UNIVERSITÄT
LEIPZIG

Development of Financial Markets and Institutions

XIII. Cryptocurrency and Central Bank Digital Currency

Leipzig University | January 22, 2024

Dr. Kristoffer J. M. Hansen | Institute for Economic Policy

XIII. CRYPTOCURRENCY AND CENTRAL BANK DIGITAL CURRENCY

1. Bitcoin
2. Beyond Bitcoin
3. Central Bank Digital Currency
4. Literature

1. BITCOIN

THE PREHISTORY OF BITCOIN

Cypherpunk Monetary Discussions

- The cypherpunks in the 1990s concerned with online privacy, security of information
- In part inspired by the desire for private (non-government issued) money
- In part inspired by free banking theory

Early Attempts at Digital Money and Related Technologies

- E-gold, launched 1996 – users held accounts denominated in gold
    - Legal troubles from 2007 meant decline
- Hashcash 1992, 1997: a proof-of-work protocol for email, to protect against spammers
- Bitgold proposed 1998 by Nick Szabo but never implemented
    - Combines many of the elements later used in bitcoin (cryptography, proof-of-work)

THE PROBLEM

P2P in the Digital World

- Peer-to-peer transactions are not possible in the digital world
- There is no digital “cash” to send from person to person
- Trusted third parties necessary to facilitate and verify transactions (Byzantine Generals)
- Double-spending: the same amount is spent twice, defrauding one recipient (at least)

Central Third Parties Necessary

- Central third parties: credit card companies, banks, paypal
- A system so dependent on central authorities is vulnerable: single point of failure
- Potential privacy concerns
- Abuse of authority → inflation

THE SOLUTION: BITCOIN

"A Peer-to-Peer Electronic Cash System"

- Proposed by Satoshi Nakamoto in 2008
- A decentralized payments system, payments validated and recorded in the "blockchain"
- Individual transactions authorized by private key and broadcast to the network
- Only the public signature is known, the address from which or to which bitcoin is sent

The Blockchain

- Transactions collected in blocks and validated by proof-of-work
- A new block is added to the blockchain every 10 minutes
- The blockchain is a cryptographically "sealed" record of all transactions with bitcoin
- Miners rewarded for adding blocks, verifying payments – overcoming P2P problems

BITCOIN MINING

Proof-of-Work

- Each block is secured by a mathematical puzzle, the proof-of-work
- Miners compete in solving the puzzle, the first to solve it broadcasts it to the network
- New bitcoin are created as a reward for mining blocks, at the moment 6.25 per block
- Proof-of-work difficulty automatically adjust to mining power

Blocks and Blockchain

- The longest blockchain is the correct one, new blocks only added to the longest chain
- If two blocks are broadcast simultaneously, different nodes work on different blocks
- Once next block broadcast, the longest chain is kept, the other discarded
- The production of bitcoin is capped at 21 million, thereafter rewards only from fees

MORE ON THE BLOCKCHAIN

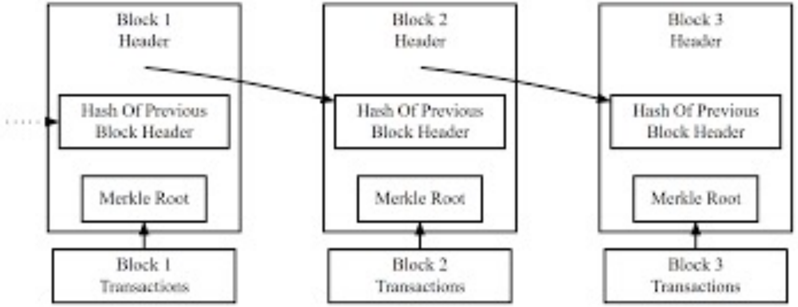
Size of Blocks

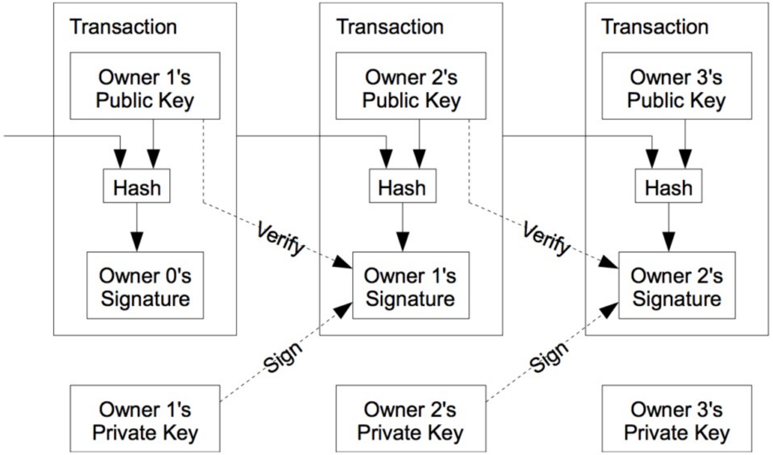
- Originally, there was no size limit on the individual blocks
- Miners simply gathered all the transactions into the next block
- 1MB limit introduced early, to protect the blockchain from "bloat"
  - ➢ People with malicious intent could spam the blockchain with micro-payments
  - ➢ Thus making the blocks too big to be economically broadcast

