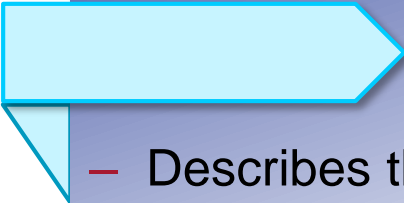


**Cryptocurrencies, Blockchain - Intro**

**FTMBA - Trim 4**

**Jun-25**

***Fintech: n.* A blanket term for disruptive technologies affecting the financial services industry.**

- 
- Describes the intersection between software and technology to deliver financial services.
  - May refer to technical innovation applied in a traditional financial services context or to innovative financial services offerings that disrupt the existing financial services market.

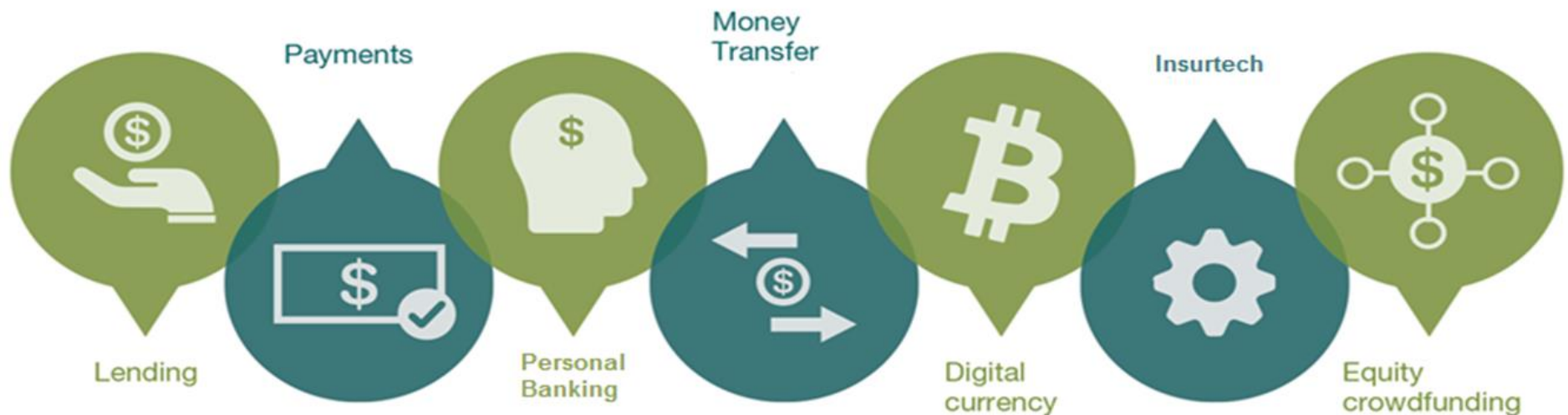
# What is "Fintech"

"Fintech" is combination of the words financial technology

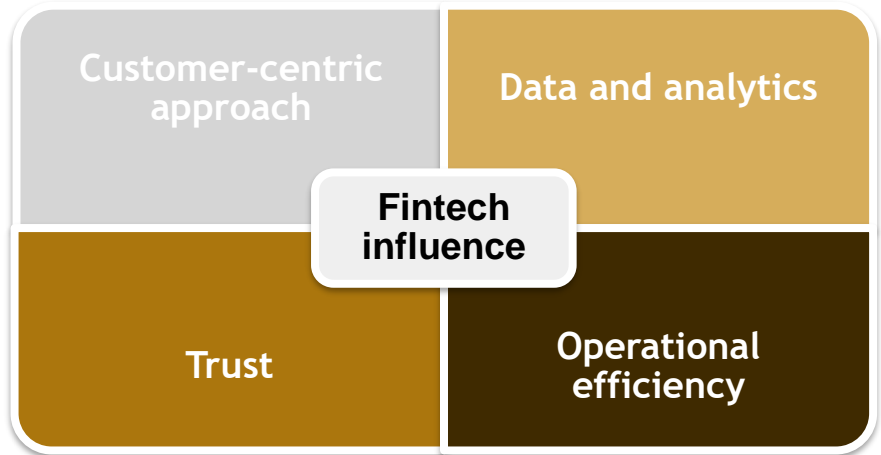
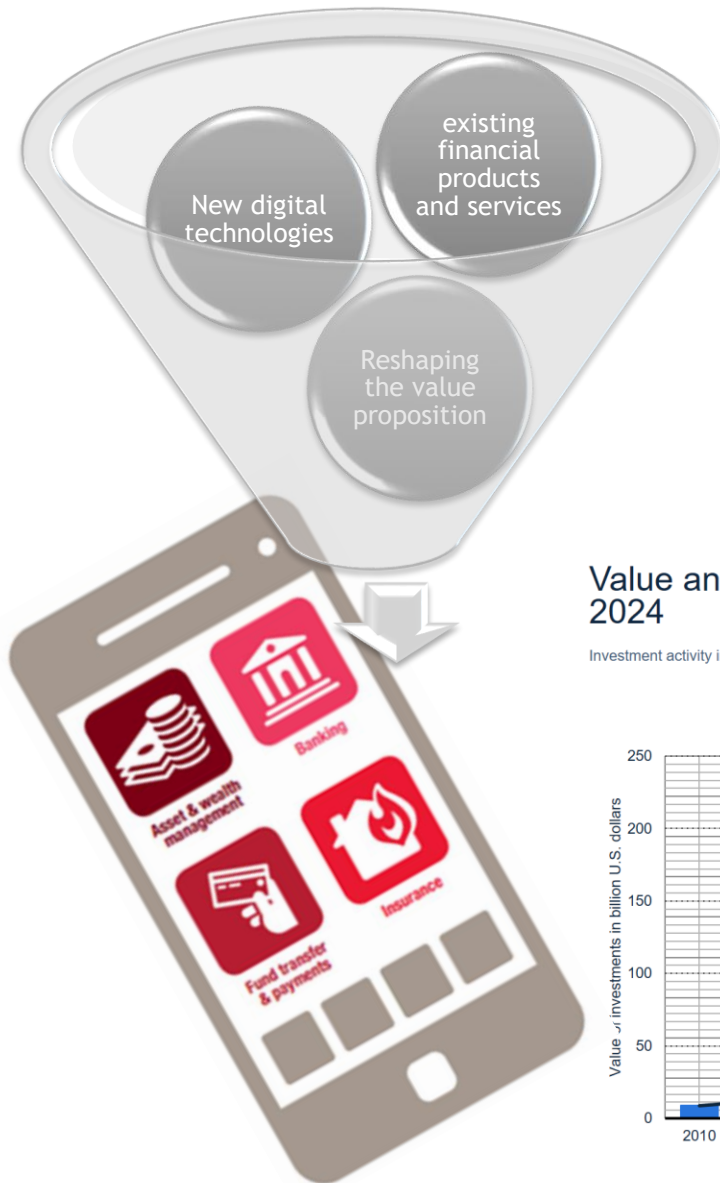
Fintech is a very young industry

Use technology to make financial systems more efficient

## MAJOR FINTECH'S SERVICES SEGMENTS

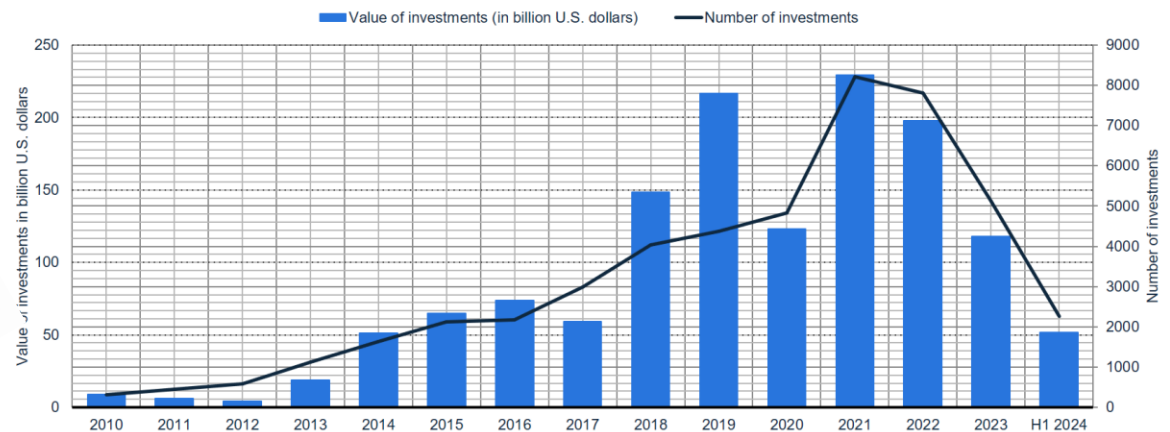


# Influence of Fintech



## Value and number of investments in fintech worldwide from 2010 to 1st half of 2024

Investment activity in fintech globally 2010-2024



# *Transformation through Fintech*

---

- Fintech startups: stepping in between banks, their customers
- Banks: getting side-lined in different areas
- Robo-advisors: replacing human wealth advisors
- Fintech start-ups: distributing insurance plans without the use of agents
- POS technology is going mobile
- Blockchain: streamlining processes throughout financial institutions

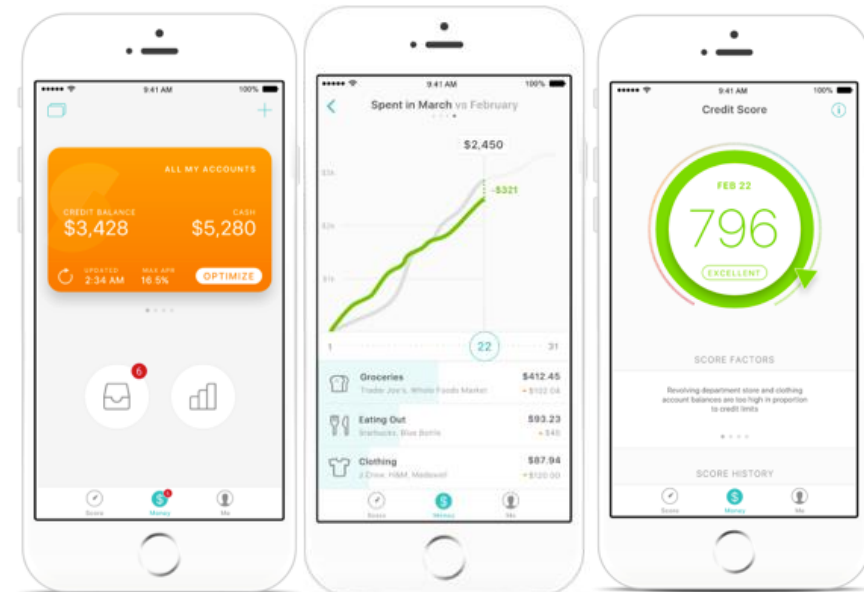
# Disruption Potential

## ■ More efficient information sharing and contract management

### Scope for distributed ledger technology

- Smart contracts can enable automated clearing upon trade completion
- Real time updates on security title and interests updating
- Allowing access to multiple users for robust monitoring
- Increased transparency as information asymmetries are eliminated
- Real time updates on the positions of the underlying collateral with consistent valuation methodologies
- Securely, transparently move securities and assets in seconds or minutes
- Enables point-to-point settlement, lowering the cost and risk of transactions
- Smart contracts can facilitate robust custodian services on decentralised platforms eliminating intermediaries.

## ■ Improved customer experience

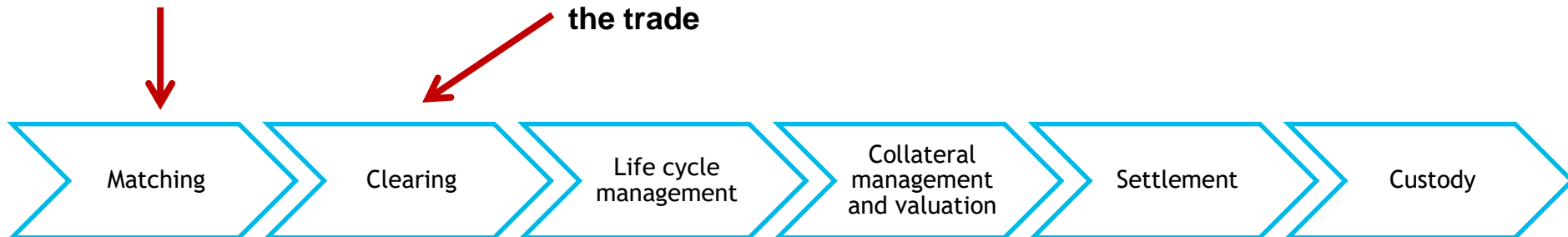


- Financial transactions involve complex steps with multiple verification points

## Example: Securities settlement

All parties have to confirm terms and conditions

Clearinghouse sets up the trade



# Reality

- The Blockchain uses a global network to verify transactions
  - Potential to reduce bank payments, securities trading, and compliance costs
    - As much as \$15 billion-\$20 billion in annual savings by 2022

## Current blockchain

Transaction 999  
Transaction 998  
Transaction 997  
Reference to Prior Block

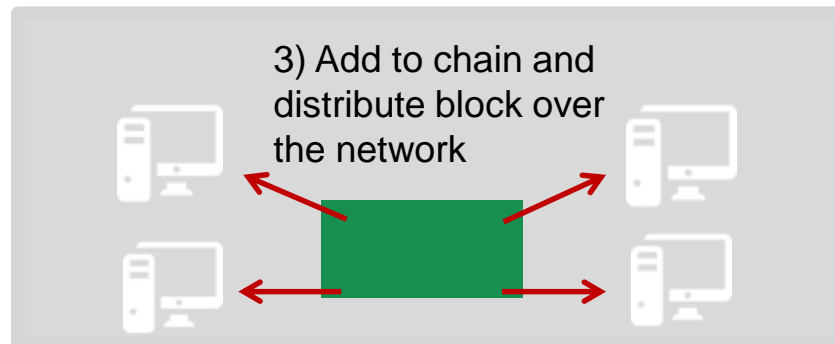


Transaction 996  
Transaction 995  
Transaction 994  
Reference to Prior Block

1) Bundle recent transactions into a block



2) Verify block using cryptography and computing power



## Updated chain

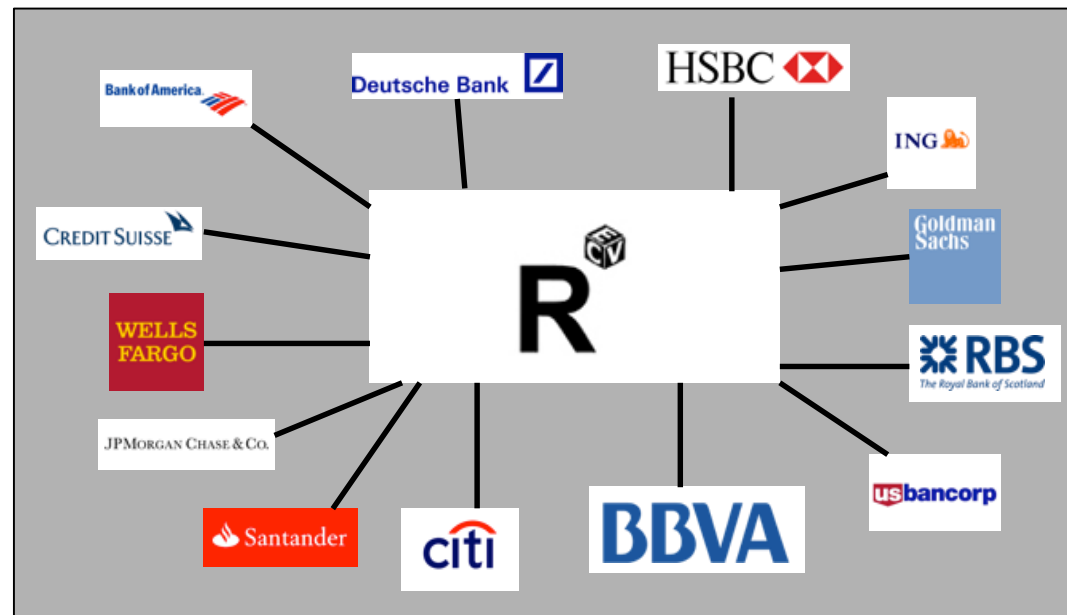
Transaction 1,002  
Transaction 1,001  
Transaction 1,000  
Reference to Prior Block



