University of Warsaw
Faculty of Economic Sciences

Cryptocurrency

Łukasz Matuszczak, Phd

Introduction – basic concepts

- **Block.** A block is a group of Bitcoin transactions over a certain period of time. The transactions are verified by "**miners**," who are rewarded for verifying the transactions with newly created BTC.
- **Bitcoin units.** Each Bitcoin is divisible to eight decimal places. A millibitcoin (mBTC) is 1/1,000th of a Bitcoin. The smallest unit is a satoshi (sat), which is 1/100,000,000th of a Bitcoin.
- **Blockchain.** Each transaction forms an unbroken link on the chain. This transparent, public chain is what allows Bitcoin to exist and be usable. All blocks of transactions are linked to previous blocks of transactions, forming the etymology for the word "blockchain."
- **Mining.** Independent individuals or groups complete intensive and costly computer calculations to create a block.

Introduction – basic concepts

- **Blockchain address.** A sequence of 25 to 34 alphanumeric characters. This is the information that is given to other parties so they know where to send the coins.

- **Wallet.** Any individual or entity wishing to exchange Bitcoin (and not store them on an exchange, in someone else's custody) must create a digital collection of the credentials, known as a wallet, necessary to transact coins.
  - **Full clients.** This is a wallet that includes a full copy of the entire blockchain. This is the safest form of storage other than offline or "cold storage," but it requires substantial digital space.
  - **Lightweight clients.** This is a wallet that includes a more limited version of the blockchain to enable it to be portable on devices such as a smartphone. Since the entire blockchain is not available, a party using a lightweight wallet must trust intermediaries who have full wallets.

Introduction – basic concepts

- **Keys.** These are the credentials stored in the wallet. Like a safe deposit box, there are two keys necessary for each transaction.

  - **Public.** This is the technology necessary to encrypt and decrypt transactions. It is "one way," meaning that it easily unlocks transactions, but it can't be used to reverse the transaction. This key enables the blockchain to be uninterrupted.

  - **Private.** This is the passcode that transacting parties initiate so that the transaction is unique to themselves. To spend Bitcoin, one must know their own private key and digitally sign the transaction. The party's signature is verified by the public key without revealing the private key.

1. A brief history

•Before the creation of Bitcoin, there were quite a few examples of online digital currencies, but none succeeded in attracting much interest or establishing themselves in financial markets. Two examples of such currencies are B-Money and Bit Gold.

•In 2013, Forbes named Bitcoin (BTC) the year's best investment.

•In 2014, Bloomberg countered with its proclamation that Bitcoin was the year's worst investment.

•In October 2021, the Securities and Exchange Commission approved ProShares Bitcoin Strategy (ticker: BITO), the first U.S. Bitcoin futures exchange-traded fund.
•In November 2022, FTX – the leading cryptocurrency exchange by trading volume – declared bankruptcy, creating some of the darkest days in the crypto history timeline.

1 Bitcoin adoption and controversy

Some countries, most notably China, have banned Bitcoin and other cryptocurrencies. However, others are embracing it fully:

•El Salvador adopted Bitcoin as its legal tender in 2021 to resolve deep economic woes. The country has lost an estimated $40 million of its total investment in Bitcoin since adoption, leading many to question its value as legal tender given that the country is still struggling to meet its debt obligations and public health needs.

1 Bitcoin adoption and controversy

Some countries, most notably China, have banned Bitcoin and other cryptocurrencies. However, others are embracing it fully:

•Ukraine posted two crypto wallets at the beginning of the Russian invasion to raise funds, attracting more than $10.2 million within the first week to fund both humanitarian needs and military support. Ukraine anticipates rebuilding its economy using blockchain technology. Kuna, an exchange led by Michael Chobanian, has emerged as the most popular cryptocurrency exchange in Ukraine with about 60,000 active traders and over $100 million in assets. In February 2022, Kuna partnered with Ukraine's Ministry of Digital Transformation, a governmental agency formed in 2019 to create a universal access point for all electronic governmental services provided to Ukrainian citizens.

Kuna

1 Bitcoin adoption and controversy

•Iran has found Bitcoin to be an effective method to bypass U.S. financial sanctions on the country. Because of its abundant natural resources, Iran has easily pivoted to producing electricity for Bitcoin mining when the U.S. clamped down on its oil and gas operations.

• However, illegal Bitcoin mining activities have created significant electrical outages during peak usage periods in the country. All mined Bitcoin, currently valued at approximately $1 billion, must be sold to Iran's central bank. Iran also began accepting imports using cryptocurrency, placing its first international order worth $10 million immediately after the announcement in August 2022.