Limited Space

- Lack of space on each block for all transactions
- Transaction fees introduced to economize the space
- Fee automatically set according to the demand for space
- In times of high use, these fees have been high - $50 or more

BLOCKCHAIN AND TRANSACTIONS





BITCOIN AND PRIVACY

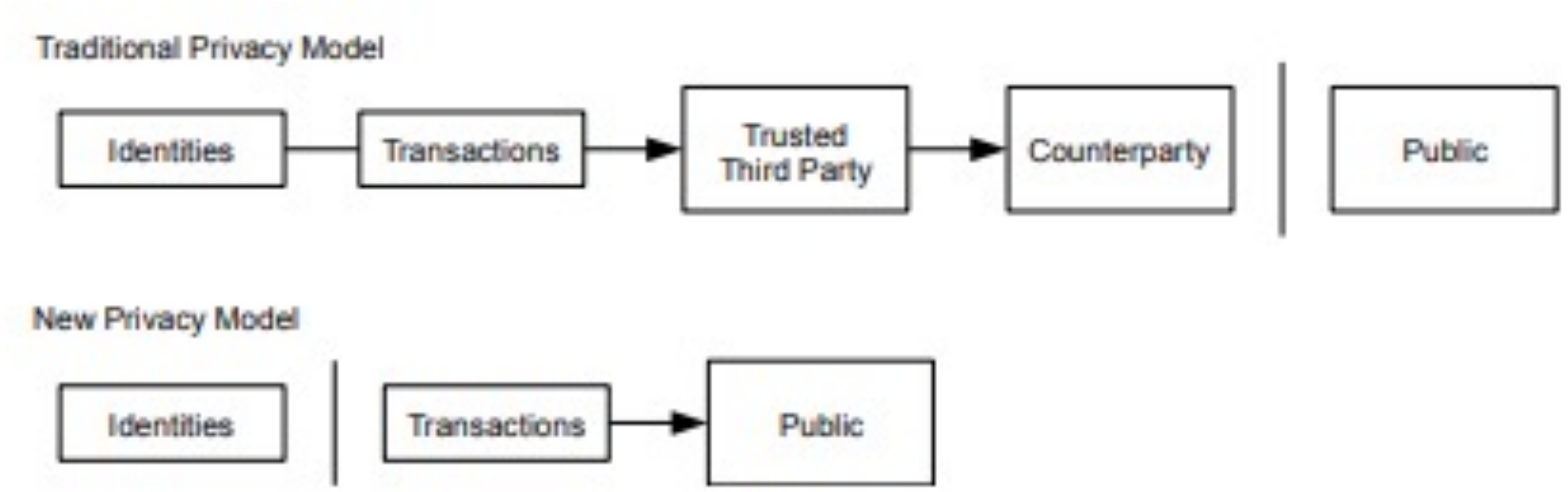
Traditional System

- Intermediaries key, they have data on the transacting parties and the amounts sent etc.
- This data is private, not available to the public
- But potentially everything is accessible to everyone

Bitcoin

- Transactions data are public in the blockchain – but they cannot be tied to individuals
- All that can be seen are the amounts sent and the addresses sent from and to
- It is still possible to lose privacy: if a link is made between an address and an individual
  - ➢ KYC regulations on bitcoin exchanges
  - ➢ Bitcoin detectives can track down ownership and spending of coins

BITCOIN AND PRIVACY (BITCOIN WHITE PAPER)



DOUBLE-SPEND AND 51-PERCENT ATTACKS

The Problem of Double-Spending

- Double-spend: the same bitcoin transferred to different wallets
- A coin first goes to one, but before validation, it is reversed and send to someone else
- Alternatively, a dishonest miner or node must replace one block with another
- This is no problem so long as a majority of nodes are honest

51 Percent Attack

- A dishonest node will have to control 51 percent of computing power
- Limited rewards: he can only reverse the previous block, falsify the latest transactions
- Mining is costly, is dishonesty really profitable?
- High opportunity costs: honest bitcoin mining

BITCOIN GOVERNANCE

Open Source

- The software behind bitcoin is all open source, publically available
- Bitcoin Improvement Proposals (BIP) debated in the community
- Once rough consensus is achieved, the proposal is integrated into the software
  - ➢ Uploaded to the recognized code repository
  - ➢ Only a few persons have access to the code repository
- The proposal is only integrated once users (nodes) download and install it

Consensus and Forks

- Ultimately, there is no central authority
- If consensus is not achieved on a BIP, but some want to implement it, a fork happens
- Two blockchains emerge: one with the old and one with the new software
- Their past is the same, but from the fork, we are dealing with two new coins

