing Cryptocurrencies

- Crypto investors may be called “natives,” “newbies,” and “the curious.” The most successful are “whales.”
- Investors who do not sell are “HODLers” in reference to a 2013 Bitcoin forum post by an apparently inebriated user who wrote, “I AM HODLING.”
 - It may also be translated as "Hold On for Dear Life!"
- Bitcoin futures contracts started on CME in Dec 2017.
 - Bitcoin margin trading, exchange traded funds (ETFs), and derivatives have followed.
- Markets are unregulated and segmented, with no single data feed and different prices on different exchanges
 - Cryptocurrencies have gained notoriety due to their association with criminal activity and fraudsters, and regulators cracking down in many countries.

Cryptocurrencies

• Hard Forks



- When the holders of a cryptocurrency disagree and vote to split, it can lead to the creation of a new digital coin with a similar name.
 - A new blockchain is created to verify new transactions; these new coins are no longer recognized as valid by the original blockchain.
 - Both coins share the same transaction history up to the fork.
- Bitcoin Cash forked on Aug 1 2017 at block 478,558 on the Bitcoin blockchain.
 - The hard fork was in response to Segregated Witness (SegWit), which aimed to increase processing speed.
 - Bitcoin Cash introduced larger block size up to 8M, requiring a more complex mining process that favored large miners with more computing power.

Cryptocurrencies

- **Initial Coin Offerings (ICOs)**

- Cryptocurrencies are created through mining (Bitcoin) or through a crowdsale of pre-mined tokens (ICO).
- Ethereum pioneered the crowdsale in 2014, but the term ICO was first used for Breakout Coin (BRO) .
- ICOs exploded in 2016, but were shut down in mid-2018.

Table 5.3. Capital Raised in Initial Coin Offerings (ICOs)

Period	Number of ICOs	Capital raised (US\$ millions)	Media mentions of ICOs ²
2014	7	30.4	7
2015	7	8.6	0
2016	43	256.4	50
2017	343	5,482.0	3,069
2018, first half ¹	<u>460</u>	<u>14,295.4</u>	<u>7,397</u>
Total	860	\$ 20,072.8	10,523

1. January 1 to July 31, 2018. 2. Search in Factiva for "initial coin offering" or ICO w/10 (crypto* or crowdsale)
 Source: CoinDesk ICO Tracker; Factiva.

Cryptocurrencies

- **Initial Coin Offerings (ICOs)**

- All the marketing, book building, and pricing takes place over the internet.
- Instead of an offering document, the founders would post a “whitepaper” online, explaining how the proceeds will be used.
 - In June 2018 the cryptocurrency EOS raised \$4.2 billion to build an open-source blockchain for businesses.
- Purchasers subscribe during a month-long period, placing buy orders using fiat currency or other crypto (bitcoin, ether).

Case Study: Ripple XRP's Search for a Use-Case

- Ripple Labs runs an interbank payments network called the RippleNet (founded 2011)
 - Goal: to create a global interbank payments network to allow for fast money transfers across borders
 - Ripple's original design needed a cryptocurrency XRP to make the transfers, but the banks did not want it.
 - Founders pre-mined 100 billion XRP tokens and kept 20 billion for themselves
 - From 2012 to 2016, Ripple raised \$55 million in funding from leading VCs and financial institutions
 - Transactions on the *permissioned* distributed ledger, are verified by 35 trusted third parties, not by mining.
 - Transfers are executed within five seconds; users can track the transfer end-to-end on a mobile app.
 - XRP rose from \$0.03 in mid-2017 to \$3.30 by Jan 2018...