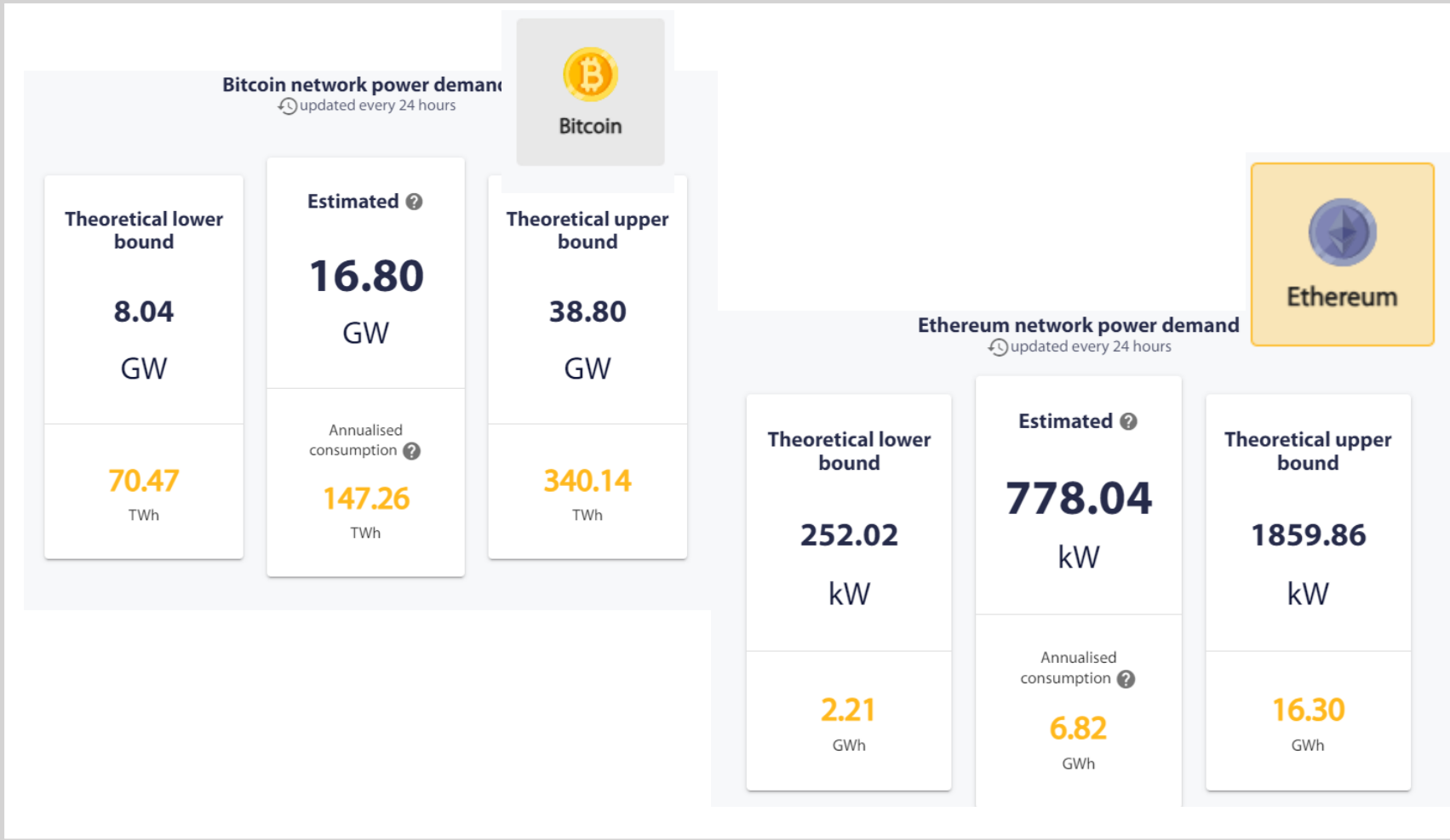
1 Bitcoin adoption and controversy

- Mining Bitcoin requires significant electricity use and is responsible for 0.1% of global greenhouse gas emissions. The University of Cambridge publishes the Cambridge Bitcoin Electricity Consumption Index (CBECI), which provides estimates on the greenhouse gas emissions related to Bitcoin.

- Its calculations show that Bitcoin miners release about 70 metric tons of carbon dioxide equivalent annually.
- Many rural, low-income communities have been selected for additional mining centers due to few zoning laws. The mining centers often bring a small handful of new jobs, but they create intense pressure on local resources and significant, 24-hour noise pollution.