Transaction 999  
Transaction 998  
Transaction 997  
Reference to Prior Block



# Reality



- Banks: most benefit
  - Banks: burdened with high operating costs
    - Mostly from Intermediaries
  - Companies functioning solely as intermediaries: need to reinvent
- 70 global financial companies: ecosystem of more than 300 firms
  - Build distributed applications on top of Corda (CorDapps)
    - Usage across industries
      - Financial services, insurance, healthcare, trade finance, digital assets

# Introduction

- Money: System of value
  - Facilitates exchange of goods and services in an economy
  - Serves as medium of exchange, unit of account, store of value
    - Unit that things are priced in within a society
    - Can be saved, retrieved, exchanged without loss in value
  - Part of monetary economy
    - Currency refers to paper money/coins circulating in an economy
      - Standardization of money
      - Easier to measure, compare value
    - Credit/electronic records stored in databases in banks/FIs
- Usage allows buyers, sellers to pay less in transaction costs

- Properties of Money: makes it easy to exchange
  - Fungible
    - Allows for exchange, substitution, or return
      - Assumption of equivalent value
    - Units of money are interchangeable with one another
      - Metal coins: standard weight, purity
      - Commodity money: relatively uniform in quality
      - Usage of non-fungible goods as money:
        - » Transaction costs that involve individually evaluating each unit of the good before the exchange
  - Durable
    - Ensures retaining usefulness for many exchanges
    - Not perishable - does not degrade with usage

- Properties of Money (Contd.)
  - Portable: Easy to carry and divide
    - Difficulty in transporting raises transaction costs
  - Recognizable
    - Authenticity, quantity should be readily apparent to users
      - Easy agreement to the terms of an exchange
      - Otherwise rise in transaction costs
        - » Authenticating the goods, agreement on quantity needed for an exchange
  - Stable supply
    - Supply of the item used as money: should be relatively constant over time
      - Prevents fluctuations in value
    - Lack of stability: risk that value might rise or fall
      - Because of scarcity or over-abundance
        - » Before the next transaction

# Introduction

- Currency
  - Fiat, commodity, representative
- Alternative currency
  - Currency or medium of exchange
  - Not a national (fiat) currency
    - Thought of as supplementing or complementing national currencies
  - Usually not legal tender
    - Use is based on agreement between the parties exchanging the currency
  - Complementary currency, Auxiliary currency, Microcurrency
- Barter: exchange systems - trade in items without currency

- ECB (2012) Virtual Currency
  - Type of unregulated, digital money
    - Issued and usually controlled by its developers
    - Used, accepted amongst members of specific virtual communities
  - (2014), Also "Directive 2018/843/EU"
    - Digital representation of value
    - Neither issued/guaranteed by central bank / public authority
      - Not necessarily attached to a fiat currency (legally established)
        - » Does not possess a legal status of currency or money
    - Accepted by natural or legal persons as a means of exchange
      - Which can be transferred, stored or traded electronically
  - As opposed to: Central Bank Digital Currency
    - Digital currency that is issued by a central bank

# Introduction

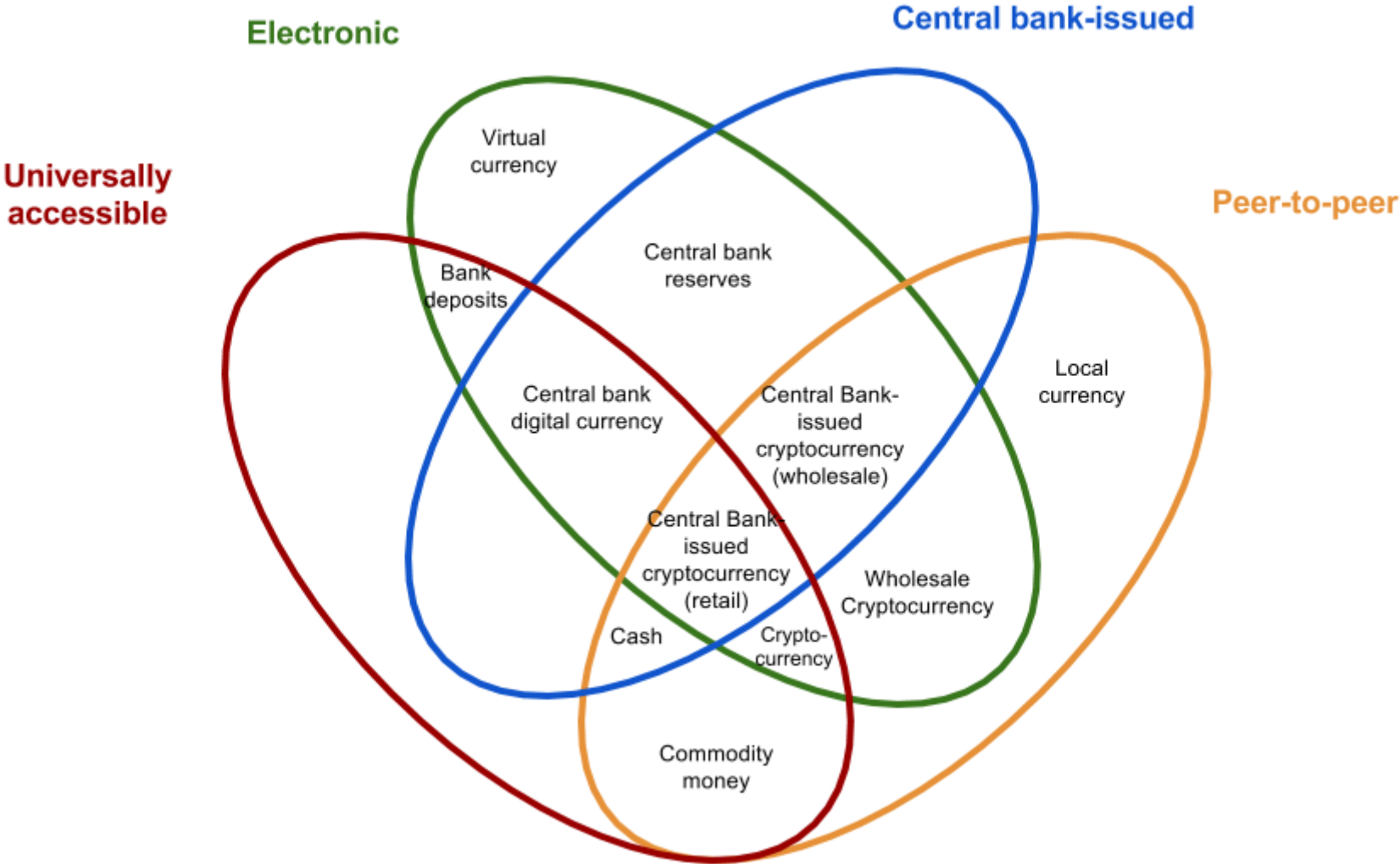
- Digital currency (digital money, electronic money or electronic currency)
  - Type of currency available in digital form
    - In contrast to physical, such as banknotes and coins
  - Exhibits properties similar to physical currencies
    - Can allow for instantaneous transactions, borderless transfer-of-ownership.
  - Digital money can either be centralized or decentralized
    - Central point of control over the money supply
    - Control over the money supply can come from various sources

# Introduction

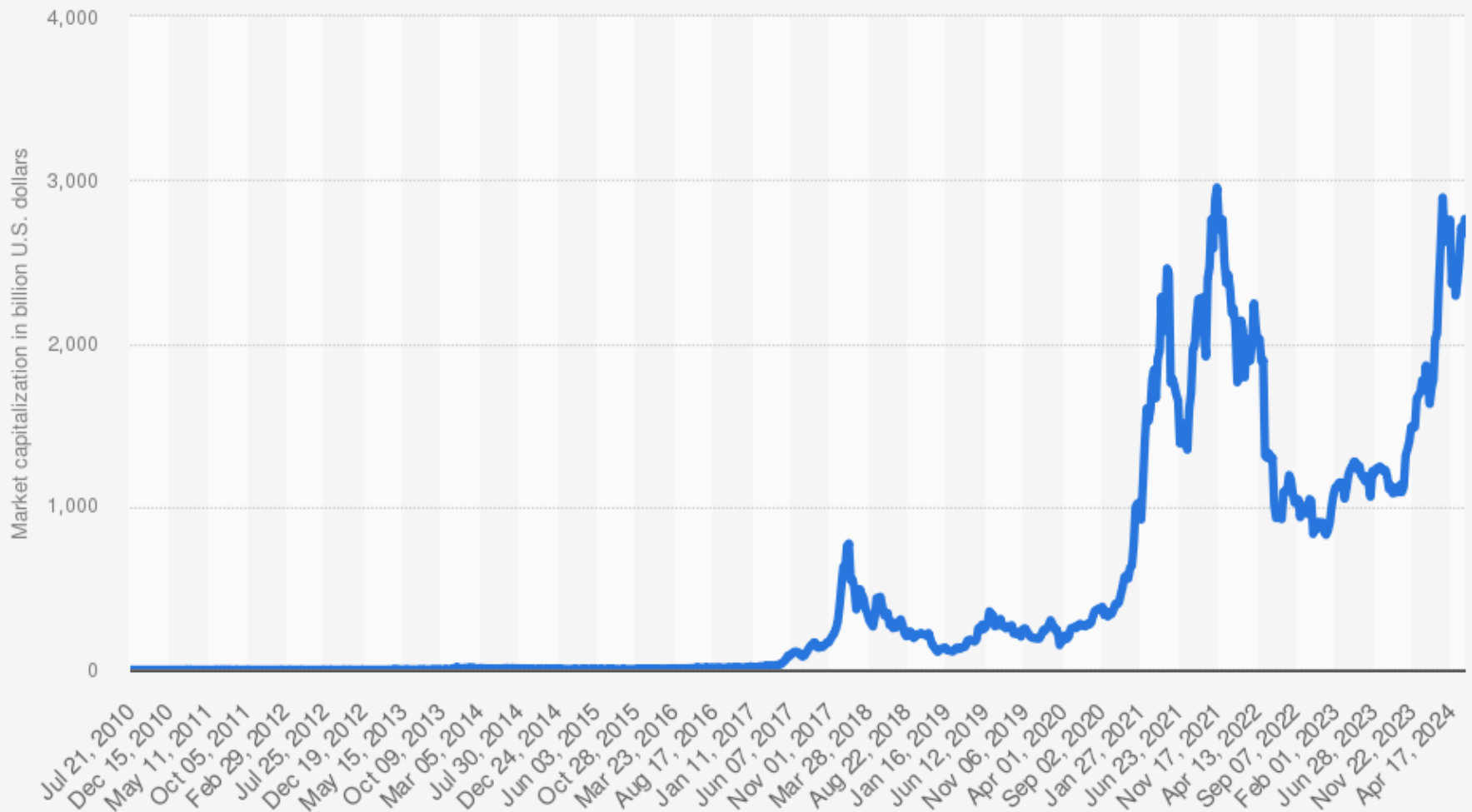
| The money matrix<br>adapted from an ECB work, <i>Virtual Currency Schemes</i> <sup>[2]:11</sup> |             |                  | Money format                   |                                     |                                |
|---|-------------|------------------|--------------------------------|-------------------------------------|--------------------------------|
|   |             |                  | Physical                       | Digital                             |                                |
|   |             |                  |                                | Not based on cryptography           | Cryptocurrency                 |
| Legal status  | Unregulated | Centralized      | Coupon                         | Internet coupon <sup>[note 1]</sup> |                                |
|   |             |                  |                                | Mobile coupon                       |                                |
|   |             | Local currencies | Centralized virtual currencies |                                     |                                |
|   |             | Decentralized    | Physical commodity money       | Ripple, Stellar <sup>[20]</sup>     | Decentralized cryptocurrencies |
|   | Regulated   |                  | Banknotes and coins (cash)     | E-money                             |                                |
|   |             |                  |                                | Commercial bank money (deposits)    |                                |



# Taxonomy of money



## Overall cryptocurrency market capitalization per week from July 2010 to June 2024 (in billion U.S. dollars)



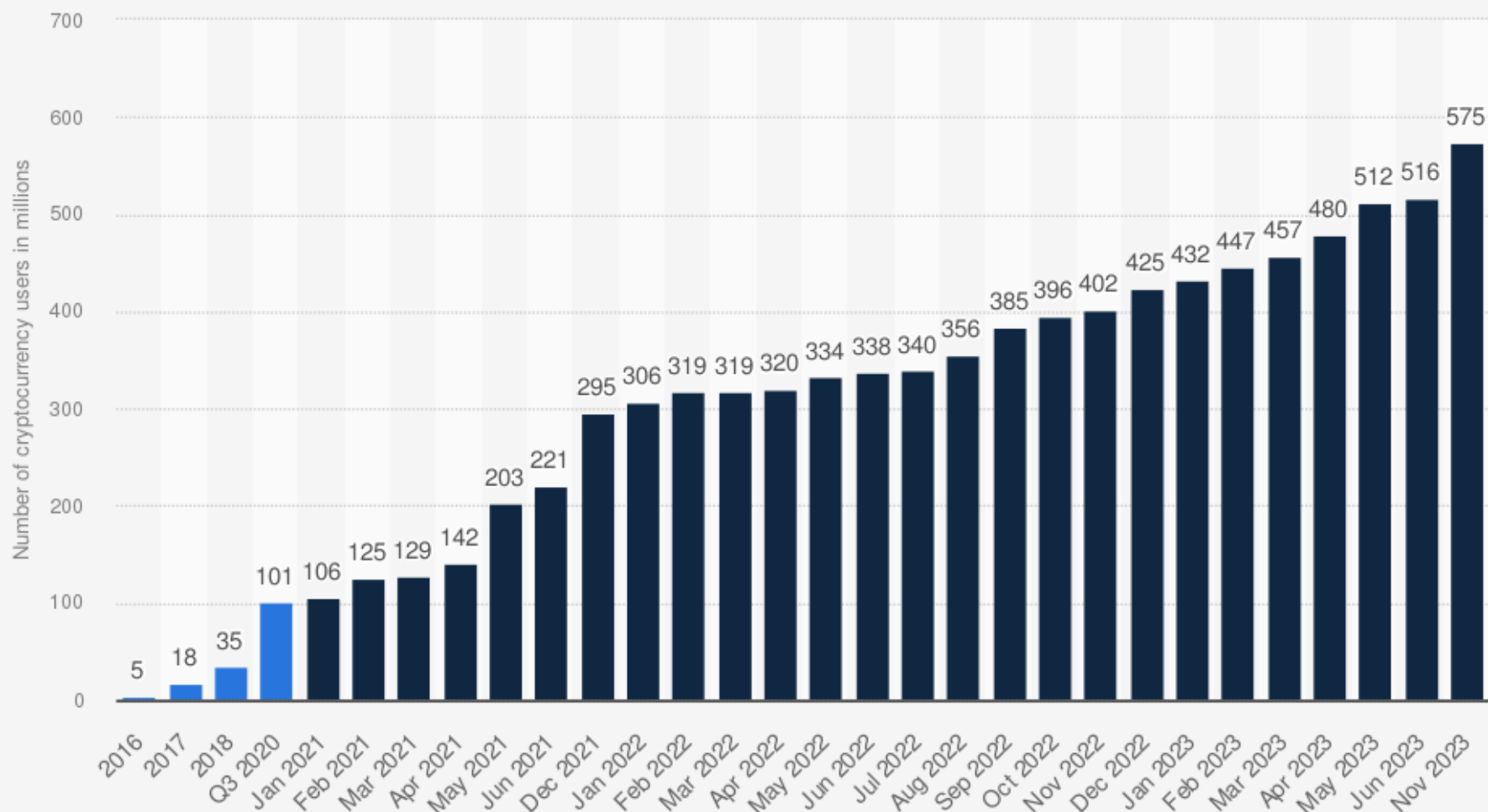
### Source

CoinGecko  
© Statista 2024

### Additional Information:

Worldwide; July 2010 to June 2024; Note that due to changing exchange rates, the USD values as reported can change from time to time. This applies in retrospect.