Case Study: Ripple XRP's Search for a Use-Case

- **What's the problem with XRP?**
 - In Jan 2018, it came out that RippleNet's bank members were not using XRP for money transfers.
 - Banks preferred fiat currencies, leaving XRP with no use-case.
 - XRP is a purely speculative asset with no value behind it.
 - It crashed from \$3.30 in Jan 2020 to \$0.14 in Mar 2020.
 - Then miraculously, like a phoenix, it began to climb during COVID, with big swings over the next 18 months.
 - As of year-end 2023, XRP was \$0.67 with a market capitalization of \$36 billion.
 - Whether the wisdom of the crowds proves to be true or not remains to be seen...

Cryptocurrency Growing Pains

- Like any radical innovation, cryptocurrencies have faced growing pains.
 - These pain points led to more innovations to smooth the way for growth and mainstream adoption.
- **Cryptowallets: From Paper to Hardware**
 - The Bitcoin Core software creates a “wallet” where the user can store the addresses of bitcoins on a designated node on the Bitcoin network.
 - In the early years, the only way to own and transfer a bitcoin was P2P from one node to another.
 - Hodlers secured their bitcoins against theft by storing the addresses offline, either encrypted on a computer or a USB key, or on a piece of paper locked up somewhere.
 - Many coins were accidentally thrown away, lost, stolen, or hacked...

Cryptocurrency Growing Pains

- **Cryptowallets: From Paper to Hardware**

- Cryptocurrency wallets solve this storage pain point.
 - A wallet is a software application or hardware device used to receive and send cryptocurrencies.
 - A user needs a public key and a private key to transfer coins. The public key is shown on the blockchain where the crypto is held.
 - The wallet stores the user's private key, as well as a recovery seed (a list of words in a specific order that will open it).
- There are two types of cryptowallets:
 - A **software wallet** ("hot wallet") is an app connected to the internet. It is convenient but less secure and can be hacked.
 - A **hardware wallet** ("cold wallet") is a USB that stores this information. It is also called cold storage because it is not connected to the internet.
 - The first hardware wallet was the Trezor, sold in 2014. It included two-factor authentication and was easy to use.

Cryptocurrency Growing Pains

• **Cryptoexchanges: Marketplaces or Honey Pots?**

- Electronic cryptoexchanges facilitate buying and selling of cryptocurrencies for a fee.
- Most (but not all) exchanges require customers to register and verify their identity (“know your customer”).
- A customer transfers funds (either fiat or crypto) into an account to start trading.
- The coins are effectively owned by the exchange. It holds the private keys and is listed as owner on the blockchain.
- This set-up is convenient but creates a security risk, turning the cryptoexchange into a honey-pot for hackers.
 - In 2014 Mt. Gox filed for bankruptcy after revealing that hackers had stolen approximately 850,000 bitcoins valued at \$460 million over a period of years.
 - Other hacks: Bitfinex (2016); Binance, Nicehash (2017); Coincheck, BitGrail, Coinrail, bethumb, Zaif (2018).

Cryptocurrency Growing Pains

- **Scams, Bans, and Criminal Cases**

- With crypto rising in value, it inevitably attracted criminals and scam artists, and the scrutiny of regulators
 - Researchers found that 80% of ICOs in 2017 were scams
 - The *Wall Street Journal* reviewed 3,291 ICO whitepapers and found 2,000 of them showed signs of fraudulent activity, improbable returns, and plagiarism.
- In 2017, the U.S. SEC stepped in to regulate ICOS arguing a digital token was an investment contract under the “Howey test.”
 - Any future ICOs would need to be registered and the exchanges that traded in them would need to be regulated.
 - The SEC established a Cybersecurity unit and cracked down
- Regulators globally acted to shut down the ICO market.
- The SEC warns, “If the investment sounds too good to be true, it probably is.”