1 Bitcoin adoption and controversy

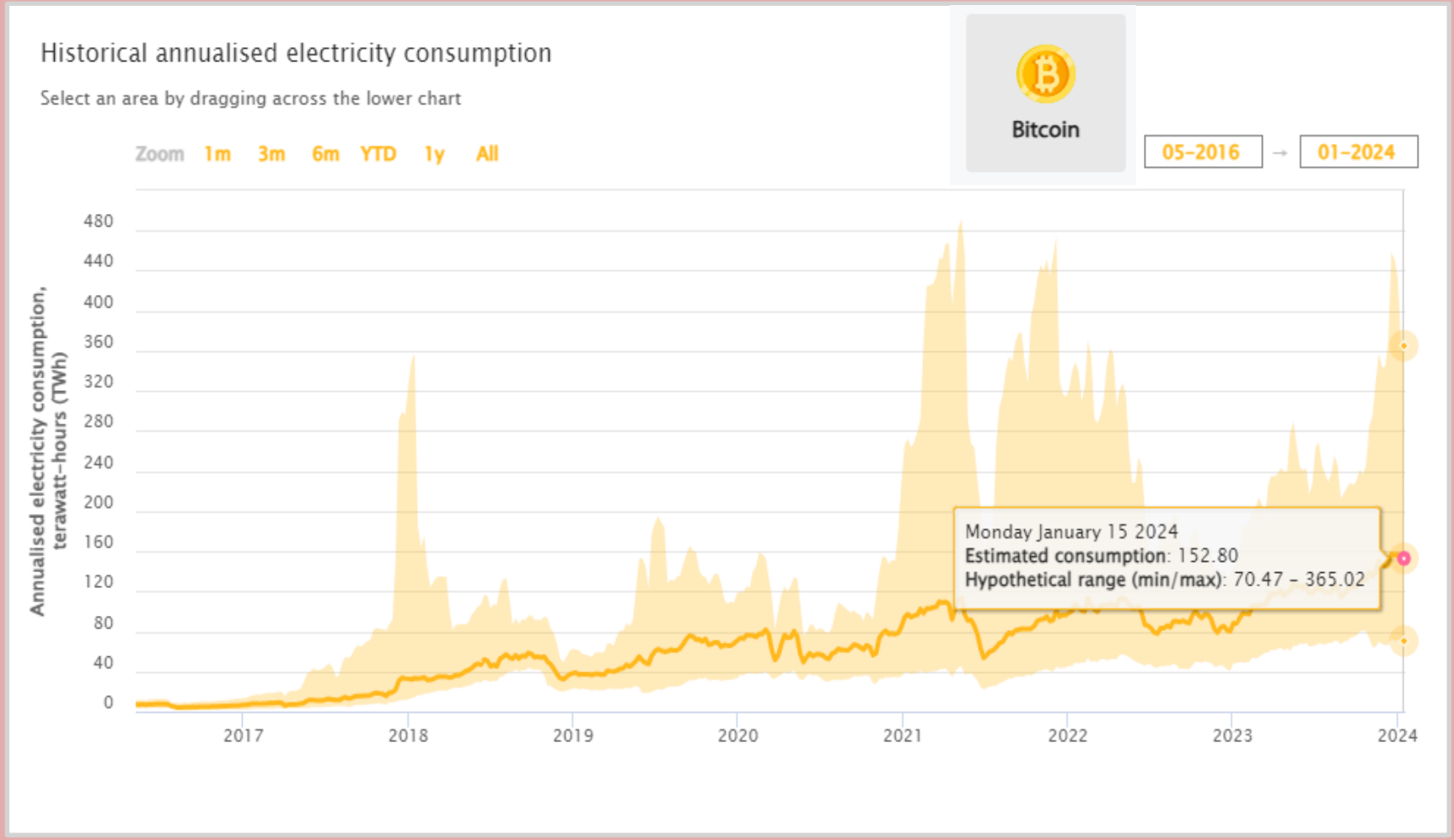
FIGURE 12-1



https://ccaf.io/cbnsi/cbeci

1 Bitcoin adoption and controversy

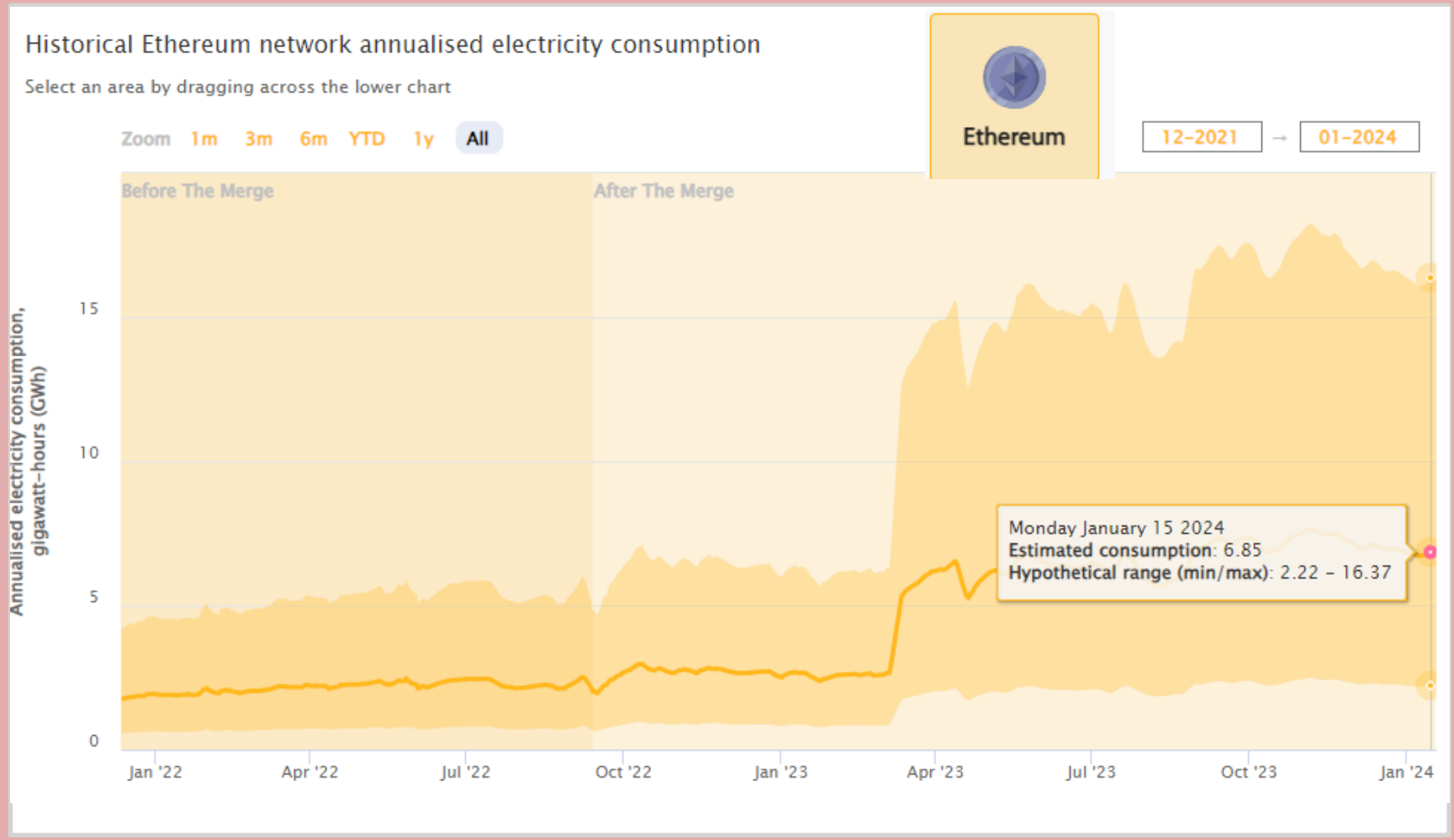
FIGURE 12-2



https://ccaf.io/cbnsi/cbeci

1 Bitcoin adoption and controversy

FIGURE 12-3



https://ccaf.io/cbnsi/cbeci

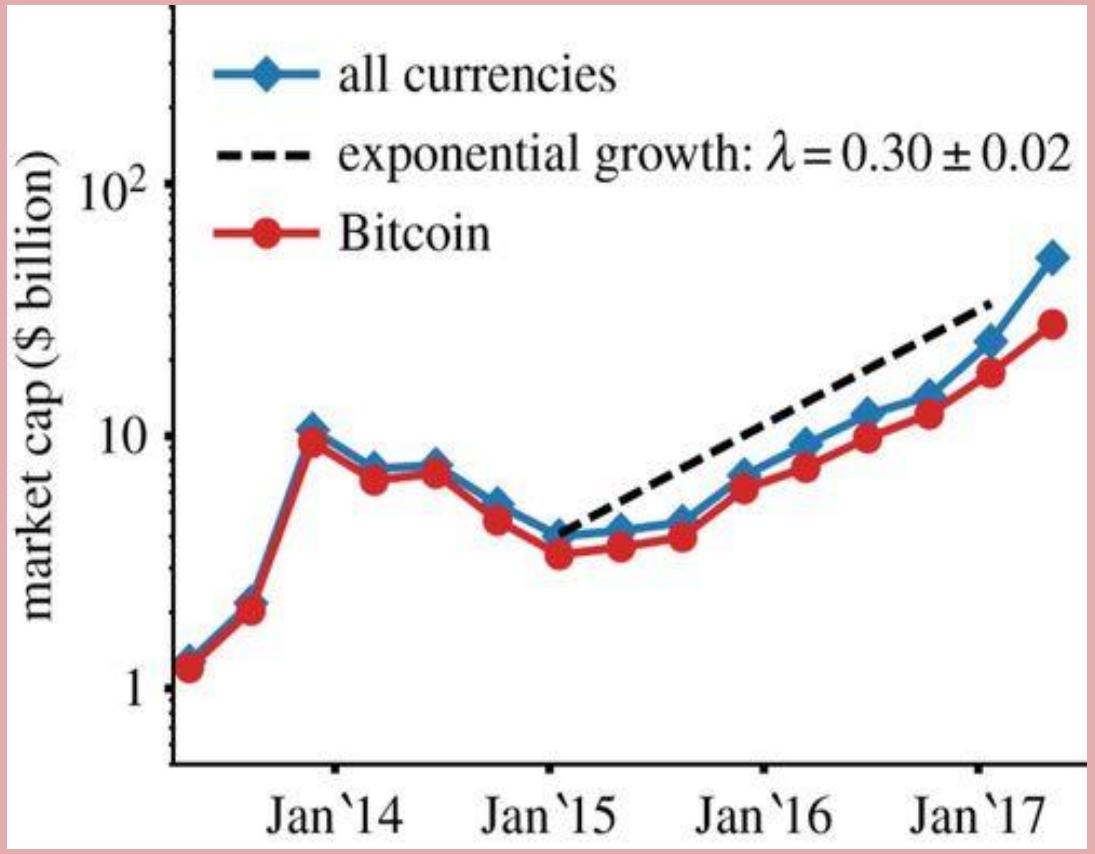
2 Bitcoin Price Trajectory

- After Nakamoto rolled out Bitcoin in 2009, he mined about 1.1 million Bitcoins and disappeared in 2010.
- The development responsibility was ceded to Gavin Andresen, formerly known as Gavin Bell, who worked to realize Bitcoin's decentralized vision. **This meant that there was no central authority, server, storage, or administrator.** The price of Bitcoin dropped with the new uncertainty surrounding these actions.