MINING BOOM

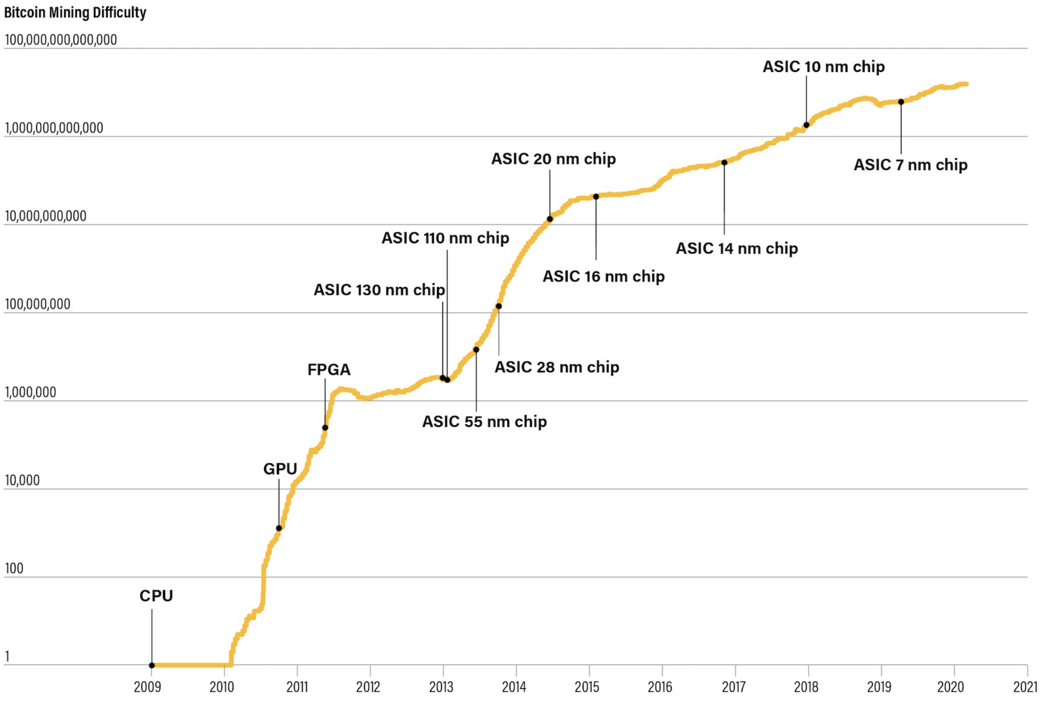
Technological Progress

- Bitcoin mining began with simply downloading a client to your laptop
- As mining became more profitable, mining hardware advanced
- From CPU to GPU, from laptops to dedicated rigs to large-scale mining operations

Economic Factors Determining Mining

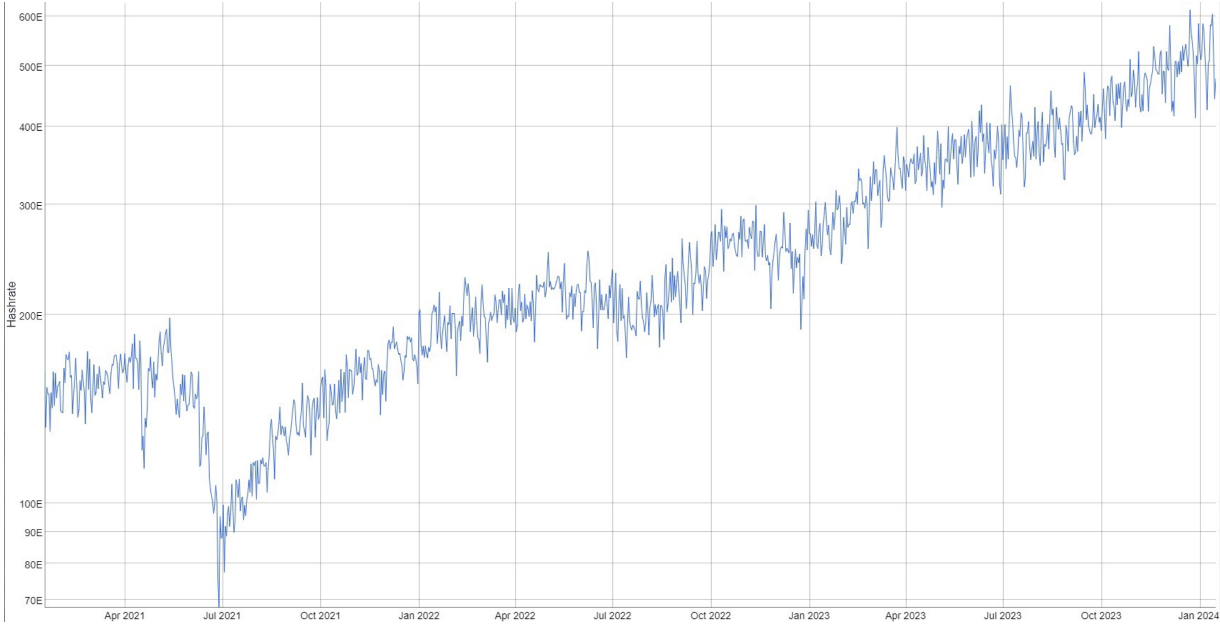
- Bitcoin price, chance of mining the next block, input costs
- Rising bitcoin prices means more resources are dedicated to mining
- Falling bitcoin prices eliminate profits, mines are turned off, switched to other purposes
- The main inputs: hardware rigs and electricity
- Miners locate where electricity is cheap, migrate according to seasonal changes
    - ➢ E.g., wet season in China

MINING DEVELOPMENT (SOURCE: COINDESK)