Cryptocurrency Growing Pains

- **Central Bank Digital Currencies**

- Critics argue Bitcoin is not money because it does not meet all three functions of money: unit of account, medium of exchange, and store of value.
 - Bitcoin may function as unit of account, but it is unsuccessful as medium of exchange, as few merchants accept it for payment.
 - The constant volatility of Bitcoin undermines its usefulness as a store of value.
- More than 80 central banks are investigating the creation of digital versions of fiat currencies, known as central bank digital currencies (CBDCs).
 - The CB would act as trusted intermediary to verify transactions
 - Will a CBDC be recorded on a blockchain or not?
 - Will a CBDC undermine the country's fiat currency or its conduct of monetary policy?
 - Will a CBDC be available for small, retail transactions?

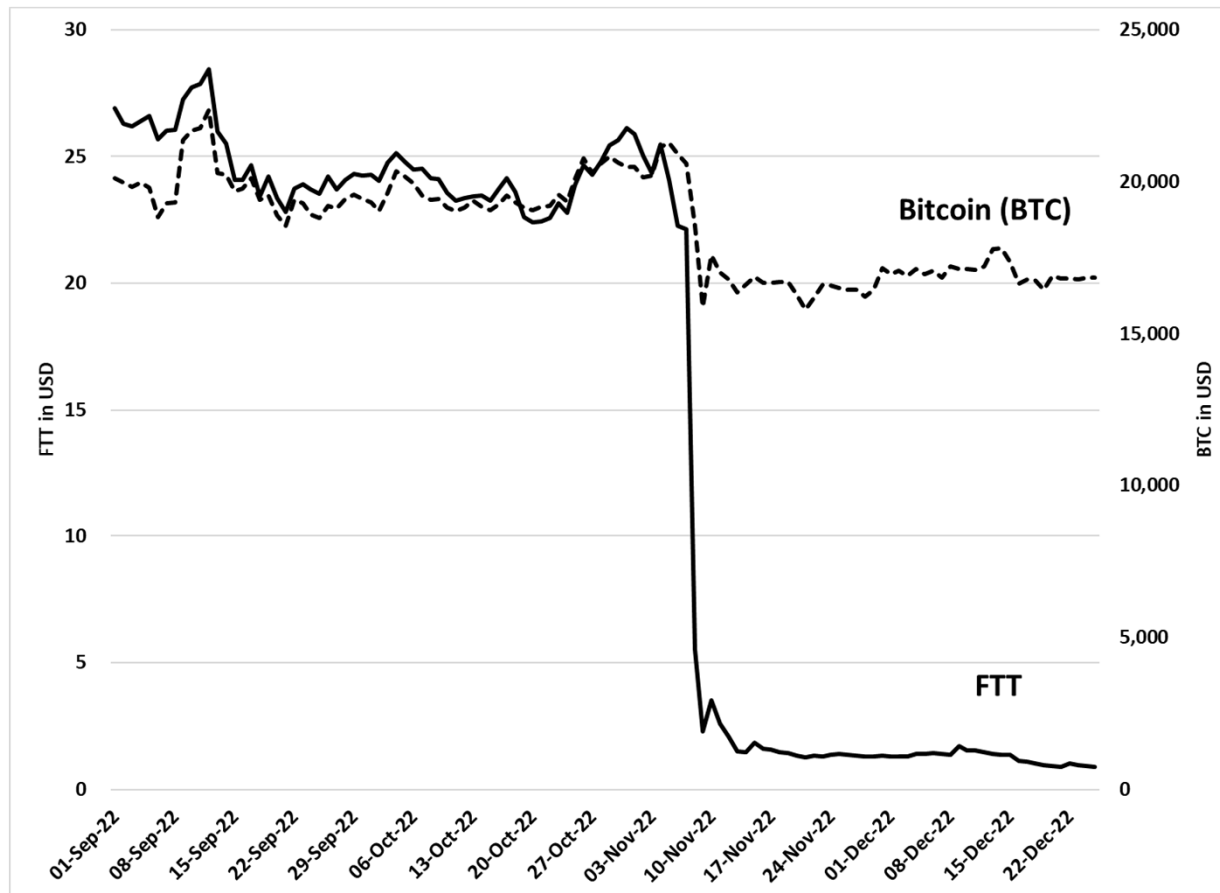
Case Study: The Collapse of FTX Cryptoexchange