- The first real-world Bitcoin transaction occurred on May 22, 2010, a date known to Bitcoin enthusiasts now as Bitcoin Pizza Day. Laszlo Hanyecz paid 10,000 BTC to have two Papa John's pizzas delivered to him. The pizzas retailed for about $25. At the peak of Bitcoin's pricing in 2021, the two pizzas would have cost north of $680 million. Due to Bitcoin's extreme volatility, the pizzas would currently be worth about $250 million.

2 Market description

FIGURE 12-4 The total market capitalization

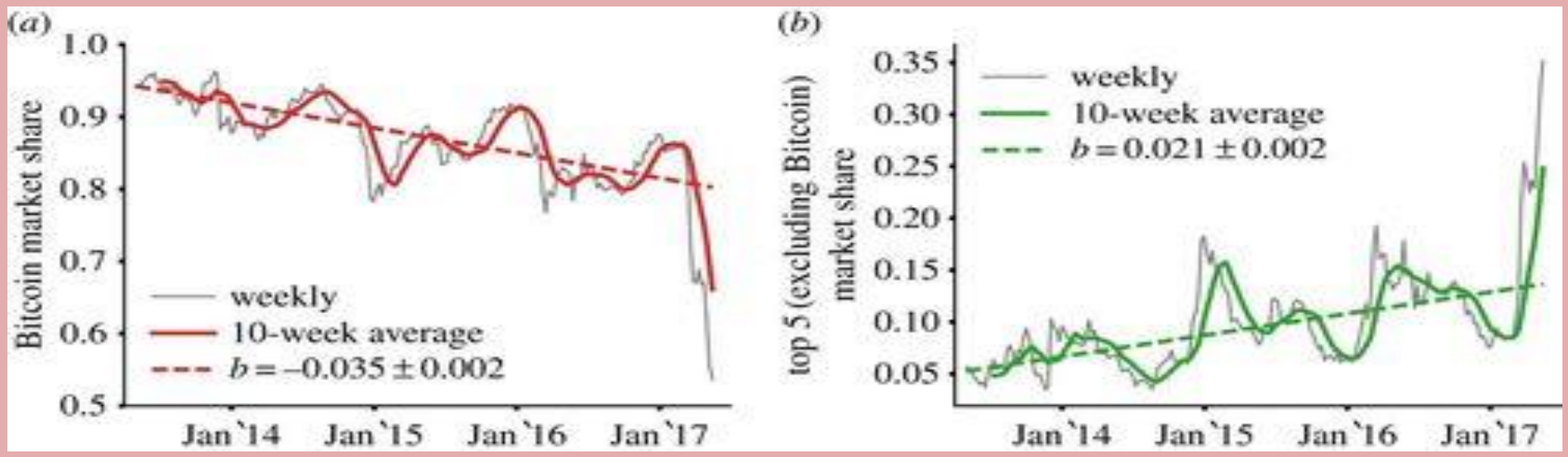


Evolutionary dynamics of the cryptocurrency market, Volume: 4, Issue: 11, DOI: (10.1098/rsos.170623)

- In the history between 28 April 2013 and 13 May 2017 there were 1469 cryptocurrencies, of which around 600 were active by that time
- The total market capitalization C of cryptocurrencies has been increasing since late 2015 after a period of relative tranquillity
- As of May 2017, the market capitalization is more than four times its value compared to May 2016 and it exhibits an exponential growth

2 Market description

FIGURE 12-5 The total market capitalization

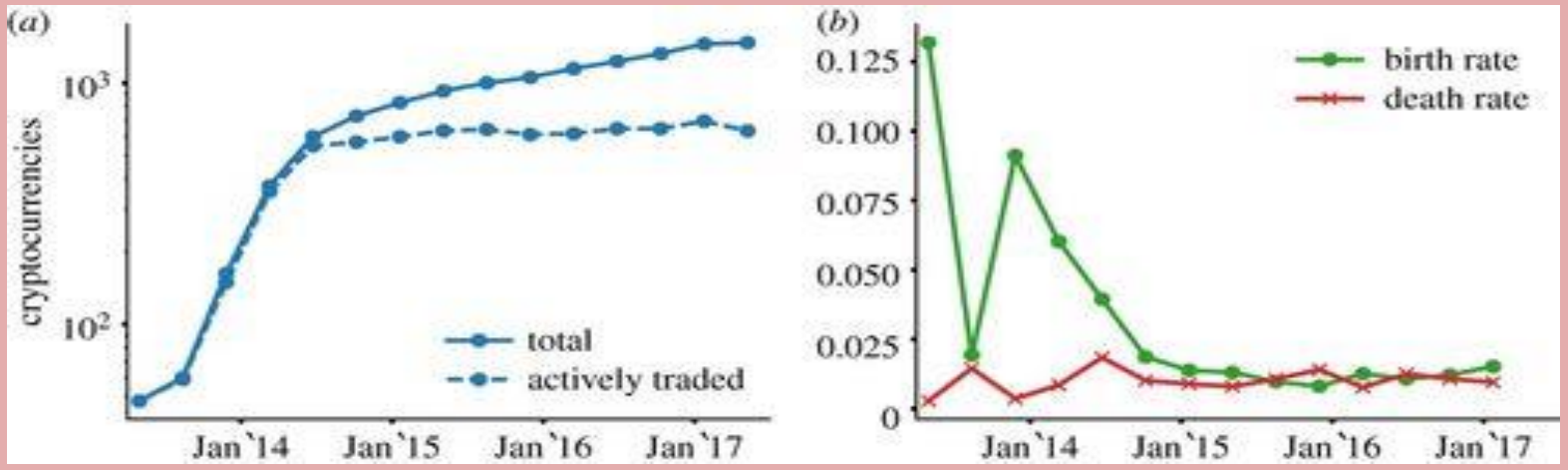


- Bitcoin's market share has been steadily decreasing for the past years, beyond oscillations that might mask this trend to short-term investigations.
- Neglecting the impact of nonlinear effects and potential changes in the competition environment, the model indicates that Bitcoin's market share can fluctuate approximately around 50% by 2025.
- Panel (b) showes that the top 5 runners-up have gained significant market share and now account for more than 20% of the market.