## Number of identity-verified cryptoasset users from 2016 to November 2023 (in millions)



### Sources

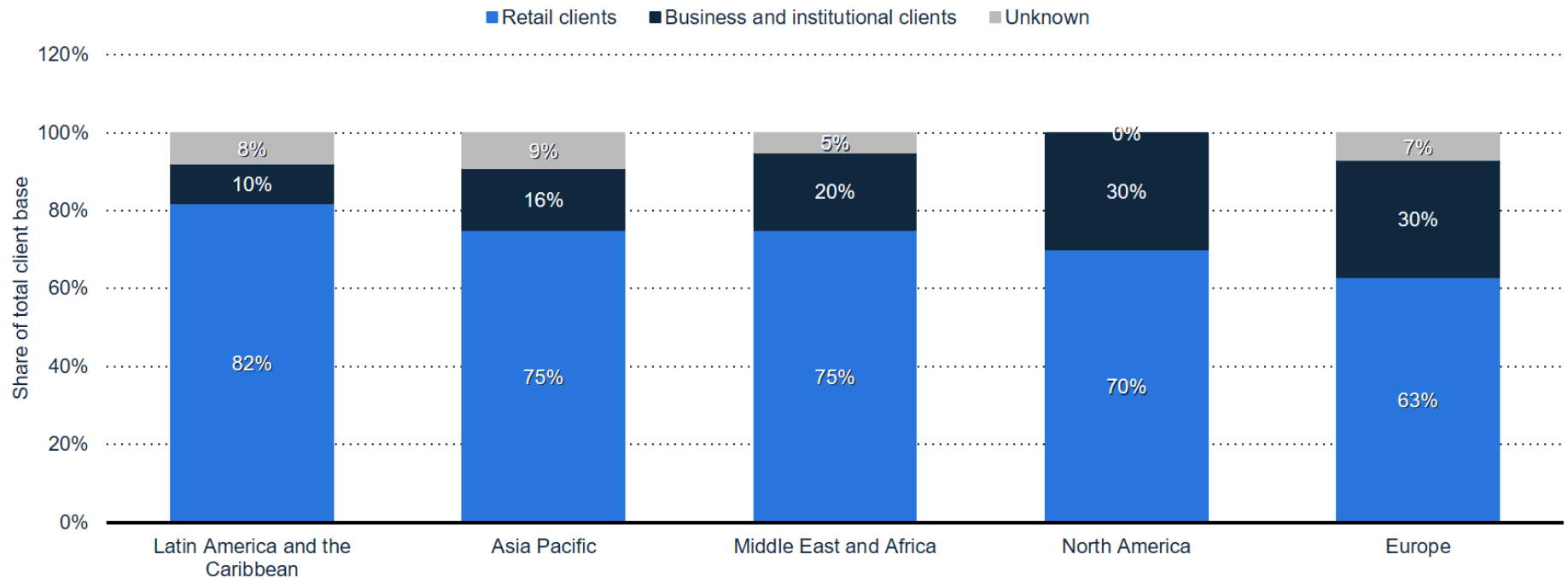
Cambridge Judge Business School; Crypto.com  
© Statista 2024

### Additional Information:

Worldwide; Statista; 2016 to November 2023; Figures as of December 1, 2022; Both sources explicitly state all figures provided are estimates and the methodology used has its limitations

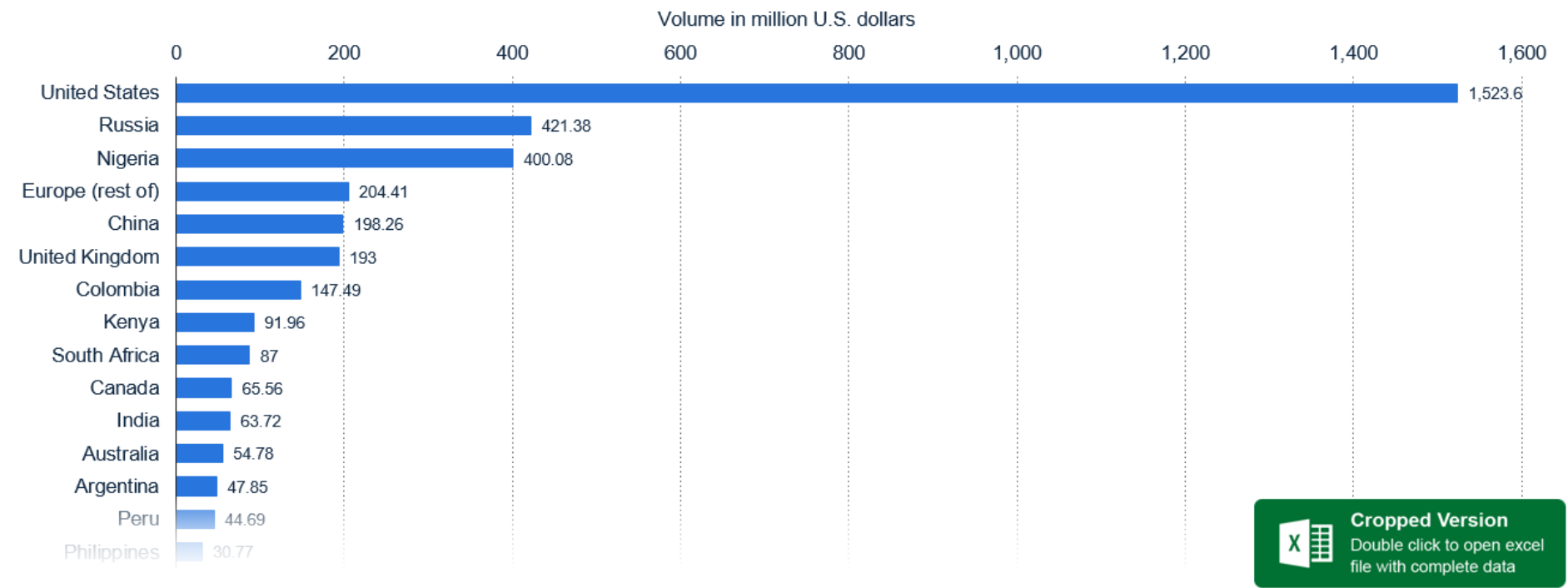
# User type of cryptocurrency services providers in various regions worldwide in 2020 (in millions)

Customer profile of companies that offer cryptocurrency services 2020, by region



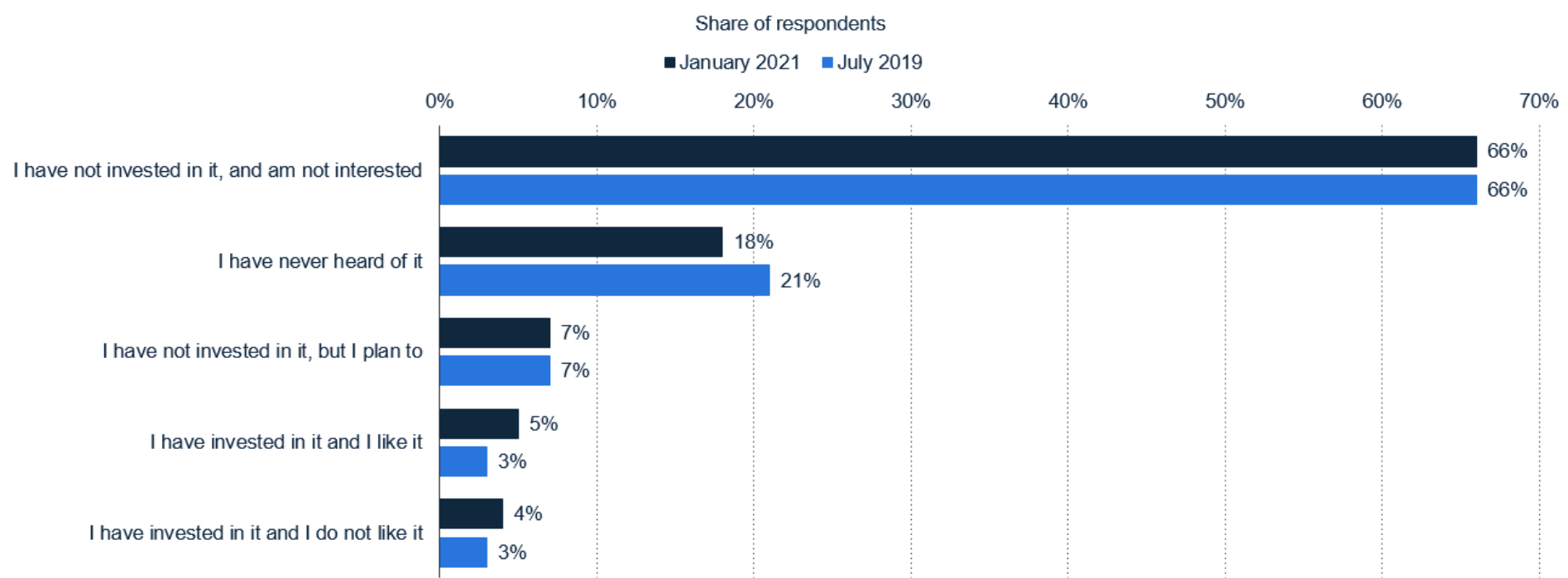
# Bitcoin trading volume, only using domestic currencies, on online exchanges in various countries worldwide in 2020 (in million U.S. dollars)

Bitcoin (BTC) trading volume in 44 countries worldwide in 2020



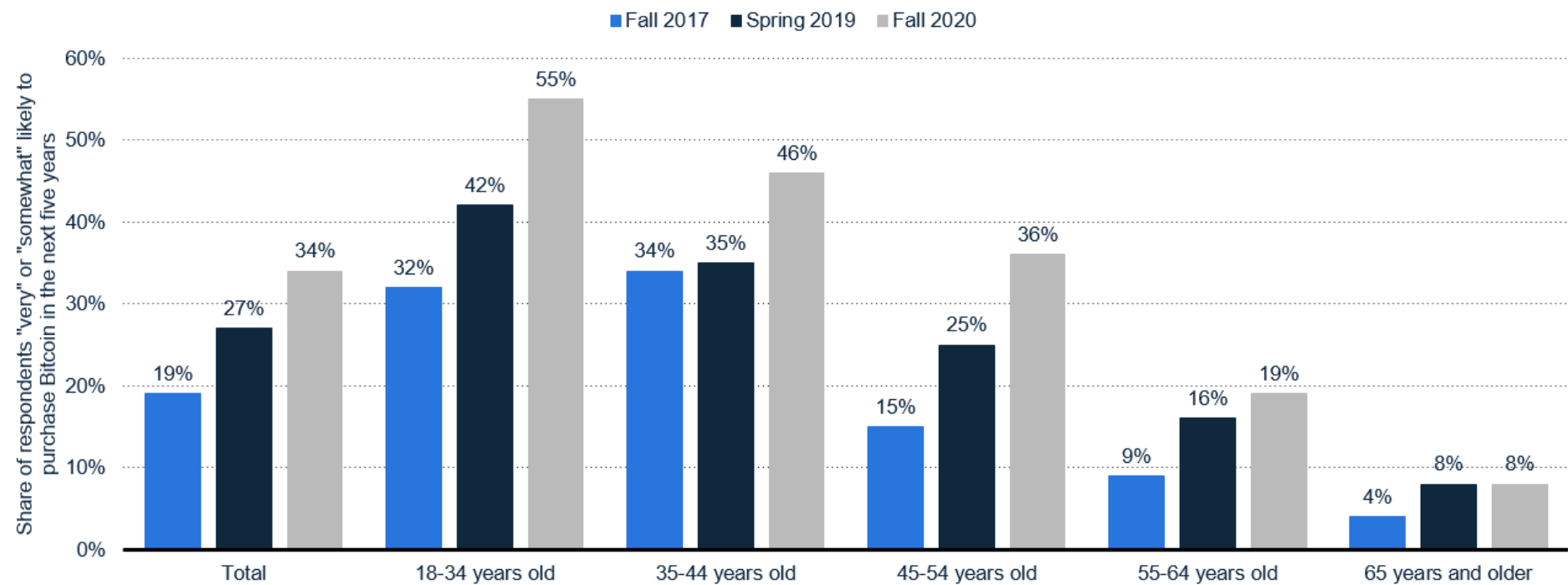
# Use of and interest in cryptocurrency among consumers in the United States in 2019 and 2021

User experience with cryptocurrency in the U.S. in 2019 and 2021



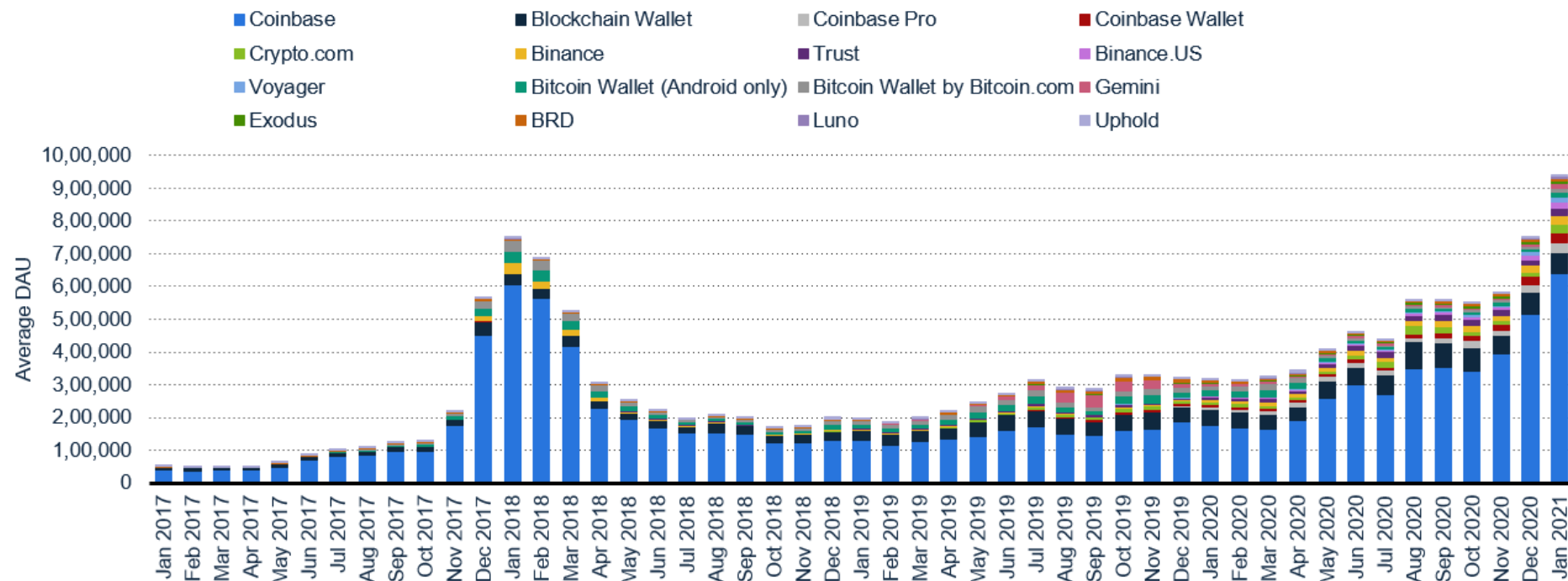
# Age groups in the United States who are likely to purchase Bitcoin in the next five years from 2017 to 2020

Likelihood to buy cryptocurrency in the U.S. 2017-2020, by age



# Average number of daily active users (DAU) of selected apps that allow for cryptocurrency storage in the United States from January 2017 to January 2021