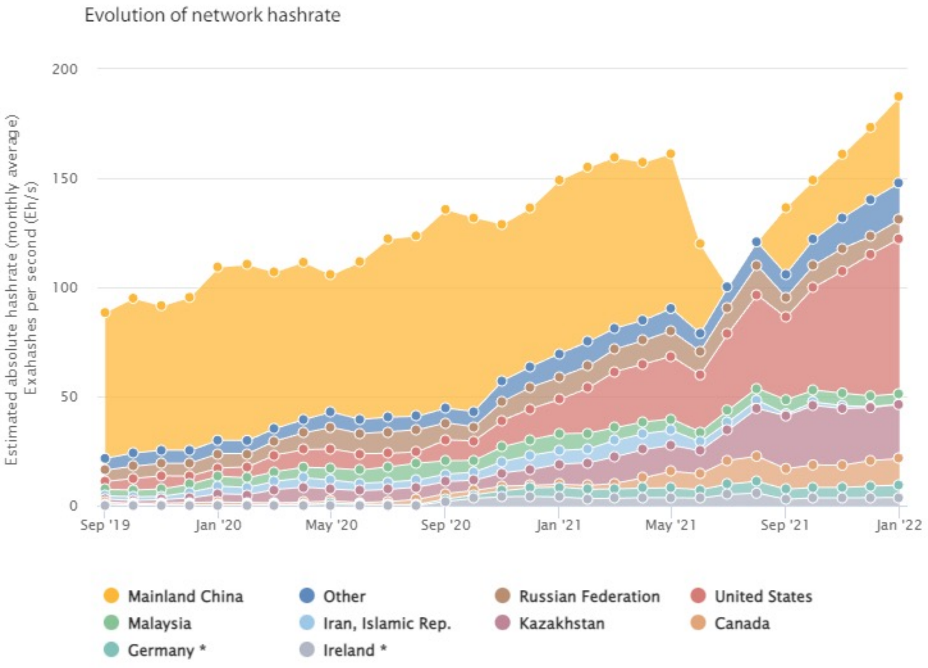
HASHRATE AND POW

- The number of "guesses" per second
- It measures the computational power assigned to the blockchain
- The larger, the more secure the blockchain is
- And the more resources are devoted to bitcoin mining



Source: bitinfocharts.com

BITCOIN MINING BY COUNTRY, 2019 – JAN. 2022 (SOURCE: CBECI)