Evolutionary dynamics of the cryptocurrency market, Volume: 4, Issue: 11, DOI: (10.1098/rsos.170623)

2 Market description

FIGURE 12-5 **Stability of the cryptocurrency market**

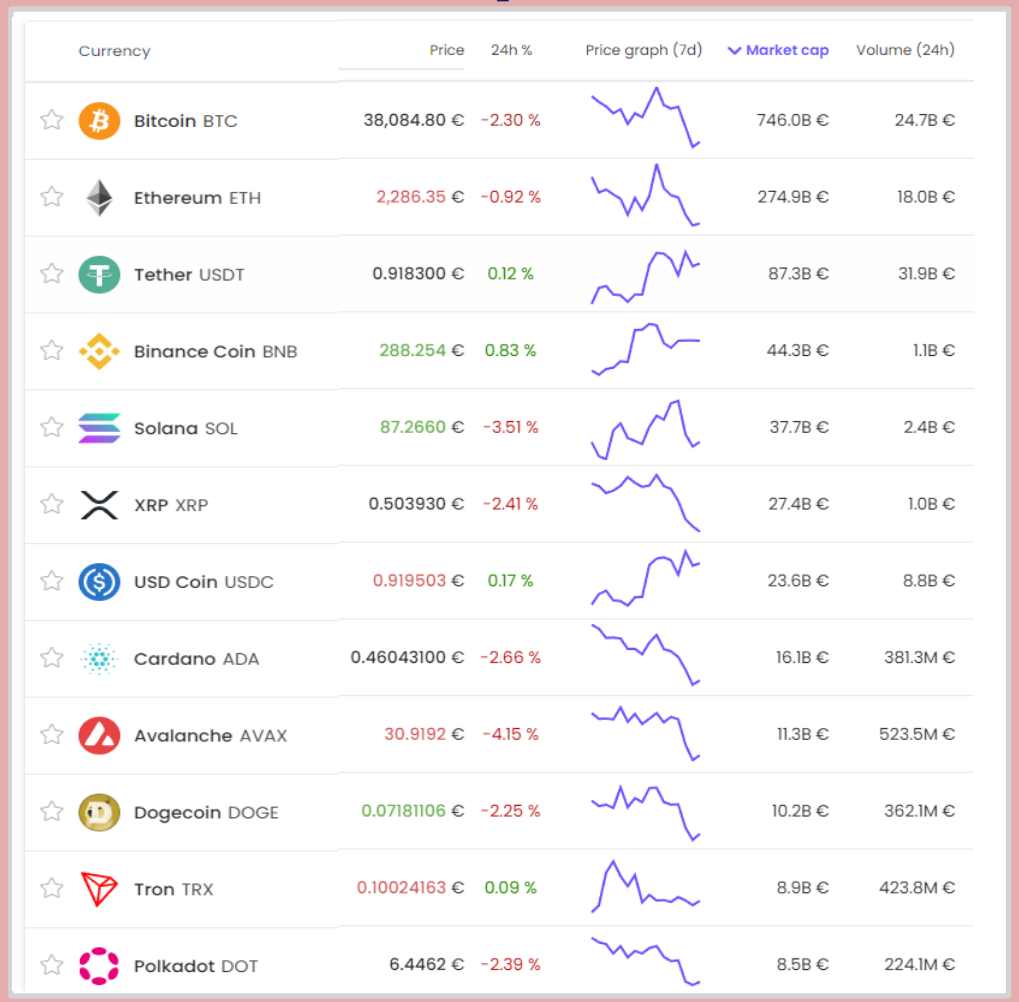


- Panel (a) shows the evolution of the number of active cryptocurrencies across time, averaged over a 15-week window.
- The number of actively traded cryptocurrencies is stable due to similar birth and death rates since the end of 2014 (b). T
- The average monthly birth and death rates since 2014 are 1.16% and 1.04%, respectively, corresponding to approximately seven cryptocurrencies appearing weekly while the same number is abandoned.

Evolutionary dynamics of the cryptocurrency market, Volume: 4, Issue: 11, DOI: (10.1098/rsos.170623)

2 Bitcoin Price Trajectory

FIGURE 12-4 The price evolution



Currency	Price	24h %	Price graph (7d)	Market cap	Volume (24h)
Bitcoin BTC	38,084.80 €	-2.30 %		746.0B €	24.7B €
Ethereum ETH	2,286.35 €	-0.92 %		274.9B €	18.0B €
Tether USDT	0.918300 €	0.12 %		87.3B €	31.9B €
Binance Coin BNB	288.254 €	0.83 %		44.3B €	1.1B €
Solana SOL	87.2660 €	-3.51 %		37.7B €	2.4B €
XRP XRP	0.503930 €	-2.41 %		27.4B €	1.0B €
USD Coin USDC	0.919503 €	0.17 %		23.6B €	8.8B €
Cardano ADA	0.46043100 €	-2.66 %		16.1B €	381.3M €
Avalanche AVAX	30.9192 €	-4.15 %		11.3B €	523.5M €
Dogecoin DOGE	0.07181106 €	-2.25 %		10.2B €	362.1M €
Tron TRX	0.10024163 €	0.09 %		8.9B €	423.8M €
Polkadot DOT	6.4462 €	-2.39 %		8.5B €	224.1M €

- In January 2013, the price of a single Bitcoin **exceeded $1,000** for the first time.
- The market's biggest cryptocurrency exchange was a website called Mt. Gox. In January 2014, it was hacked. The hackers got away with **850,000** bitcoins
- **2017: Bitcoin reaches $20,000**
- **2018: Back to Reality:** The market's growth was unsustainable, so in retrospect it seems inevitable that the bubble burst and prices began a step decline. Many projects collapsed as they were poorly conceived or too ambitious.