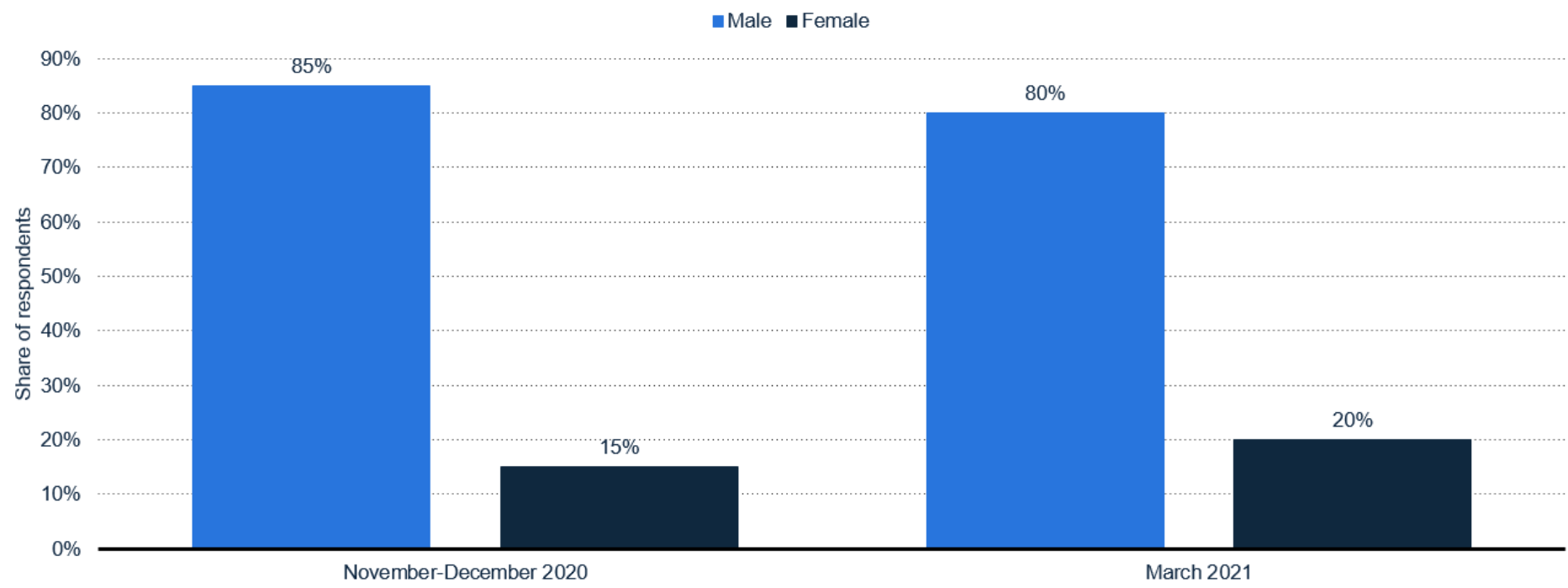
Ranking of cryptocurrency wallet apps in the U.S. 2017-2021





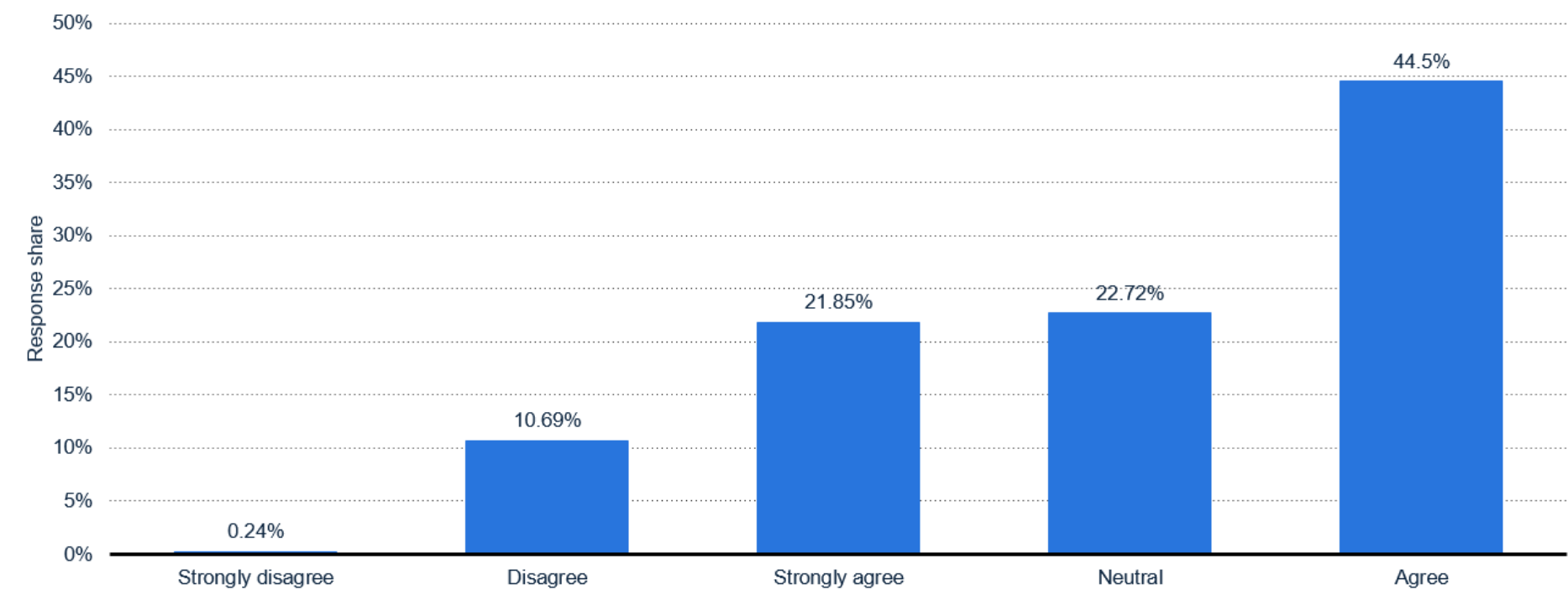
# Share of men and women among the customer base of cryptocurrency exchange CoinDCX who own a cryptocurrency in India in 2020 and 2021

Cryptocurrency ownership among users of India's CoinDCX 2020-2021, by gender



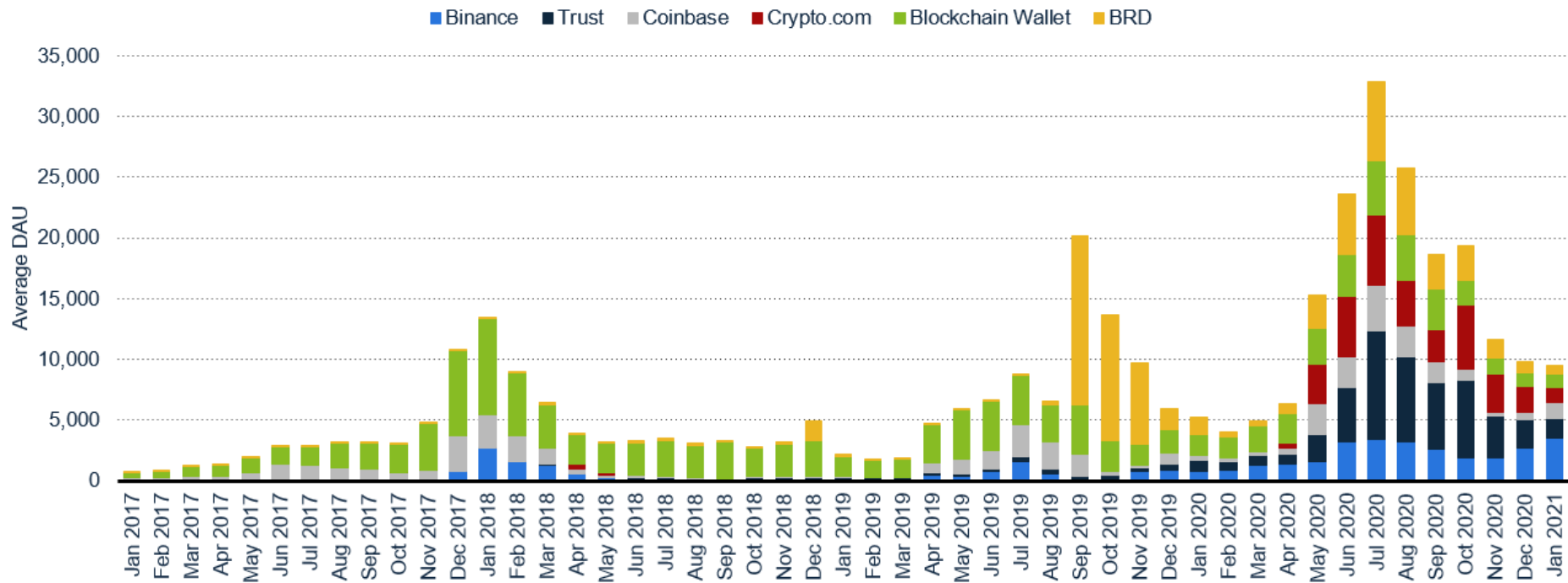
# Intention on use of bitcoin as means of payment in future in India as of July 2020

Intention of bitcoin use as means of payment in future in India 2020



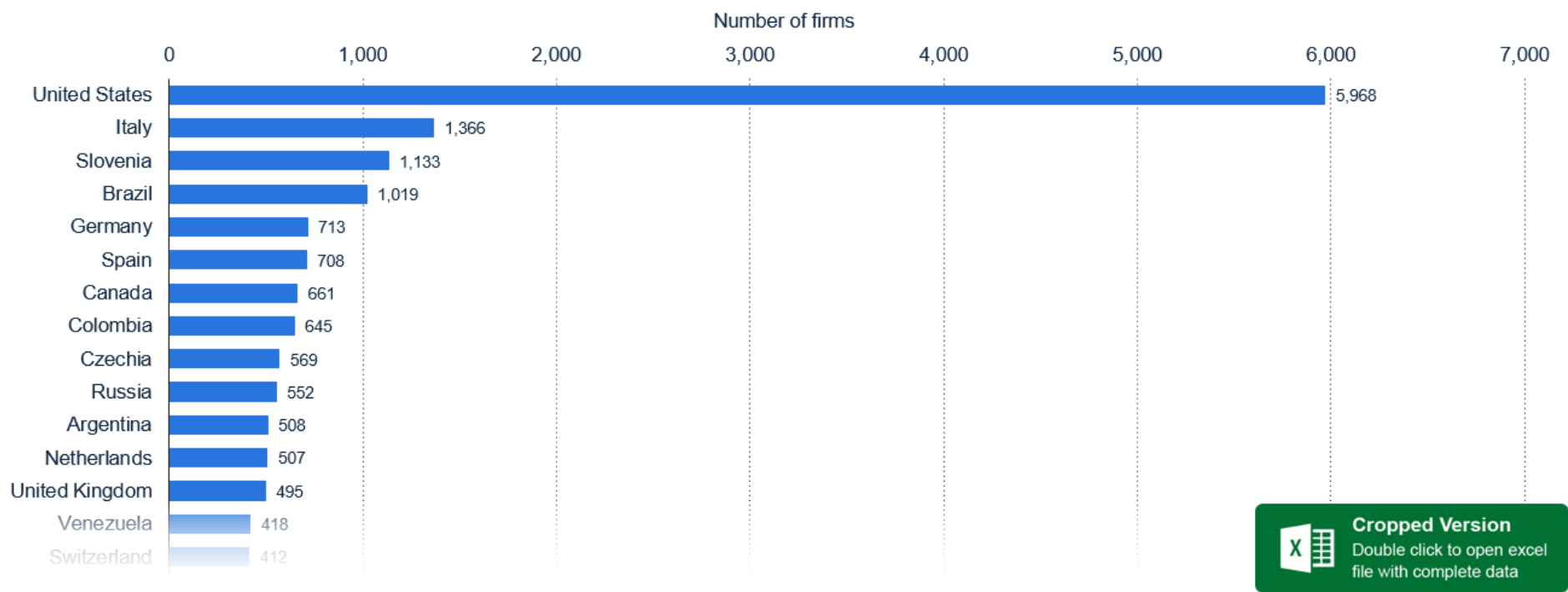
# Average number of daily active users (DAU) of selected apps that allow for cryptocurrency storage in India from January 2017 to January 2021

Ranking of cryptocurrency wallet apps in India 2017-2021



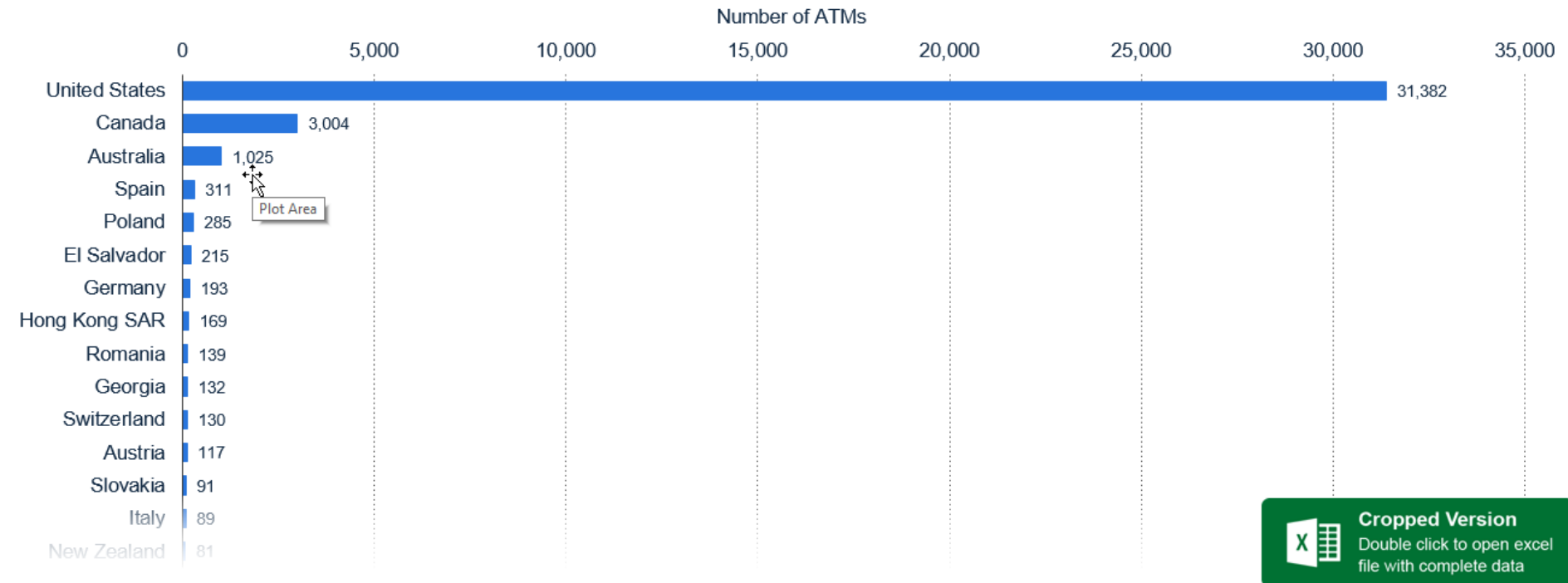
# Number of businesses that either have a cryptocurrency ATM or offer crypto as an in-store payment method as of March 9, 2021, by territory

Companies that accept cryptocurrency payments in 147 countries as of March 9, 2021



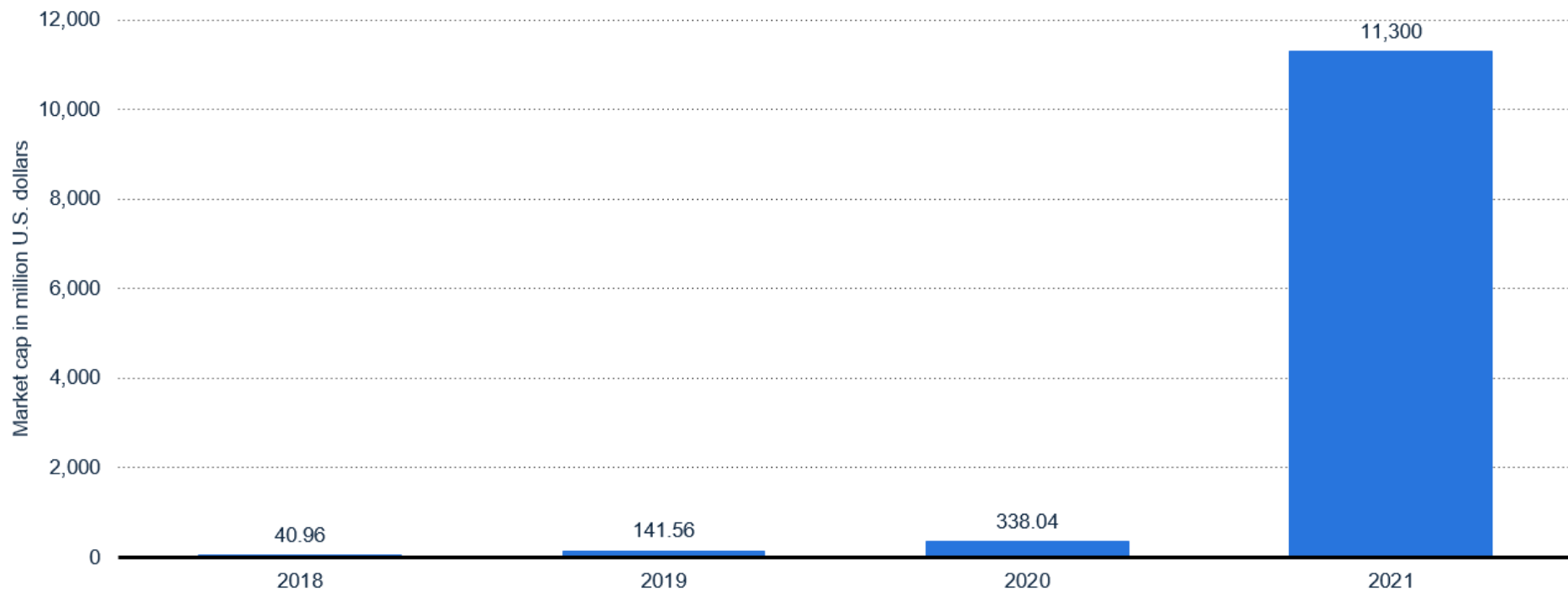
# Number of Bitcoin ATMs in 73 countries and territories worldwide as of May 6, 2024