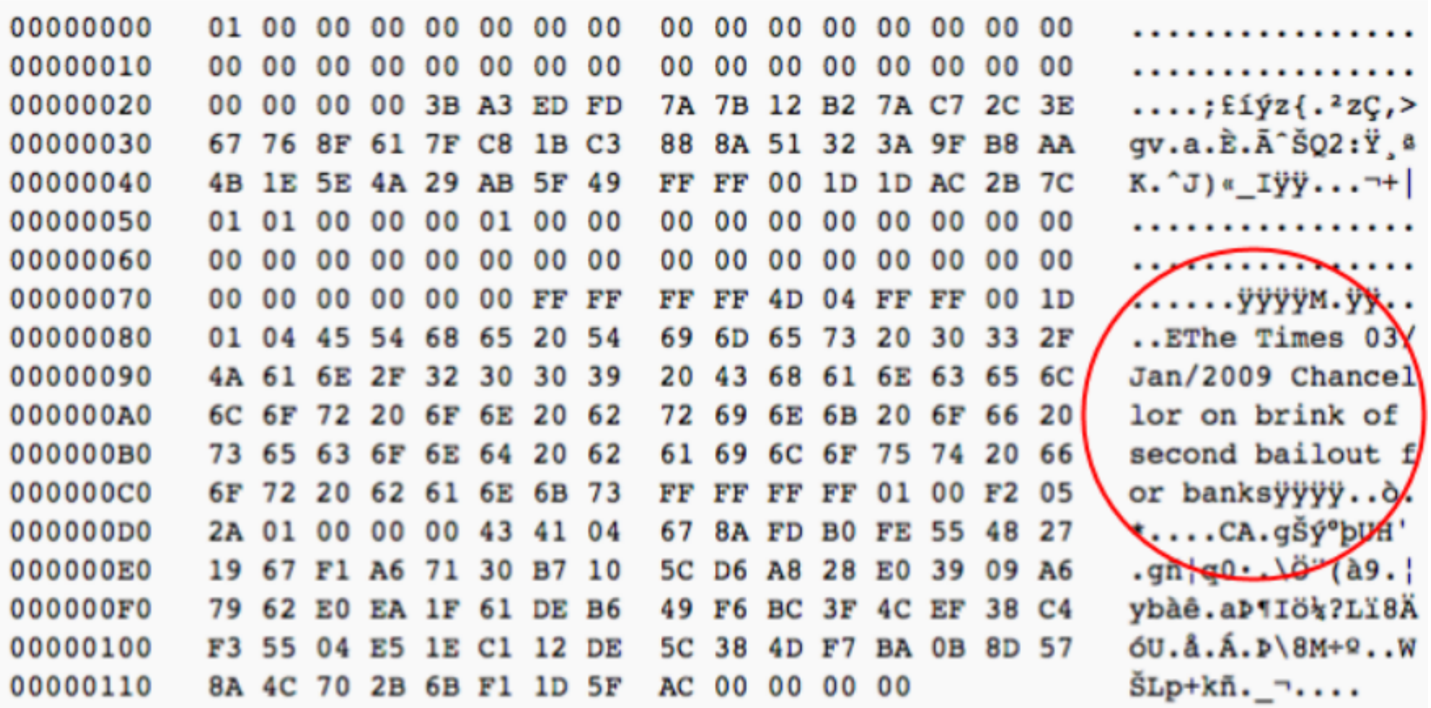


2. BEYOND BITCOIN

OTHER USES OF THE BLOCKCHAIN

- Secure records on the blockchain (sales, land titles, marriages)
- Smart contracts
- Contracts that automatically execute once certain conditions are met
- Decentralized finance (DeFi)
- Decentralized lending platforms
- Initial coin offerings – ICOs
- To fund new startups
- ...there seems to be a lot of scam going on here
- The original bitcoin blockchain can be used for some, not all of these purposes

THE GENESIS BLOCK MESSAGE



```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of 
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00            ŠLp+kñ._¬....
```

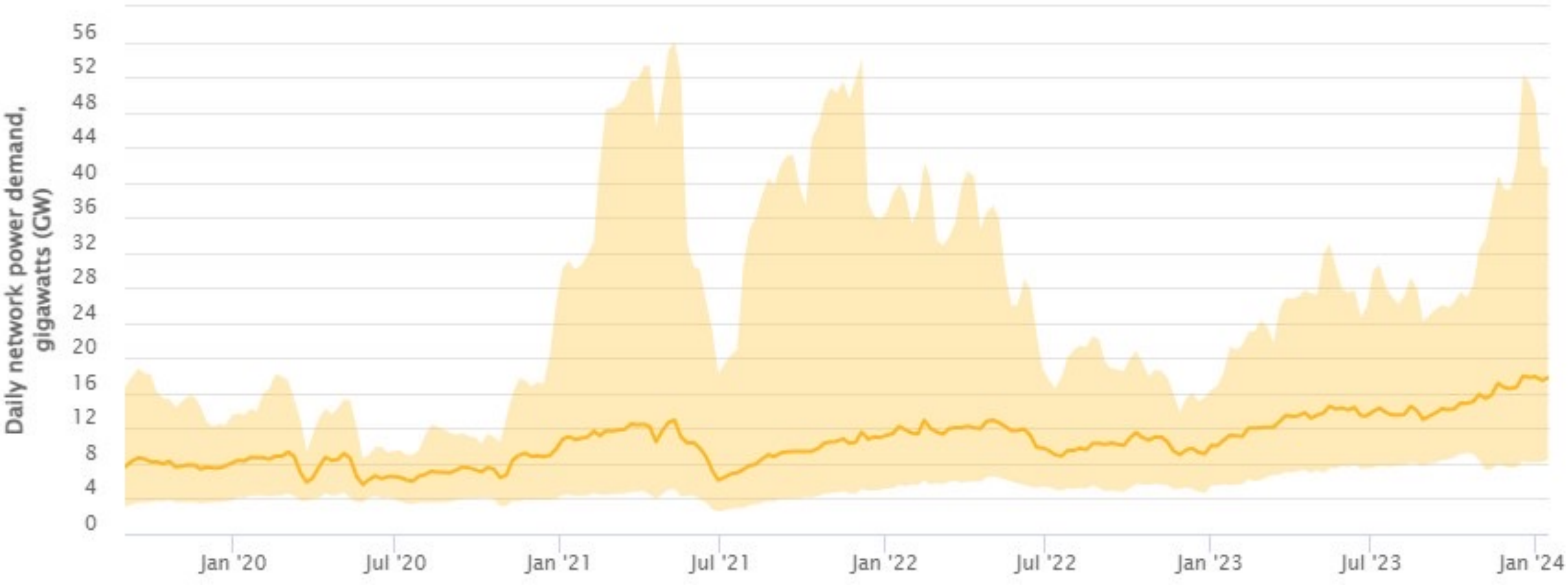
NEW CRYPTOCURRENCIES

- Since the basic software is publically available, it is very easy to launch your own crypto with your own specific features
- The joke coin dogecoin (2013) was an early example
- Mainly to make fun of crypto speculation
- Since then championed (?) by Elon Musk
- Dog Money by Remy
- Litecoin (2011) another early example
- Ethereum, announced in 2013 and public 2015 a more “advanced” blockchain
- More possibility for smart contracts
- Basis for tokens, scripting…
- Coins with enhanced privacy features another important category

PROOF-OF-WORK OR PROOF-OF-STAKE?