https://kriptomat.io/cryptocurrency-prices/

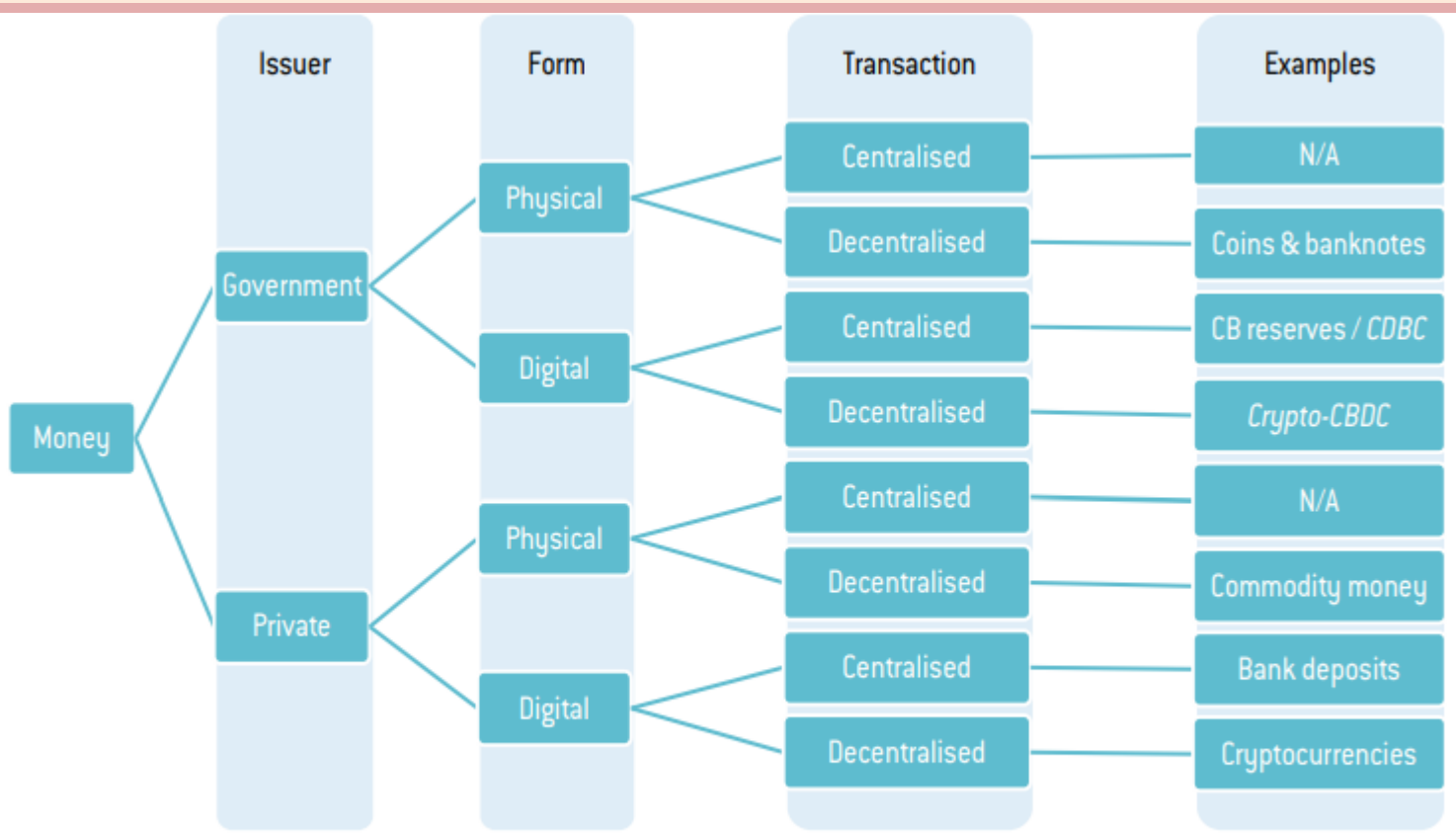
3 Cryptocurrencies and monetary policy

•The emergence of cryptocurrencies enabled by the development of intelligent digital technologies could be a challenge to the monopoly of official central bank-controlled currencies.
•Cryptocurrencies are increasingly thought of as actual currencies that can be used as mediums of exchange

•Money is a social convention that, in particular, facilitates trade when there is a lack of a double coincidence of wants by solving the problem of a lack of trust in exchanges. Money characteristics: **a unit of account, medium of exchange, a store of value.**

2 Market description

FIGURE 12-5 **Stability of the cryptocurrency market**



Source: Bruegel based partly on the typology proposed by Bech and Garratt (2017). Note: CDBC stands for Central Bank Digital Currency (not discussed further in this Policy Contribution).

3 Cryptocurrencies and monetary policy

Cryptocurrencies would thus represent a form of money that was not previously available as a particular combination in the money taxonomy. Specifically, cryptocurrencies are:

- Privately issued. This is not new per se. Privately-issued currencies have been used and have performed well in the past. However, unlike bank deposits, they are not a liability and cannot be redeemed.

- Digital. This is also not new per se; it is similar to electronic money issued by central and commercial banks. Like this type of money, cryptocurrencies are also fiduciary (they have no intrinsic value).

- Allowing the settlement of transactions in a decentralised fashion. Exchanges via cryptocurrencies are peer-to-peer. Decentralised ledger technology (DLT) – for example, the blockchain – is used to avoid the so-called 'double spending problem' that arises with digital currencies because of their easy replicability and which is traditionally solved through record-keeping by a trusted central agent. This means that with a DLT there is no central authority needed for the settlement of digital transactions between counterparties1

3 Cryptocurrencies and monetary policy

What are the conditions for currencies to fulfill the functions of money?

Historically, two key features have characterised successful currencies: price stability and a sufficiently large network of users. In other words, unless the value of money is relatively stable over time, it will not be widely used, either as an accounting device or a medium of exchange.

- Digital. This is also not new per se; it is similar to electronic money issued by central and commercial banks. Like this type of money, cryptocurrencies are also fiduciary (they have no intrinsic value).

- Allowing the settlement of transactions in a decentralised fashion. Exchanges via cryptocurrencies are peer-to-peer. Decentralised ledger technology (DLT) – for example, the blockchain – is used to avoid the so-called 'double spending problem' that arises with digital currencies because of their easy replicability and which is traditionally solved through record-keeping by a trusted central agent. This means that with a DLT there is no central authority needed for the settlement of digital transactions between counterparties.