- The story of Sam Bankman-Fried is as old as finance
 - In 2019, 27-year old SBF launched the cryptoexchange FTX Trading Ltd. and its native cryptocurrency token, FTT.
 - FTX specialized in trading of derivatives, allowing customers to take leveraged positions in crypto.
 - SBF also ran Alameda Research, a hedge fund focused on quantitative trading in crypto.
 - At its peak in 2021, FTX had over one million users and was the third largest cryptoexchange by volume.
 - The token FTT peaked at US\$80.
 - SBF had a personal worth estimated at US\$26.5 billion.
 - At year-end 2022, SBF was extradited in handcuffs from the Bahamas to the United States.
 - In Nov 2023, he was found guilty of fraud, conspiracy, and money laundering. He had misappropriated \$8 billion of customer funds, making it one of the largest frauds in U.S. history.

Case Study: The Collapse of FTX Cryptoexchange

- A Nov 2022 CoinDesk article pointed out that \$5.8 billion of the \$14.6 billion in assets on Alameda's balance sheet was the token FTT, issued by FTX, financed by \$7.4 billion in loans. When rival exchange Binance liquidated its \$2 billion holdings in FTT, the disclosure triggered a run.

Figure 5.3. FTT vs. Bitcoin



Case Study: The Collapse of FTX Cryptoexchange



• What happened?

- In 2014 SBF graduated from MIT then worked for a proprietary trading firm in New York City.
- In 2017 he quit to work for the Centre of Effective Altruism before setting up his hedge fund, Alameda Research.
- In 2019 he founded FTX to allow trading in crypto derivatives.
 - Big investors backed FTX including Sequoia, BlackRock, Binance, pension plans, & sovereign wealth funds.
 - SBF became a star speaking to the media, lobbying regulators, and giving testimony (+ donations) to politicians.
- By 2021, SBF was using customer funds from FTX to finance trading by Alameda – much of it in the token FTT.
 - When FTT collapsed in 2022, the loans could not be repaid and the customer funds were lost. FTX and Alameda were bankrupt.
 - The bankruptcy lawyer stated that SBF and his execs ran the company “with a lack of corporate controls that none of us in the profession ... have ever seen.”

Crypto Research Findings

- **Cryptoeconomics** is the study of Bitcoin, cryptocurrencies, and blockchain
 - Researchers have studied trust, operational efficiency, and stability
 - Public trust has been undermined by Bitcoin's association with illegal activity on Silk Road and the darknet, incidents of price manipulation, hacks and frauds, and high price volatility.
 - Some researchers conclude that Bitcoin is an intrinsically worthless, storable, non-dividend paying object that will never replace the U.S. dollar.
 - Others look at how a more efficient crypto economy can be built on a different blockchain, called DeFi (Ch. 6)

Crypto Research Findings

- Research highlight many risks to crypto currencies:

Table 5.6. Risks to HODLers of Cryptocurrencies

Risk	Description
Price risk	Users face market risk due to the extreme volatility in Bitcoin prices versus fiat currencies and other coins.
Counterparty risk	Unregulated cryptoexchanges are a source of counterparty risk for cryptocurrency holders, along with wallets, smart contracts, and other protocols. Any protocols that act as financial intermediaries on a cryptocurrency network are a honey pot for thieves.
Settlement risk	Bitcoin transactions may be delayed, and payments are irreversible, creating transaction (or settlement) risk. If bitcoins are sent due to error or fraud, the system offers no built-in mechanism to undo this event.
Operational risk	Bitcoin's technical infrastructure and security creates operational risk. A user's private key may be lost through human error, hacks, or malware that steals wallet credentials and private keys. The arrival of quantum computing will undo the security provided by hashing algorithms.
Governance risk	Bitcoin is governed by a pro bono group of programmers who maintain the code and network, posting updates and dealing with technical problems. This group was responsible for the Segregated Witness (SegWit) protocol update, where the format of a Bitcoin transaction was changed to remove the witness information from the input field of the block. ⁵⁶ The breakdown of consensus can lead to forks, such as the August 2017 fork that led to the creation of Bitcoin Cash. Other forks led to Bitcoin SV, eCash, and Bitcoin Gold.
Legal and regulatory risks	Bitcoin is subject to legal and regulatory risks that vary across countries and over time. Many users believe Bitcoin transactions are anonymous. They are in fact pseudonymous, with each transaction linked to the user's public key published on the blockchain. The user's identity may be revealed through a hack of an exchange, when they convert Bitcoin into fiat currency, or when paying retailers with Bitcoin.