- PoW has been criticized for being too costly, using too much electricity
- Bitcoin mining uses more power than a country like the Netherlands (roughly 100 TWhs annually)
- These estimates come with a great deal of uncertainty, however
- PoS is an alternative way to mine new blocks
- How many coins a miner stakes determines his "power"
- Energy needs minimized
- Criticized for fostering centralization
- Implemented on ethereum, no plans for bitcoin

BITCOIN NETWORK POWER DEMAND, 2018-2023



WHICH BITCOIN? THE BLOCKSIZE WARS

Hard Forks of Bitcoin

- Leading to several versions of bitcoin
- Bitcoin Core (BTC) and Bitcoin Cash (BCH) are the most important ones
- Each is an independent coin and blockchain
- Bitcoin Core is the "main" bitcoin

The Core Issue: the Blocksize

- Should there be a limit on the size of each block?
- Tradeoff: cheap transaction with bigger blocks
- Vs. larger fixed costs for mining, the danger of centralization

BLOCKSIZE

The Blocksize Limit

- The blocksize limit was added in 2010 by Satoshi, set at 1MB
- A security feature for the network: to avoid spamming that could take bitcoin down
- Transactions free at this point, therefore spamming was a potential risk
- Spamming could in theory raise the size of new blocks indefinitely
- Hence the limit – but it was only meant as a temporary security measure

Problems of the Limit

- The number of transactions limited to about 3 per second – much too little
- Scaling is impossible with this limit, transactions become very costly
- Transaction fees introduced, people bid for (artificially) scarce space on the blockchain
- Transaction fees became very high, defeating the purpose of bitcoin

THE BLOCKSIZE WARS

The Big Block Arguments

- It's impossible to scale bitcoin with small blocks
- Blocksize increases can easily be programmed into bitcoin
- The extra data storage needed is not a real problem
- It's reasonable to expect continuing improvement – Moore's Law also applies here

The Small Block Arguments

- Bigger blocks compromise the bitcoin network
- Costs of running a node increases
- Centralization of mining into fewer hands results
- Larger blocks are not necessary: bitcoin is only for ultimate settlement

RESOLUTION: BITCOIN CORE

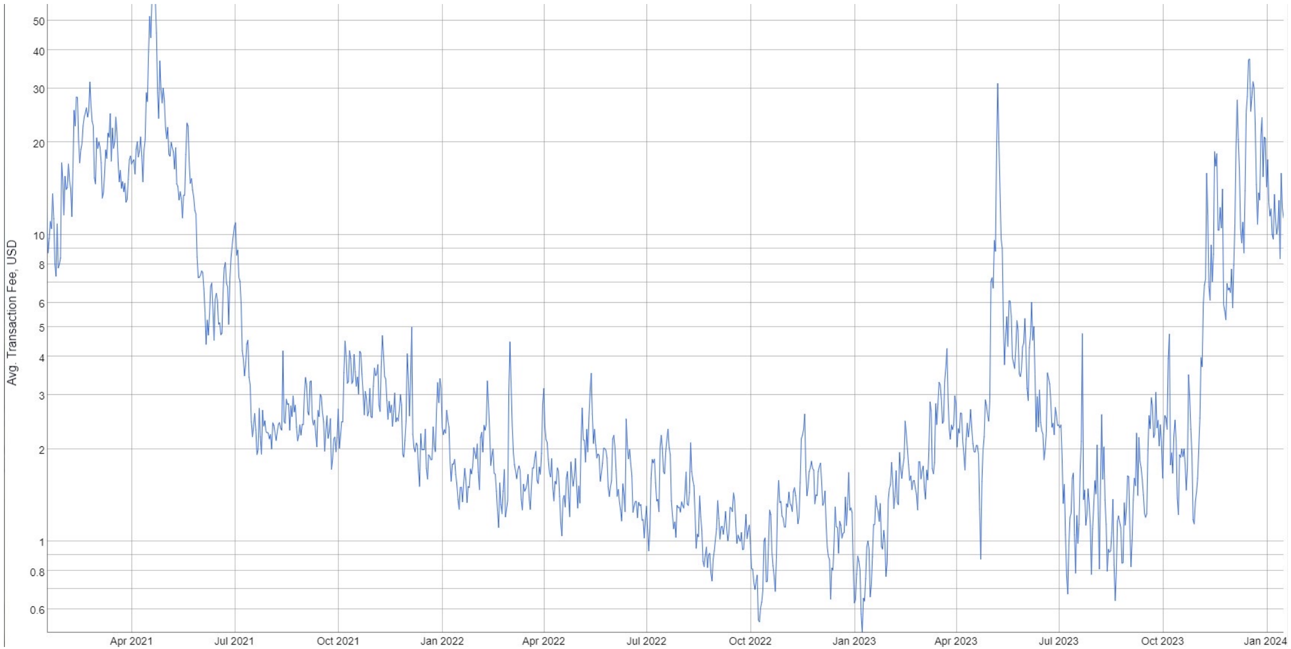
Small Block Solutions

- Block size limit, but BIP "segregated witness" would effectively raise the limit to 2MB
- Side chains and a "secondary layer" proposed: Blockstream and the Lightning Network
- Most of the (Chinese) miners were convinced by the Core team 2015

Developments Since

- Transaction costs rose on bitcoin from late 2016/early 2017 on, tops of over $50
- Much less more recently – generally below $1, but daily purchases effectively priced out
- Widespread adoption hampered – Steam discontinued December 2017
- The role of bitcoin (BTC): it's a store of value, a settlement asset – not cash
- Lightning Network has grown in popularity since 2021