Bitcoin ATMs in 73 countries worldwide as of May 6, 2024



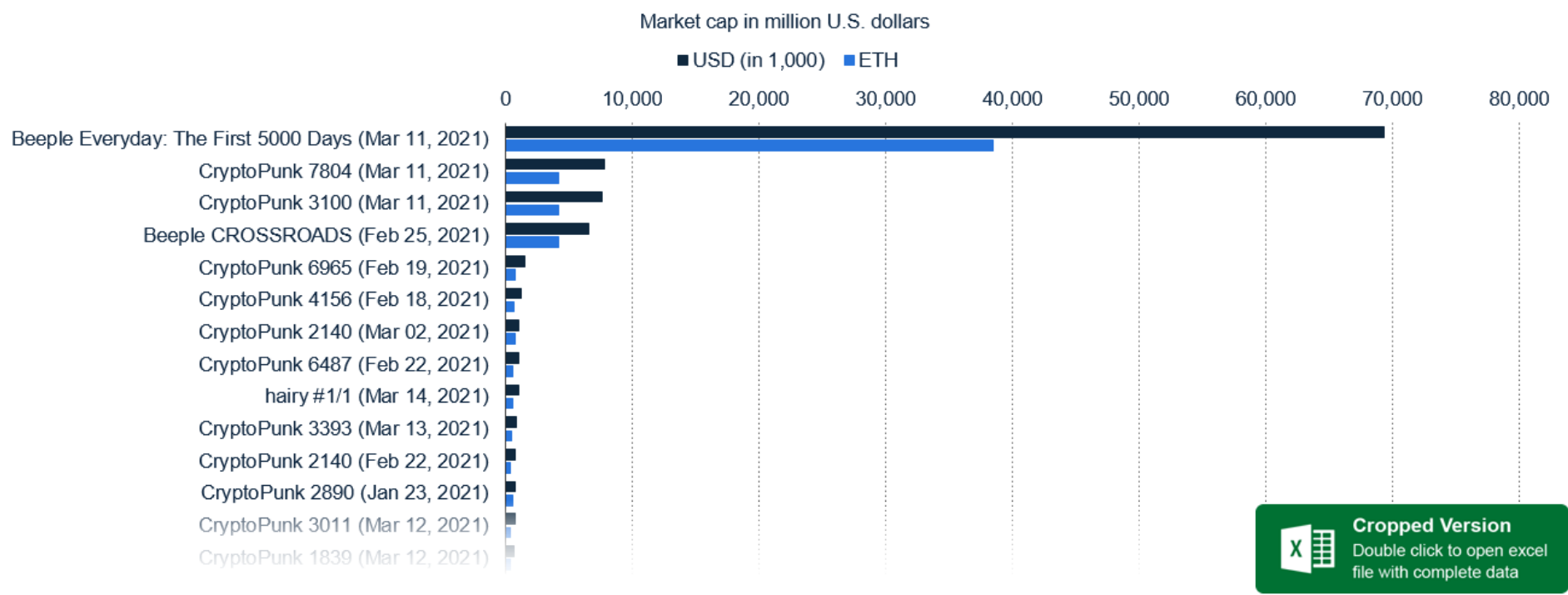
# Market capitalization of transactions globally involving a non-fungible token (NFT) from 2018 to 2021 (in million U.S. dollars)

Annual market cap of NFT worldwide 2018-2021

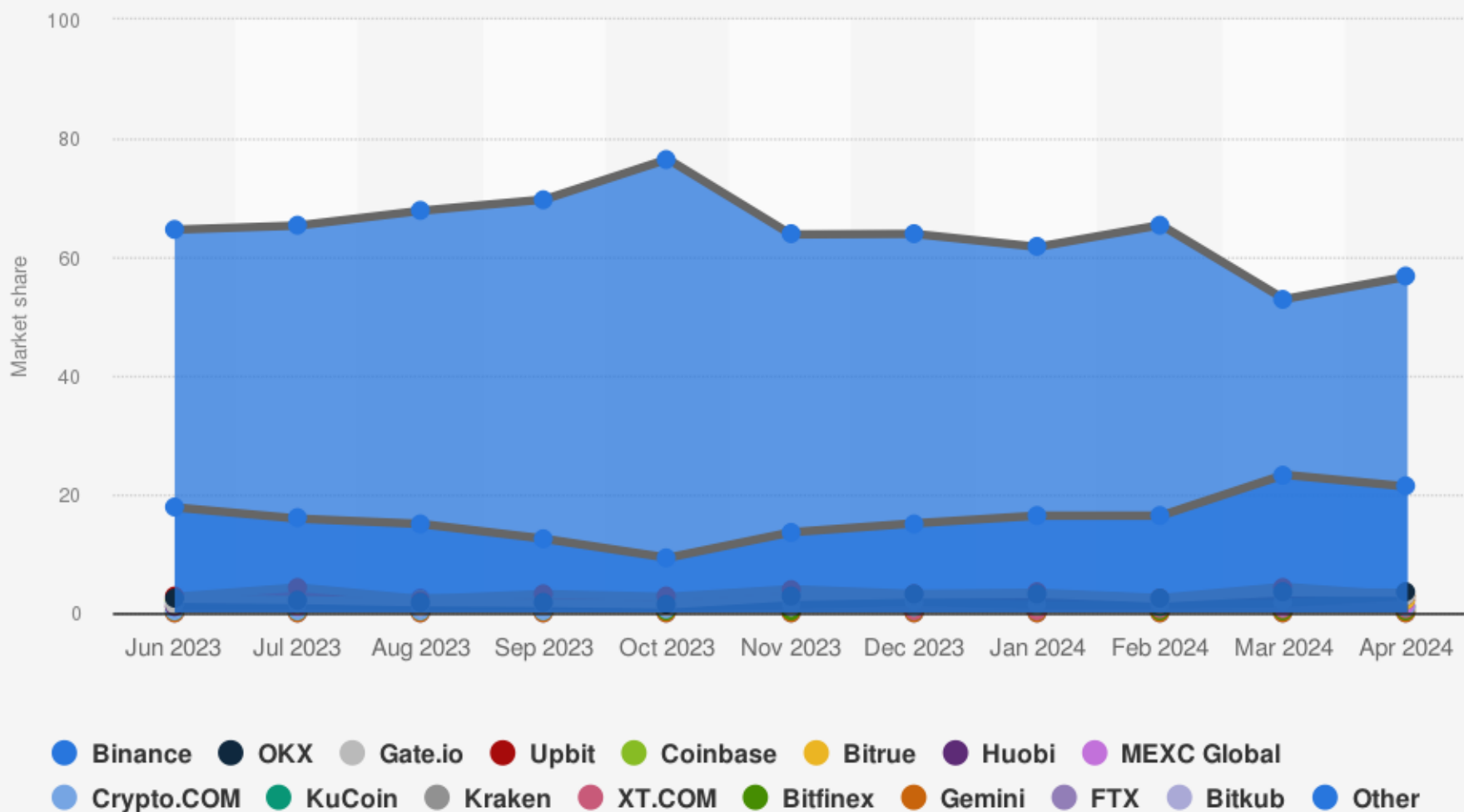


# Most expensive non-fungible token (NFT) sales worldwide as of March 16, 2021

The 50 biggest NFT sales worldwide as of March 16, 2021



## Biggest cryptocurrency exchanges based on trade volume market share from June 2023 to April 2024



### Sources

CoinGecko; Statista  
© Statista 2024

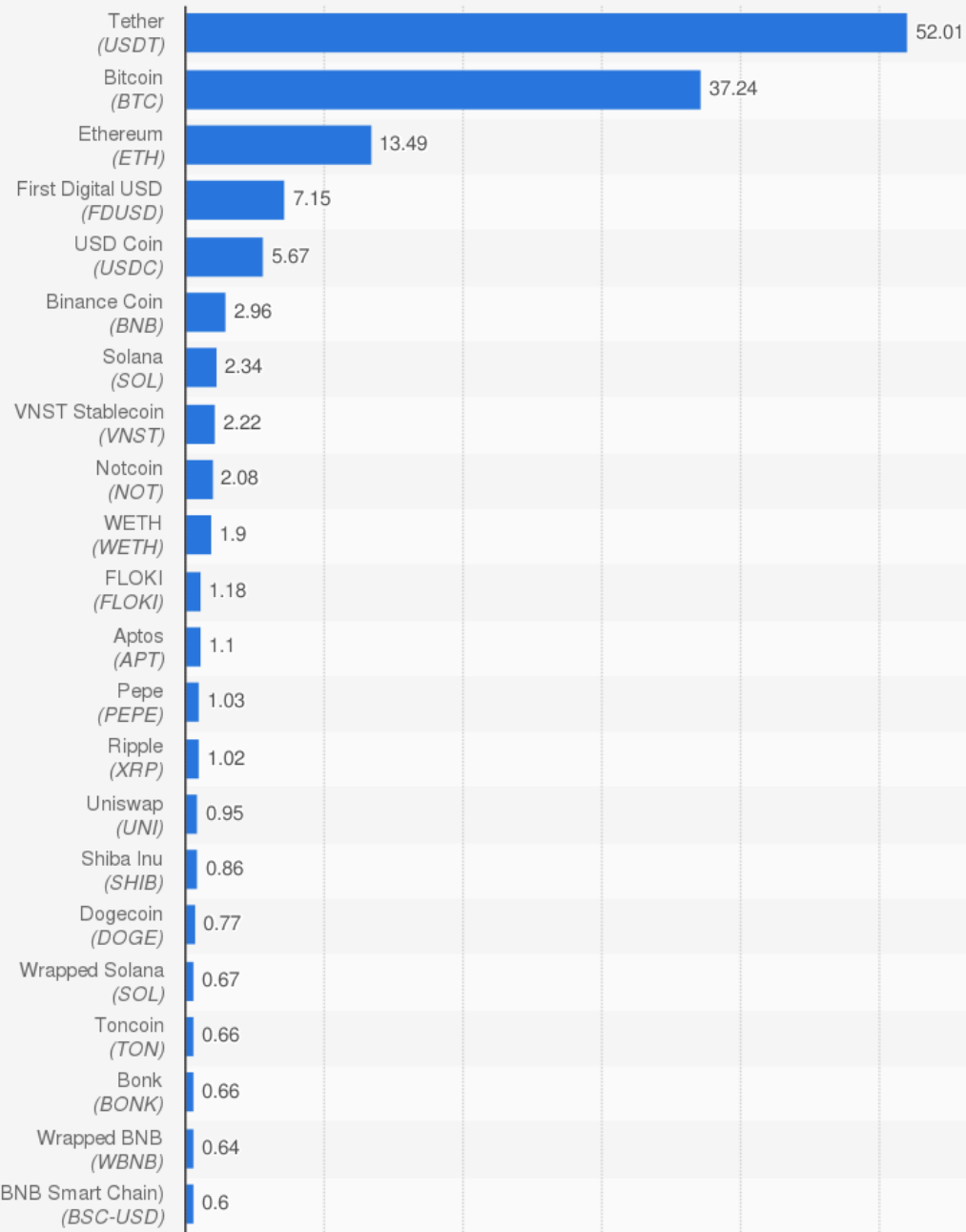
### Additional Information:

Worldwide; Statista; CoinGecko; September 2021 to January 2023; Spot trading only, does not include derivatives; Monthly data; within that month, not the end of the month