3 Cryptocurrencies and monetary policy

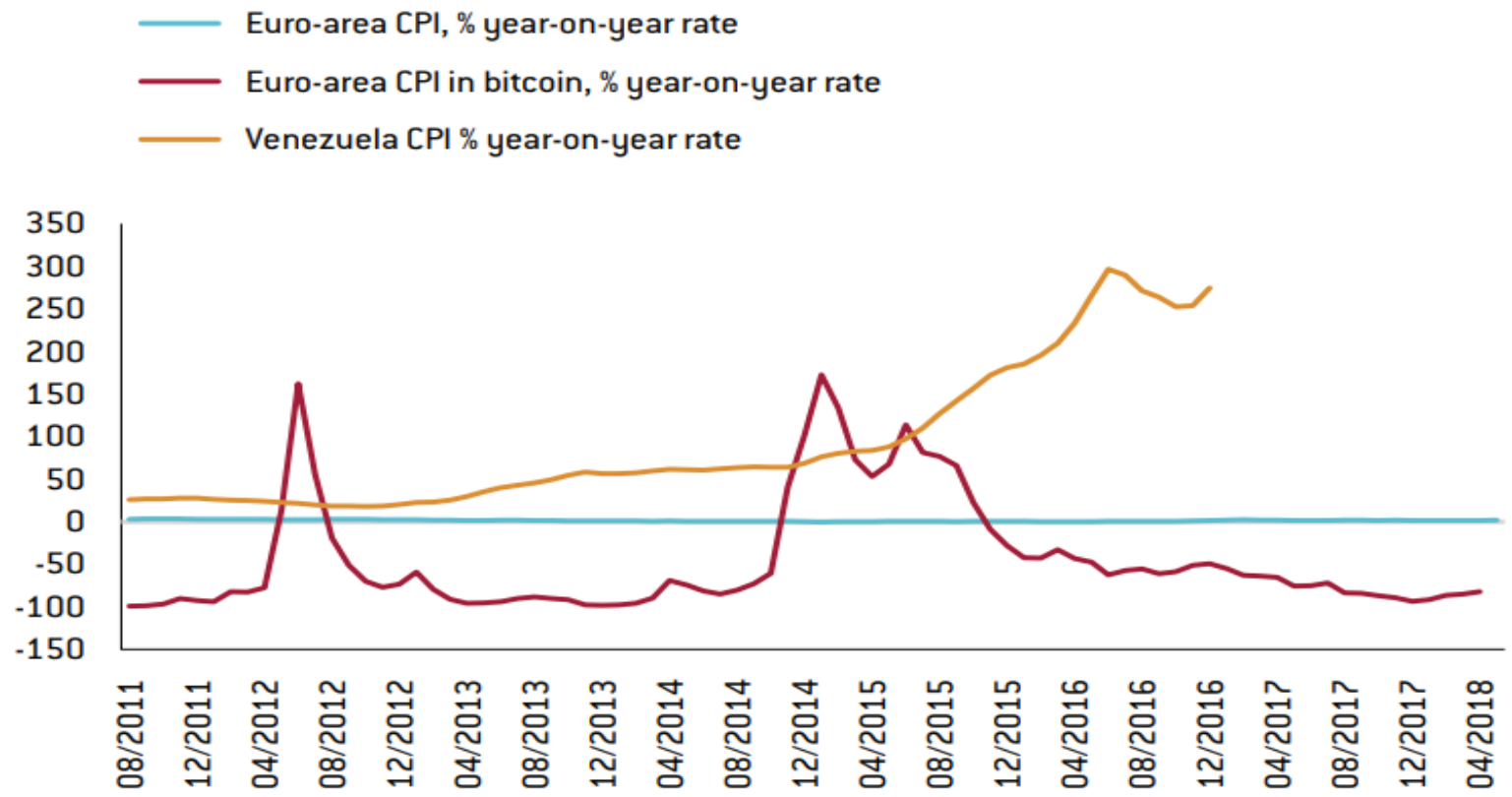
Evaluating the money role of cryptocurrencies?

1. The first reason for this is the inherent volatility of the values of today's main cryptocurrencies, which are by-products of their supply protocols. In the case of bitcoin, the quantity supplied is fixed at an upper limit (21 million), which is approached following a predictable, near-predetermined path.
   Importantly, the supply does not match the quantity demanded

2. The inelastic nature of the supply embedded in the protocol rules (which for bitcoin looks like a rule derived from the gold standard) **results in volatility**, which prevents these currencies from functioning as good stores of value. This, in turn, also limits their adoption and keeps the network of users relatively small.
   Reducing their role as mediums of exchange and as units of account

2 Market description

FIGURE 12-5 **Inflation in the euro area (in €, bitcoin) and in Venezuela**



Sources: Bruegel based on Bloomberg, ECB and IMF. Note: Venezuelan CPI is not available in monthly frequency after the end of 2016. However, the IMF reports a yearly inflation rate for 2017 of 1087.5 percent.

3 Cryptocurrencies and monetary policy

Evaluating the money role of cryptocurrencies?

3. Cryptocurrencies are not a good medium of exchange because of the cost of the transactions and the time they take to be recorded in the decentralized ledger.
4. The borderless nature of today's main cryptocurrencies could also be a major issue: price stability means that the basket of goods and services included in the CPI of a particular (homogenous) jurisdiction has a stable price. However, current cryptocurrencies are global and not attached to a particular country or region. From a monetary policy perspective, a global cryptocurrency area **is unlikely to be an optimal currency area**, as this would lead to an inability to adjust exchange rates within the 'area.' **The result would thus be a crypto-monetary policy.**

5. Other major risks that could undermine trust in cryptocurrencies could arise from market concentration (which could lead to the falsification of the ledger and to 'double spend' issues), from the manipulation of the value of the currency via insider trading and from the reliance on unregulated intermediaries necessary to use cryptocurrencies

3 Cryptocurrencies and monetary policy

Crypto- and official currencies: a 'peaceful' coexistence?

- The extent of economic agents substituting cash and bank deposits for cryptocurrencies will determine the effectiveness of monetary policy. Extensive substitution of bank deposits, in particular, would translate to reduced control over monetary conditions because of the shrinking of the amount of broad money in the economy.
    - However, as Stevens (2017) points out, as long as money issued by central banks retains the role of a unit of account, the switch to cryptocurrencies as a medium of exchange would be limited and thus, the associated threat to monetary control would also be limited
- Second, the shrinking role of central bank money creates a possible fiscal risk in the form of reduced seigniorage revenue. The response could be higher distortionary taxes that would hurt growth. That said, such risks appear to be exaggerated given that seigniorage revenues make up an insignificant fraction of total government revenue.
- The last, but probably most pertinent, threat does not emanate from the potential use of cryptocurrencies as money, but from their attractiveness as investment assets. As a speculative investment – an investment made in expectation of a return from capital gains only – cryptocurrencies will be prone to bubbles

3 Cryptocurrencies and monetary policy

Crypto- and official currencies: a 'peaceful' coexistence?

- Given the natural monopoly enjoyed by central bank-controlled currencies, it would take a deep crisis of trust for a cryptocurrency to replace an established currency in full.
    - An episode of very high inflation could be such a shock, but even then, agents might wish to switch to other established safe-haven currencies

- Deposit guarantees would not be available as a solution in a crypto-financial system
- In the case of today's fiat government currency, the possibility for users to hold and store its physical form (ie bills and coins) is fraught with security risks and inconvenience.
- It seems that in a full crypto-financial system, savers would have to choose between holding IOUs labelled in a cryptocurrency unit of account issued by unstable banks (not benefiting from a lender of last resort) or sticking to cryptocurrencies that stay idle in the ledger. In that case, who would provide lending to the rest of the economy?