BTC TRANSACTION FEES, 2021-2024



Source: bitinfocharts.com

RESOLUTION: BITCOIN CASH

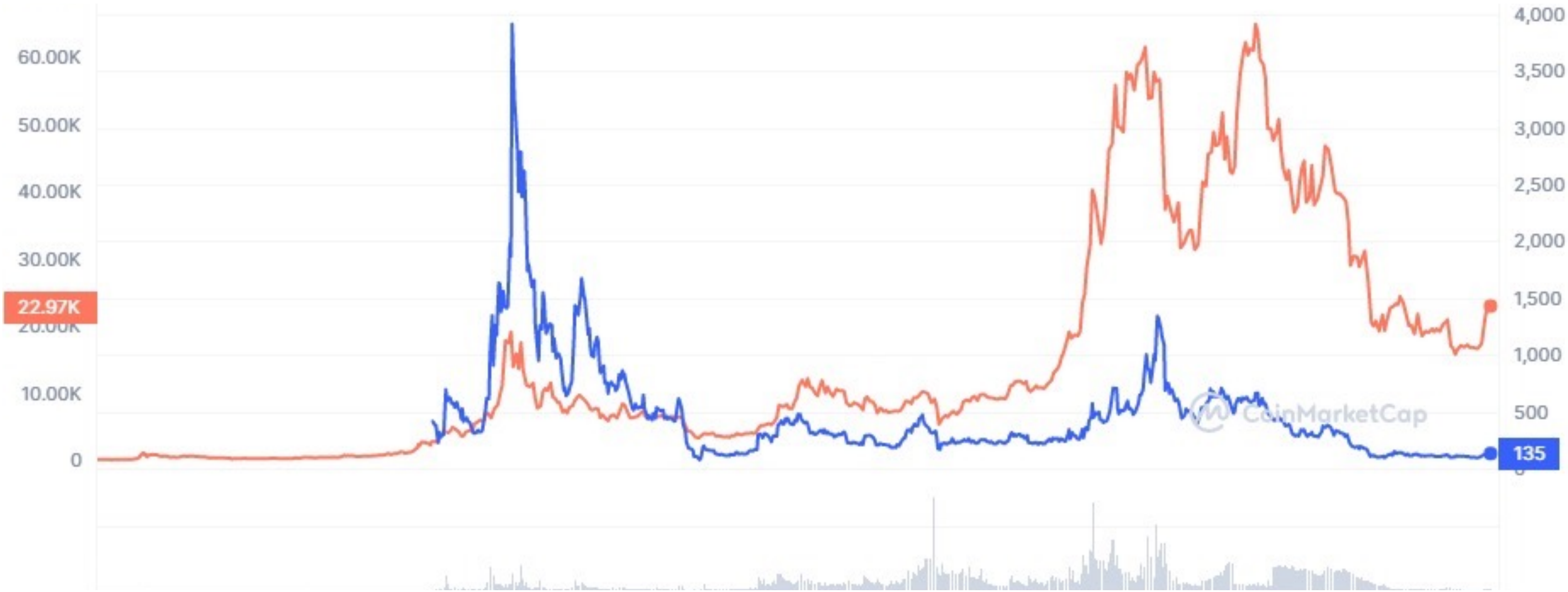
Hard Fork

- BIP that would raise the blocksize limit to 8MB rejected
- Hard fork from bitcoin (BTC) in 2017 lead to Bitcoin Cash (BCH)
- Most hashing power with BTC, “original” developer team with BTC
- Market value of BTC higher

Development Since

- Bitcoin Cash was very popular in the first years, but its popularity has since declined
  - ➢ Retail use of cryptos generally has declined
  - ➢ High fees on BTCs discourage it, confusion over forks?
- Innovation in traditional financial system caused costs to plummet
- In Europe, a hidden subsidy to credit card use make credit cards more desirable

BITCOIN CASH VERSUS BITCOIN CORE PRICE



Source: coinmarketcap.com

3. CENTRAL BANK DIGITAL CURRENCY (CBDC)

ORIGINS OF CBDCS

Early Discussions

- Academic discussions began around 2014-2015
- Discussions among central bankers in response to the rise of bitcoin
- Papers by BIS (2020), ECB (2020), Federal Reserve (2022)
- China (since 2014, active since 2020) and a few other countries already have a CBDC
- But little adoption so far: promoted via distributions, lotteries

Core Idea behind CBDC

- A digital form of the currently used currency (euro, dollar…)
- For use in the digital world, to promote financial inclusion
- Exchangeable at par with other forms (physical cash, bank money)

DESIGNING A CBDC

Blockchain or Central Issuer?

- Tokens
- Accounts with the central bank

Wholesale or Retail?

- Wholesale: a CBDC only available to banks and financial institutions, a settlement asset
- Retail: private persons have access to CBDC

Immediate or Mediated Access?