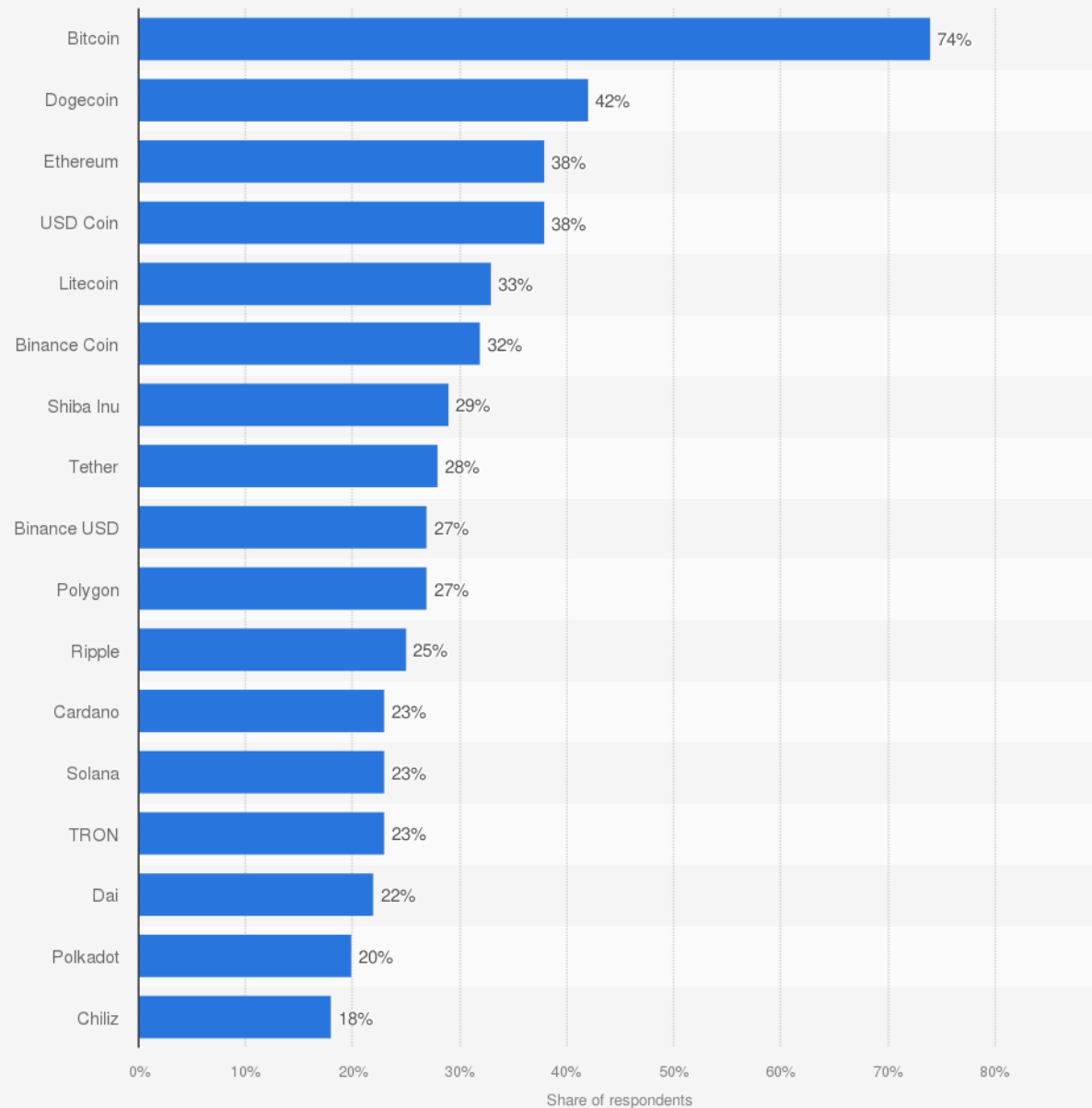




# Biggest cryptocurrencies in the world based on 24h trading volume on June 5, 2024 (in billion U.S. dollars)



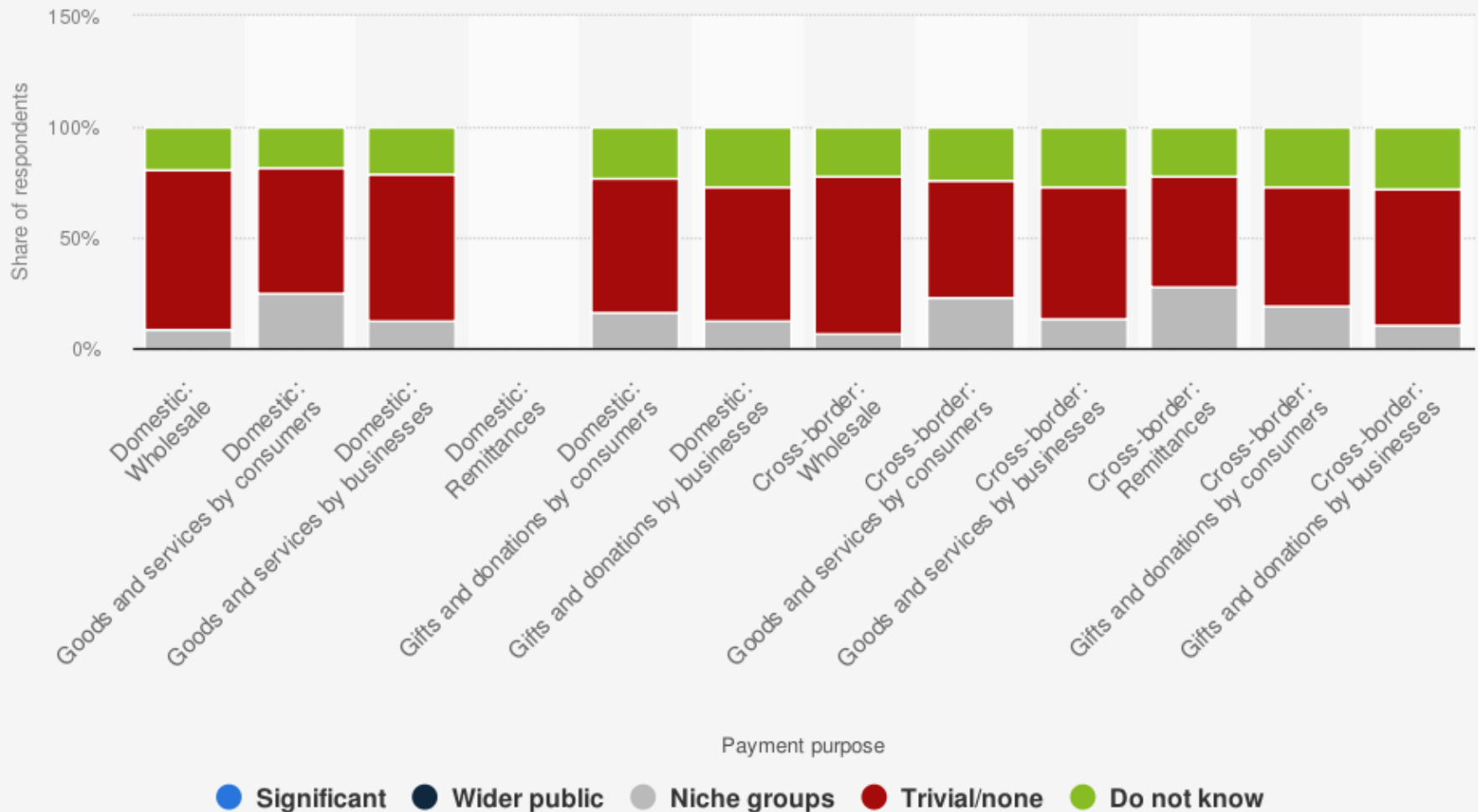
## Leading cryptocurrencies ranked by brand awareness in the United States in 2023



**Source**  
Statista Consumer Insights  
© Statista 2024

**Additional Information:**  
United States; December 2022; 1,245 respondents; 18 to 64 years; Online survey

# Use of cryptocurrency as a payments method outside the crypto ecosystem according to central banks worldwide in 2022



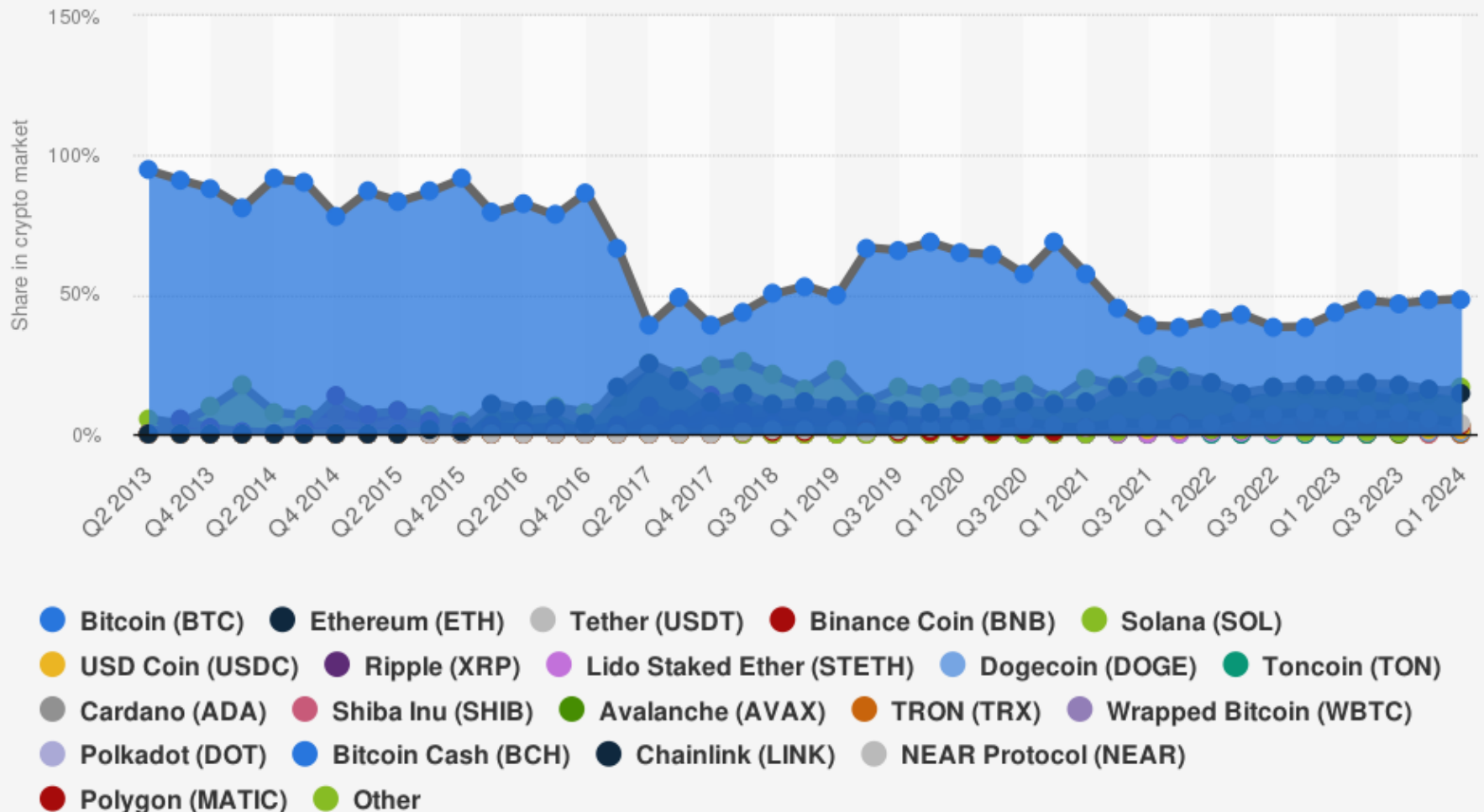
## Sources

Bank for International Settlements; Various sources (Central banks); Statista estimates  
© Statista 2024

## Additional Information:

Worldwide; Bank for International Settlements; Statista estimates; October 2022 to December 2022; 86 respondents; Central banks; retail payments, and exclude use in DeFi (Decentralized Finance); See the "Details" tab for more information about the survey methodology and questionnaire

## Dominance of Bitcoin and other crypto in the overall market from 2nd quarter of 2013 to 1st quarter of 2024



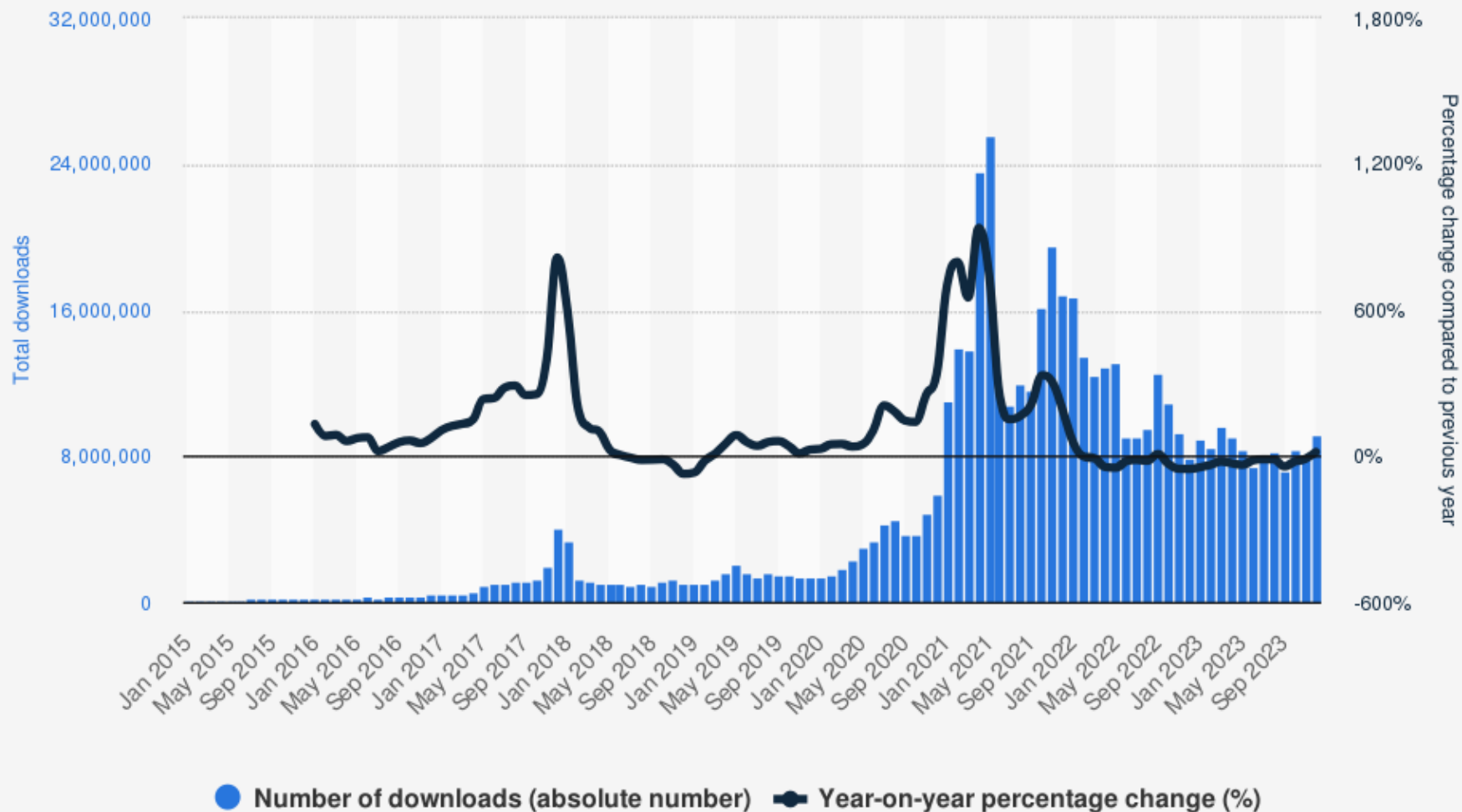
Source  
CoinGecko  
© Statista 2024

### Additional Information:

Worldwide; Statista; CoinGecko; Q2 2013 to Q1 2024; The cryptocurrencies on display are the top 20 based on market cap provided are as of the end of each quarter.

|         | Bitcoin<br>(BTC) | Ethereum<br>(ETH) | Tether<br>(USDT) | Binance<br>Coin (BNB) | Solana<br>(SOL) | USD Coin<br>(USDC) | Ripple<br>(XRP) | Lido Staked<br>Ether<br>(STETH) | Dogecoin<br>(DOGE) | Other |
|---------|------------------|-------------------|------------------|-----------------------|-----------------|--------------------|-----------------|---------------------------------|--------------------|-------|
| Q2 2013 | 94.62            | 0                 | 0                | 0                     | 0               | 0                  | 0               | 0                               | 0                  | 5.38  |
| Q1 2014 | 81.30            | 0                 | 0                | 0                     | 0               | 0                  | 1               | 0                               | 0.47               | 17.23 |
| Q1 2015 | 87               | 0                 | 0.01             | 0                     | 0               | 0                  | 7.23            | 0                               | 0.31               | 5.45  |
| Q1 2016 | 79.34            | 11.09             | 0.02             | 0                     | 0               | 0                  | 3.16            | 0                               | 0.30               | 6.09  |
| Q1 2017 | 66.79            | 17.20             | 0.21             | 0                     | 0               | 0                  | 2.91            | 0                               | 0.14               | 12.75 |
| Q1 2018 | 43.82            | 14.60             | 0.86             | 0.39                  | 0               | 0                  | 7.47            | 0                               | 0.12               | 25.75 |
| Q1 2019 | 49.47            | 10.27             | 1.41             | 1.66                  | 0               | 0.17               | 8.88            | 0                               | 0.17               | 23.24 |
| Q1 2020 | 65.21            | 8.13              | 2.40             | 1.03                  | 0               | 0.38               | 4.18            | 0                               | 0.12               | 17.10 |
| Q1 2021 | 57.40            | 11.11             | 2.13             | 2.50                  | 0.27            | 0.57               | 1.36            | 0.02                            | 0.37               | 19.96 |
| Q1 2022 | 41.09            | 18.70             | 3.76             | 3.42                  | 1.80            | 2.39               | 1.90            | 0.45                            | 0.87               | 18.71 |
| Q1 2023 | 43.79            | 17.44             | 6.44             | 4.05                  | 0.64            | 2.65               | 2.24            | 0.85                            | 0.83               | 16    |
| Q1 2024 | 48.58            | 14.92             | 3.71             | 3.28                  | 3.06            | 1.15               | 1.21            | 1.20                            | 1.02               | 16.80 |

# Estimate of the number of downloads of the 21 largest apps that allow for cryptocurrency storage worldwide from January 2015 to December 2023