Crypto Research Findings

- **Market Microstructure and Trading**

- This research examines with how prices are determined, information is created, and trading takes place. Trading is dominated by individuals, not institutional investors.
- Bitcoin returns and trading volume exhibit substantial commonality on exchanges around the world. Price changes in Bitcoin explain 80% of movements in other cryptocurrencies.
- Arbitrage opportunities across exchanges have been large, profitable, and recurring despite the introduction of futures and margin trading.
 - Price deviations increase as the Bitcoin price rises, and during unusual events (following hacks and breaches of exchanges).
 - Bitcoin traders may not take advantage of these arbitrage profits due to a lack of capital and sophistication.

Crypto Research Findings

• Asset Pricing and Crypto Returns

- Researchers examine price movements (returns), the volatility prices and returns, and trading and investment strategies.
- From 2011-2018, a crypto portfolio generated a monthly return of 20.4% vs 0.94% for U.S. stocks, but Sharpe ratios were comparable.
- Crypto returns are linked to crypto market movements (beta), the market capitalization of a coin (size), and price momentum over the previous one to four weeks.

Table 5.7. Cryptocurrency Index vs. US Stocks

	Daily		Weekly		Monthly	
	Crypto-currency	US Stock Market	Crypto-currency	US Stock Market	Crypto-currency	US Stock Market
Period: 2011 to 2018						
Average return	0.46%	0.05%	3.44%	0.22%	20.44%	0.94%
Standard deviation	5.46%	0.95%	16.50%	1.98%	70.80%	3.42%
Sharpe ratio ¹	0.08	0.05	0.21	0.11	0.29	0.27

1. While technically not correct, the Sharpe ratio shown is the average return ÷ standard deviation.

Source: Liu and Tsyvinski, 2021.

Questions for Discussion

1. What is cryptoeconomics and why use the term crypto?
2. What is Bitcoin? How did its creator Satoshi Nakamoto address the double-spend problem?
3. What is blockchain? What are its main differences relative to traditional ledgers?
4. What is hashing and SHA-256? How are these two concepts related to proof-of-work and mining of Bitcoin?
5. What are the transaction fees associated with the Bitcoin and how are they determined and allocated among miners?
6. What are altcoins and what were the first ones created? Were they mined or sold through an initial coin offering?
7. What is a hard fork and how did one lead to the creation of Bitcoin Cash?
8. What are cryptowallets? What are cryptoexchanges?
9. What are the risks of using Bitcoin as a means of payment?
10. What have researchers found explains price changes and the cross-section of returns in Bitcoin?

Key Terms

- altcoin
- blockchain
- central bank digital currency (CBDC)
- cryptoasset
- cryptocurrency
- cryptography
- distributed ledger technology
- double-spend problem
- hard fork
- hashing
- HODLer
- Howey test
- initial coin offering (ICO)
- mempool
- mining
- mining pool
- nodes
- nonce
- pre-mined
- private key
- proof-of-work (PoW)
- public key
- Secure Hash Algorithm 256-bit (SHA-256)
- security token
- stablecoin
- token
- utility token
- whitepaper