- Immediate: private persons have immediate access to CBDC
- Mediated: CBDC is administrated in accounts by banks, others

PURPOSES OF CBDC

Central Banks Want to Stay Relevant

- Claim that bitcoin shows demand for CBDC
- Claim that only central banks can provide a stable digital currency

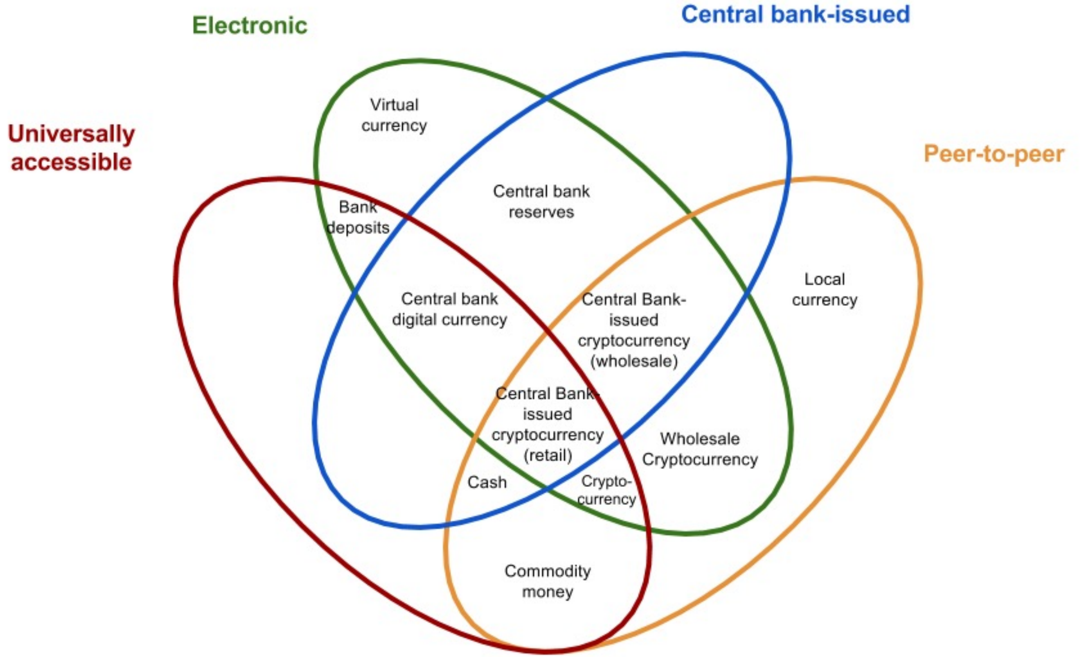
CBDC Necessary for Security

- To combat money laundering (Rogoff 2016)
- Prevent financing terrorism
- Privacy important, but conditional, CBs will have access to all transactions (ECB 2020)

CBDC a Potential Tool for Monetary Policy

- Negative interest rates
- Limits on cash holdings

THE MONEY FLOWER (BIS 2020)



CBDC AND MONETARY POLICY

Potentials of CBDC for Monetary Policy

- The "zero lower bound" on interest rates (Goodfriend 2000; Bordo & Levin 2017)
- Interest rate manipulation is difficult/impossible when nominal rates are low
- Negative rates → cash hoarding
- With a CBDC, a negative rate can be imposed on cash holdings

Encourage Spending, Penalizing Hoarding

- In a recession, it becomes possible to avoid "leakage" into hoards
- The central bank can penalize / outlaw "excessive" cash holding
- It can program money to lose value over time
  - ➢ E.g., after 1 month, holdings in excess of x euros will decline by 1 percent per month

CBDC, MONETARY POLICY AND PHYSICAL CASH

Physical Cash an Important Limit

- Negative rates can be avoided by shifting from CBDC to cash
- Same with programmed devaluation

Physical Cash and Other Concerns

- Surveillance through CBDC can be avoided through cash, other payments systems
- "Transparency" in this case really means complete government oversight and control
- Cash, private cryptos make this impossible – CBDC makes it possible, if no alternatives

Contradictory Central Bank Plans

- They want to respect privacy, they don't want to eliminate cash
- Their stated goals for CBDC can only be achieved by eliminating financial privacy, cash

CHINA, CBDCS AND INTERNATIONAL TRANSFERS

Wholesale CBDC as an Alternative to the Dollar

- China (and others) have plans for linking CBDCs
- E.g., BIS's Project mBridge (BIS 2022)
- One possible purpose: an alternative international payments system

Independent of the Dollar System

- It would make international trade risk less costly for countries not aligned with the U.S.
  - ➢ E.g., Iran, Russia, China
- Alternative to SWIFT for international payments
- Possible purpose: fixing exchange rates, recreating a system like Bretton Woods
  - ➢ Very unlikely

4. LITERATURE

LITERATURE

Bank for International Settlement. 2020. *CBDC: Central Bank Digital Currencies: Foundational Principles and Core Features*. Available online.

Bank for International Settlement. 2022. *Project mBridge: connecting economies through CBDC*. Available online.

Board of Governors of the Federal Reserve System. 2022. *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*. Washington, D. C. Available online.

Bordo, M. and A. Levin. 2017. Central Bank Digital Currency and the Future of Monetary Policy. *NBER Working Paper* no. 23711.

European Central Bank. 2020. *Report on a Digital Euro*. Frankfurt am Main. Available online.

Goodfriend, M. 2000. Overcoming the Zero Bound on Interest Rate Policy. *Journal of Money, Credit and Banking* 32, no. 4: 1007-35.

Rogoff, K. 2016. *The Curse of Cash*. Princeton, N. J.: Princeton University Press.

Satoshi Nakamoto. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online.