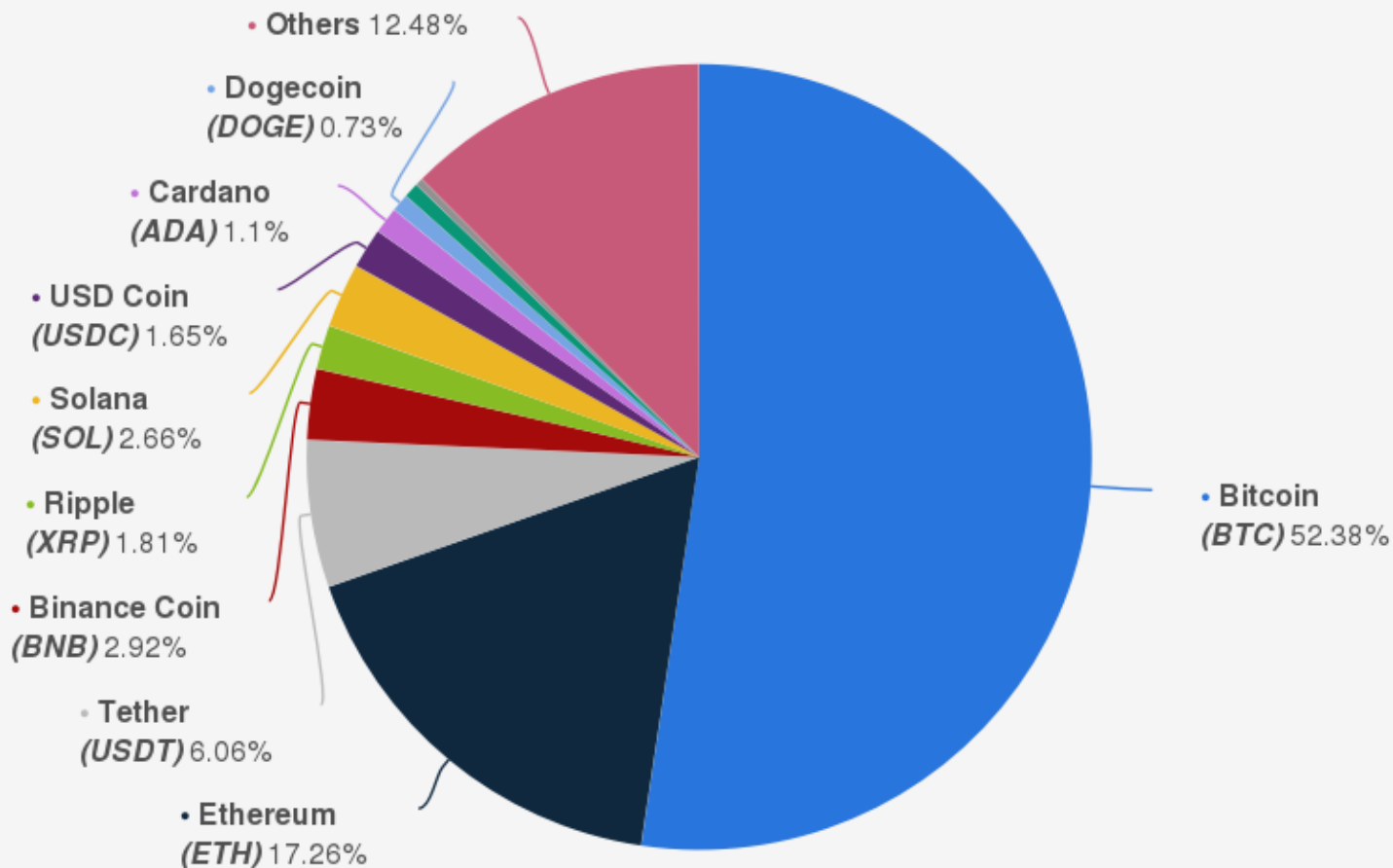
## Sources

AppMagic; Website (CryptoSlate)  
© Statista 2024

## Additional Information:

Worldwide; Statista; January 2015 to December 2023; The numbers provided are estimates based on wallets available worldwide. The chart does not include wallets that are popular in a specific country. See the "Details" tab for more information

## Bitcoin (BTC), Ethereum (ETH) dominance - their market cap relative to the market cap of all other cryptocurrencies in the world - on January 29, 2024



Source  
TradingView  
© Statista 2024

### Additional Information:

Worldwide; December 5, 2023, on 16:31 CET; The source moved Litecoin (LTC) and Bitcoin Cash (BTC) to the "Others" category as their dominance had become too low; Terra (LUNA) dropped out of the list after its decline in May 2022

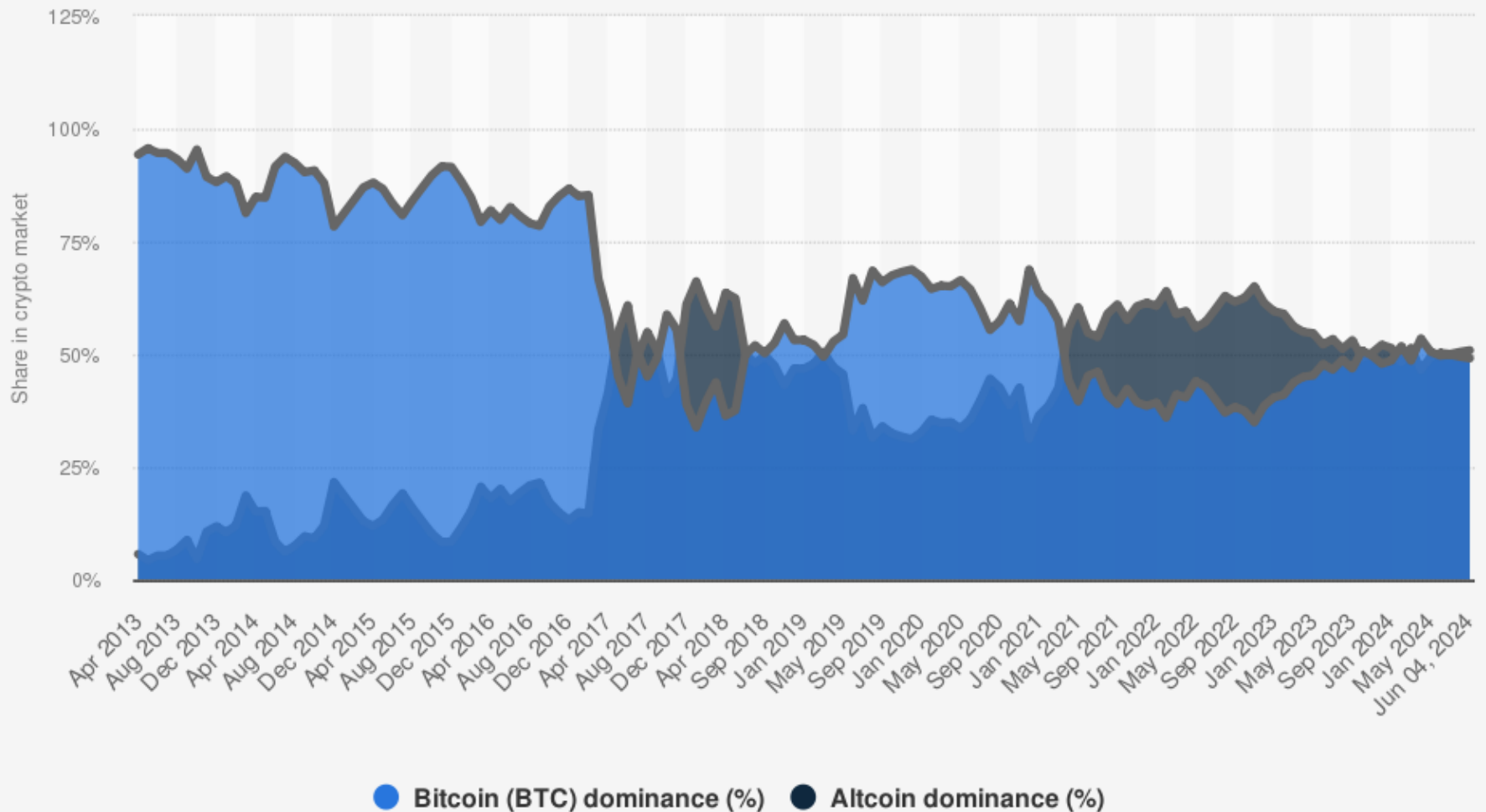


Biggest cryptocurrency in the world - both coins and tokens - based on market capitalization on June 5, 2024 (in billion U.S. dollars)

Market cap of 120 crypto - incl stablecoin, NFT, DeFi, metaverse - on June 5, 2024

|                           | Crypto category                     | Market cap in billion U.S. dollars | Low cap, mid cap, high cap |
|---------------------------|-------------------------------------|------------------------------------|----------------------------|
| Bitcoin (BTC)             | Store of value                      | 1401.05                            | High cap                   |
| Ethereum (ETH)            | Smart contracts                     | 458.04                             | High cap                   |
| Tether (USDT)             | Stablecoin                          | 112.36                             | High cap                   |
| Binance Coin (BNB)        | Exchange token (centralized)        | 107.62                             | High cap                   |
| Solana (SOL)              | Smart contracts                     | 79.92                              | High cap                   |
| Lido Staked Ether (STETH) | Smart contracts                     | 36.25                              | High cap                   |
| USD Coin (USDC)           | Stablecoin                          | 32.38                              | High cap                   |
| Ripple (XRP)              | Payments/digital currency           | 29.25                              | High cap                   |
| Dogecoin (DOGE)           | Memecoin                            | 23.54                              | High cap                   |
| Toncoin (TON)             | Payments/digital currency           | 17.44                              | High cap                   |
| Cardano (ADA)             | Smart contracts                     | 16.26                              | High cap                   |
| Shiba Inu (SHIB)          | Memecoin                            | 15.27                              | High cap                   |
| Avalanche (AVAX)          | Exchange token (decentralized)/DeFi | 14.27                              | High cap                   |

# Bitcoin market dominance — its market cap relative to the market cap of all other cryptocurrencies in the world — from April 2013 up to June 4, 2024



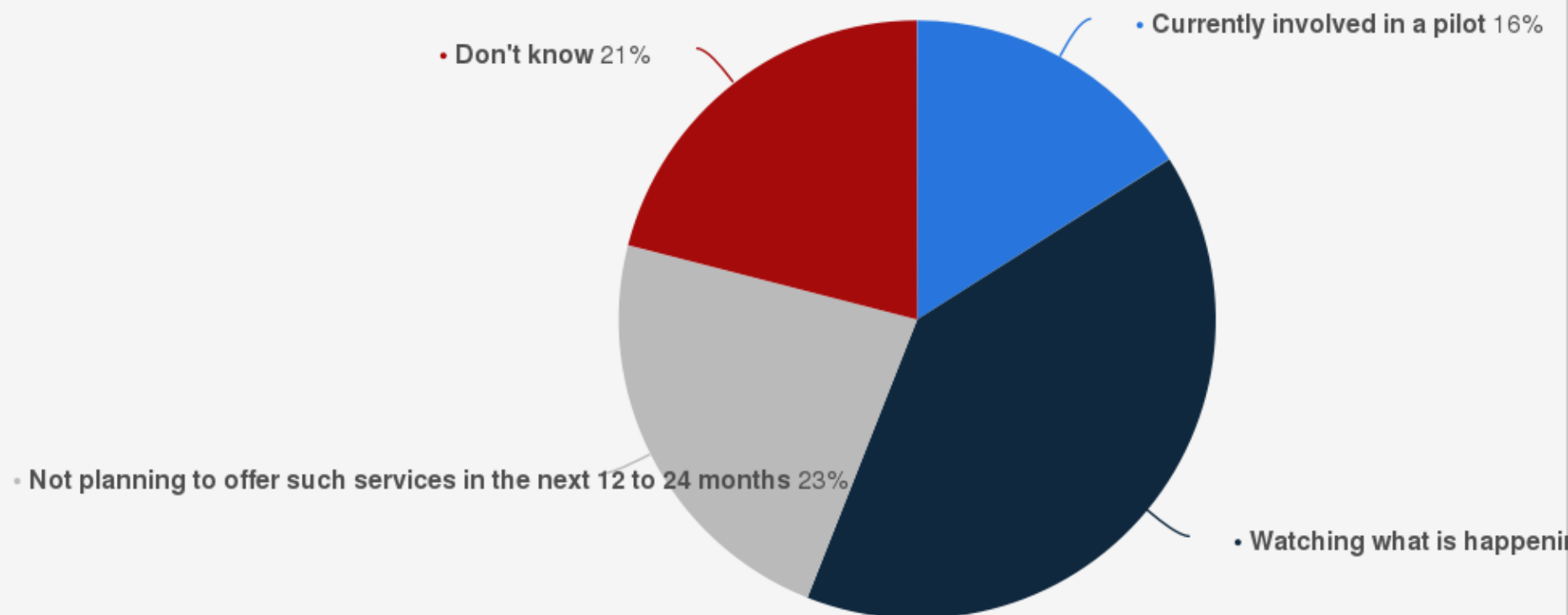
## Sources

CoinGecko; Statista  
© Statista 2024

## Additional Information:

Worldwide; Statista; CoinGecko; April 2013 up to June 4, 2024

## Approaches taken by banks on future adoption of digital assets - cryptocurrency, stablecoin, central bank digital currency (CBDC) - as of 2023



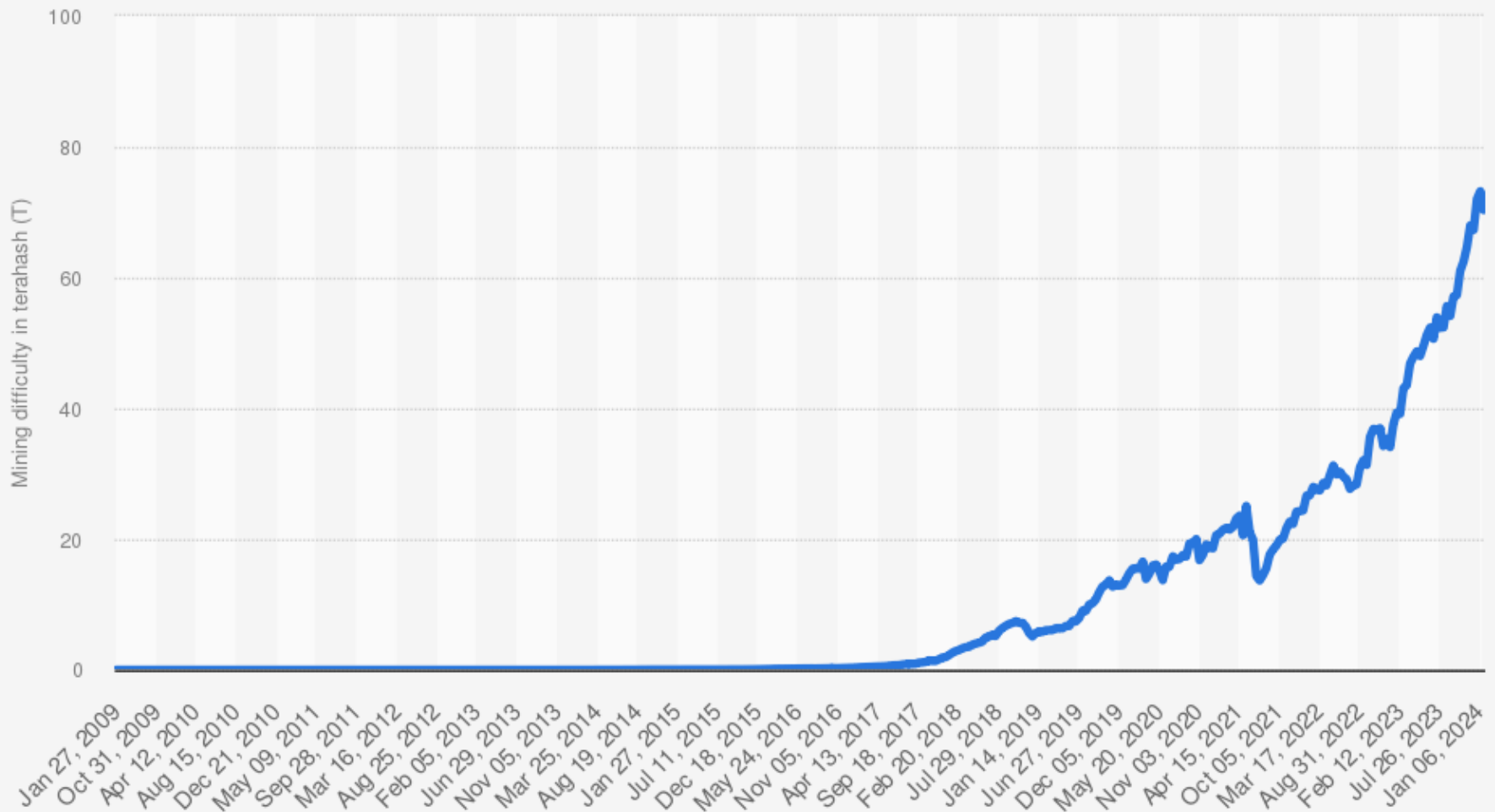
### Sources

Finastra; Aite-Novarica Group  
© Statista 2024

### Additional Information:

Worldwide; Finastra; Q4 2022 and Q1 2023; 108 respondents; 18 years and older; global bank payments and product executives

**Average mining difficulty of Bitcoin from January 2009 to January 20, 2024 (in terahash)**



Source

Website (BTC.com)

© Statista 2024

Additional Information:

Worldwide; January 2014 to January 20, 2024; The figures provided show many times on average miners should calculate cryptocurrency block; Bitcoin difficulty is adjusted every 2,016 blocks, which is roughly every two weeks, to ensure the average remains at 10 minutes.

Share of respondents who indicated they either owned or used cryptocurrencies in 56 countries and territories worldwide from 2019 to 2024

Annual cryptocurrency adoption in 56 different countries worldwide 2019-2024

|                    | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 |
|--------------------|------|------|------|------|------|------|
| Argentina          | 16%  | 14%  | 21%  | 35%  | 26%  | 30%  |
| Brazil             | 18%  | 12%  | 12%  | 22%  | 28%  | 24%  |
| India              | 8%   | 8%   | 10%  | 22%  | 27%  | 22%  |
| South Africa       | 16%  | 17%  | 18%  | 23%  | 22%  | 22%  |
| Portugal           | 9%   | 8%   | 14%  | 15%  | -    | 20%  |
| Switzerland        | 10%  | 9%   | 13%  | 18%  | 21%  | 19%  |
| Chile              | 11%  | 12%  | 14%  | 14%  | 15%  | 18%  |
| Dominican Republic | 10%  | 10%  | 11%  | 15%  | -    | 17%  |
| Mexico             | 12%  | 11%  | 9%   | 12%  | 13%  | 17%  |
| Australia          | 7%   | 8%   | 9%   | 16%  | 17%  | 16%  |
| Netherlands        | 10%  | 9%   | 10%  | 19%  | 19%  | 16%  |
| South Korea        | 6%   | 8%   | 8%   | 19%  | 20%  | 16%  |
| United States      | 5%   | 7%   | 8%   | 15%  | 16%  | 16%  |

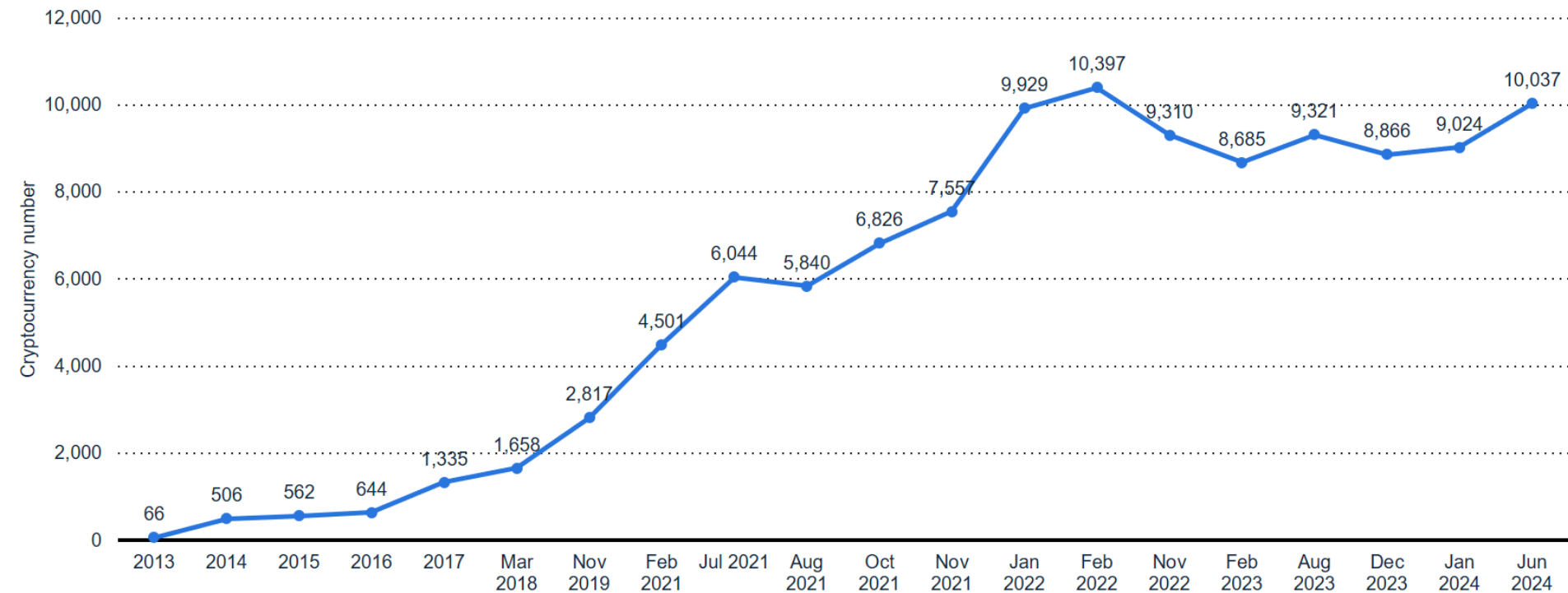
Maximum and current supply of 100 cryptocurrencies with the highest market cap as of June 5, 2024 (in millions)

Maximum/current supply of 100 cryptocurrencies worldwide as of June 53, 2024

|                           | Current supply in millions | Maximum supply in millions | Share of max supply in circulation (%) |
|---------------------------|----------------------------|----------------------------|--|
| Bitcoin (BTC)             | 19.71                      | 21                         | 93.8%                                  |
| Ethereum (ETH)            | 120.15                     | n/a                        | Unlimited supply                       |
| Tether (USDT)             | 112316.77                  | n/a                        | Unlimited supply                       |
| Binance Coin (BNB)        | 153.86                     | 200                        | 76.9%                                  |
| Solana (SOL)              | 459.92                     | n/a                        | Unlimited supply                       |
| Lido Staked Ether (STETH) | 9.51                       | n/a                        | Unlimited supply                       |
| USD Coin (USDC)           | 32377.24                   | n/a                        | Unlimited supply                       |
| Ripple (XRP)              | 55450.36                   | 100000                     | 55.5%                                  |
| Dogecoin (DOGE)           | 144572.08                  | n/a                        | Unlimited supply                       |
| Toncoin (TON)             | 2413.63                    | n/a                        | Unlimited supply                       |
| Cardano (ADA)             | 35393.53                   | 45000                      | 78.7%                                  |
| Shiba Inu (SHIB)          | 589262909.79               | n/a                        | Unlimited supply                       |
| Avalanche (AVAX)          | 393.23                     | 720                        | 54.6%                                  |

# Number of cryptocurrencies worldwide from 2013 to June 2024

Quantity of cryptocurrencies as of June 3, 2024



# Introduction

- Cryptocurrency is a system that meets six conditions:
  - The system does not require a central authority
    - Its state is maintained through distributed consensus
  - The system keeps an overview of cryptocurrency units and their ownership
  - The system defines whether new cryptocurrency units can be created
    - If yes, the system defines the circumstances of their origin, and
    - How to determine the ownership of these new units.
  - Ownership of cryptocurrency units can be proved exclusively cryptographically
  - The system allows transactions to be performed
    - Ownership of the cryptographic units is changed
    - Transaction statement can only be issued by an entity proving the current ownership of these units.
  - If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them



# Introduction

- Field of cryptocurrency technologies
  - Experienced a rapid growth in popularity
    - Since the introduction of Bitcoin (2008-09)
- To date 10,000+ different cryptocurrencies have been created
  - Some had a very short lifespan
  - Some were conceived for fraudulent purposes
  - Others brought additional innovations
    - Have vital and vibrant communities today
  - Mechanisms and underlying principles
    - Derived from the original Bitcoin protocol
    - Differ from Bitcoin in their choice of certain constants
      - Target block interval
      - Maximum number of currency units
    - Alternative algorithms
    - Additional features
    - Different consensus approaches

# Introduction

- Extensive news coverage
  - Increased interest from different communities
    - Technical enthusiasts
    - Business people, investors
    - Criminals, law enforcement agencies
- Bitcoin fundamentals
  - Hard to understand for non-expert users
  - Cannot be reconciled with the models of traditional currency
- Bitcoin design
  - Decentralized cryptographic currency
  - Does not rely on trusted third parties
    - Combining innovative incentive engineering
    - Right cryptographic primitives
    - Probabilistic distributed consensus approach
    - Practical demonstration of feasibility

# Introduction

- Underlying technologies, commonly referred to as blockchain
  - Rising interest within academia as well as the private sector
  - Many open problems remain
    - Finding a balance between different aspects
      - Performance, scalability, security, decentralization, anonymity
- Cryptocurrency Aspects
  - Financial and economic
  - Legal perspective
  - Political and sociological perspective
  - Technical and socio-technical
- Cryptocurrency community
  - Technology enthusiasts
  - Businesses & investors
  - Ideologists
  - Public authorities and policymakers
  - Researchers
  - Cypherpunks
  - Libertarians
  - Financial regulators
  - Banks
  - Criminals
- Loose structure, Mindset of avoiding trusted single points of failure
  - Sometimes hard to reach consensus
    - Regarding the direction of Bitcoin's technological development
    - Diverging interests

# Introduction

- Early work in cryptocurrencies
  - Mostly focused on required cryptographic primitives
  - Privacy guarantees
- Systems themselves still had to rely on trusted third parties
  - To be able to guarantee correct operation
- Bitcoin: launched as the first decentralized distributed currency
  - Removed the dependency on trusted third parties
  - Combination of well known primitives and techniques
    - Proof-of-work (PoW)
    - Agreement (or consensus) amongst all nodes on the state of the underlying transaction ledger
    - Consensus approach allows for permissionless participation by potentially anonymous actors

# *History of Cryptographic Currencies*

- Rests on two foundations:
  - History of distributed systems research in general
  - History of electronic cash systems
    - Earlier, very few connections with each other
      - Despite the use of cryptographic primitives
    - Both fields are related to research and advances in cryptography
    - Research in the area of electronic cash:
      - Driven by the inventions in the area of asymmetric cryptography
        - » e.g., blind signature schemes
    - Bitcoin provided the missing link between them
      - To create a decentralized cryptographic currency
      - Combined pieces from each of these areas
    - Fallout of rise of Bitcoin
      - Increased interest in distributed systems research
      - Electronic payment systems and currencies

|      |                                 |
|------|---------------------------------|
| 1983 | Blind signature (Chaum)         |
| 1984 |                                 |
| 1985 |                                 |
| 1986 |                                 |
| 1987 |                                 |
| 1988 |                                 |
| 1989 |                                 |
| 1990 |                                 |
| 1991 |                                 |
| 1992 | Cypherpunk mailing list         |
| 1993 | Clipper chip backdoor announced |
| 1994 |                                 |
| 1995 | 3 lines of RSA (Adam Back)      |
| 1996 | Clipper chip was abandoned      |
| 1997 |                                 |
| 1998 | B-money (Wai Dei)               |
| 1999 |                                 |
| 2000 |                                 |
| 2001 |                                 |
| 2002 | Hashcash (Adam Back)            |
| 2003 |                                 |
| 2004 | RPOW (Hal Finney)               |
| 2005 |                                 |
| 2006 | Bit gold (Nick Szabo)           |
| 2007 |                                 |
| 2008 |                                 |
| 2009 | Bitcoin (Satoshi Nakamoto)      |

## History

- Blind signature (David Chaum)
  - Referred to as the inventor of secure digital cash
  - Paper on cryptographic primitives of blind signatures
  - Cryptographic scheme to hide (blind) the content of a message before it is signed
    - So that the signer cannot determine the content
  - Blind signatures can be publicly verified just like a regular digital signature
  - Proposed digital cash approach allows users to spend digital currency
    - Untraceable by another party
  - Later improvement of the idea
    - Allowing offline transactions
    - Adding double-spending detection mechanisms
  - System required trusted parties for issuing and clearance of electronic cash
  - First generation of cryptographic currencies
    - Failed to reach a broad audience
    - Despite various commercialization efforts

# History

- Cypherpunk movement
  - Informal group communicating via the Cypherpunks electronic mailing list
  - Advocating the use of cryptography and privacy-enhancing technologies
  - Idea of digital cash whose value would not be dependent on the organization issuing it
  - Before David Chaum cryptography was not publicly available to consumers
    - Exclusively practiced by the military and intelligence agencies
  - Movement addressed topics such as anonymity, pseudonymity, communication privacy, data hiding, censorship, monitoring

# History

- Clipper chip chipset: escrow system
  - Developed by the NSA
  - Major issue in the mid-1990s
  - Built-in backdoor
  - Other vulnerabilities in Clipper Chip's
  - Government's efforts to limit the use of encryption by Internet users: crypto wars
  - Protest the United States' cryptography export regulations
  - Lack of adoption of the Clipper chip by smartphone manufacturers
    - Clipper Chip design was abandoned
- Debate on key escrow and government-controlled backdoors persists even to this date
  - The Snowden revelations of 2013
  - Sparked a public wave of concern
    - Resulted in an increased demand for cryptographic applications by end users and vendors



# History

- Before Bitcoin, different approaches
  - Incremental improvements on the original idea of David Chaum
  - Contained some centralized elements
- B-money (WeiDai, 1998)
  - Anonymous, distributed electronic cash system
  - "Money which is impossible to regulate"
  - Scheme
    - An untraceable network
    - Senders and receivers are identified only by digital pseudonyms (e.g. their public keys)
    - Every message is signed by its sender and encrypted to the receiver
    - Allowed the creation of money
      - Based on previously unsolved cryptographic puzzles
    - Enforce contracts without outside help

- Core concepts - B-Money
  - Requires a specified amount of computational work
  - The work done is verified by the community who update a collective ledger book
  - The worker is awarded funds for their effort
  - Exchange of funds is accomplished by collective bookkeeping
    - Authenticated with cryptographic hashes
  - Contracts are enforced through the broadcast
    - Signing of transactions with digital signatures

# History

- Bit-Gold (Nick Szabo, 1998): never implemented
  - Direct precursor to the Bitcoin architecture
  - Relied on cryptographic puzzles
    - Had to be solved using computing power
    - Later sent to a public registry
  - Assigned to the public key of the solver
    - Each solution would become part of the next challenge
      - Creating a growing chain of new property
    - Provided a way for the network to verify and time-stamp new coins
      - Unless a majority of the parties agreed to accept new solutions, they couldn't start on the next puzzle
    - Address the problem of double-spending without a central authority
      - Mimic the trust characteristics of gold
  - Theory of collectibles

# History

- Hashcash: proposed by Adam Back (1997)
  - Proof-of-Work (PoW)
    - Economic measure to deter service abuses
    - By requiring some work from the service requester
      - Typically, processing time by a computer
    - Concept was invented by Cynthia Dwork and Moni Naor
  - Used to limit email spam and denial-of-service attacks
  - Based on cryptographic hash functions
    - To derive probabilistic proof of computational work as an authentication mechanism.
    - System Requirements:
      - Hard to find a valid solution
      - Easy to verify any given solution
  - Purpose was to ensure that it was computationally hard for a spammer to transmit mails over an anonymous mail relay
    - Identity of the sender should be protected
      - No traditional authentication checks are possible in such a scenario
    - Mail server required the solution to a computational challenge as an authentication method for accepting the message for relaying

# History

- Reusable proof-of-work (RPOW): Hal Finney, 2004
  - Idea of making proofs-of-work reusable for some practical purpose
    - Szabo's theory of collectibles
  - Introduced token money that was aligned with the concept of gold value
    - Gold coin's value is thought to be underpinned by the value of the raw gold needed to make it
    - Value of an RPoW token is guaranteed by the value of the real world resources required to 'mint' a PoW token
  - Permitting the exchange of tokens
    - Without repeating the work required to generate them
  - Protected by the private keys stored in the trusted platform module (TPM) hardware
    - Manufacturers holding TPM private keys

# History

---

- Bitcoin: created as the first decentralized cryptocurrency
  - Pseudonymous developer Satoshi Nakamoto
  - Between 2008 and 2009
    - October 31, 2008
      - Bitcoin Whitepaper self published
    - January 3rd, 2009
      - Genesis block of the Bitcoin protocol was created
      - Marking the birth of Bitcoin

Thank you