3 The greatest drama in Bitcoin history

•FTX grew aggressively through high-profile acquisitions and splashy marketing campaigns, including celebrity and social media influencer endorsements. The marketing message was focused on higher yields than typical bank accounts.

•FTX was led by Sam Bankman-Fried, colloquially known as SBF, and operated in conjunction with Alameda Research, another SBF-founded entity run by Caroline Ellison, SBF's romantic partner at the time.

•In November 2022, CoinDesk published an article detailing FTX's precarious financial risks, lack of accounting oversight and potential criminal use of customer assets. Shortly thereafter, FTX went into bankruptcy as it could not create enough liquidity to cover an $8 billion shortfall from panicked customers and the collapse of the FTT digital token on which Alameda Research relied for its operations.

•On Dec. 12, 2022, SBF was arrested and indicted by the U.S. District Court on eight criminal charges, including money laundering, wire fraud, campaign finance violations and securities fraud. His $250 million bond was the largest in history.

2 The greatest drama in Bitcoin history

•On Nov. 2, 2023, SBF was convicted on seven federal counts and will be sentenced in March 2024.

•FTX was assigned a new CEO named John J. Ray III, an attorney who specializes in recovering failed corporate assets and whose most notable case was the aftermath of the Enron collapse in the early 2000s. Ray is working to claw back assets from diverse sources such as crypto exchange Bybit and SBF's parents, Joe Bankman and Barbara Fried, both tenured Stanford University law professors.

•As of early September 2023, over $7 billion in cash and liquid assets of the estimated $8 billion total assets missing have been recovered.

•FTX investors have filed a class action civil lawsuit against FTX, its celebrity/influencer endorsers and significant venture capital investment firms, which is still pending.

• .

3 Cryptocurrency theft statistics

Few government regulations

- Because cryptocurrency platforms are not regulated by a central authority, they are subject to fewer government regulations.

- Although some people view this as a positive, it also means there aren't as many rules for securing systems from unauthorized access or protecting users in the event of a security breach.

- For example, compared to a bank, cryptocurrency platforms might have less rigorous systems for password management, two-factor authentication, and data encryption. They might also lack the same level of fraud mitigation tactics, physical security measures, and Know Your Customer (KYC) processes.

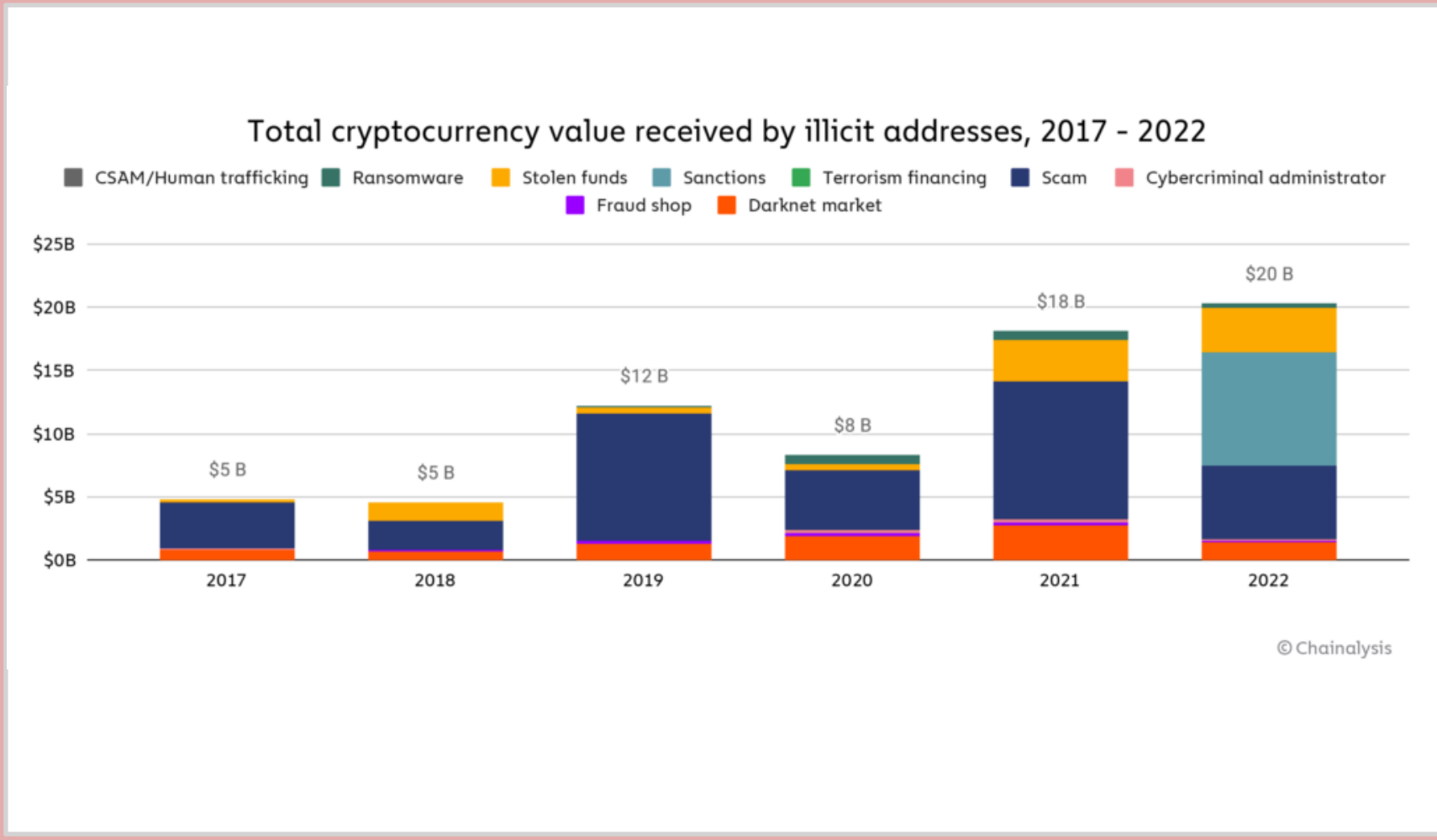
3 Cryptocurrency theft statistics

Cryptocurrency theft statistics

1. Cyber criminals stole a record $3.8 billion in cryptocurrency in 2022, according to a report from the blockchain analysis firm Chainalysis. It represents a 15% increase over the previous year ($3.3 billion).
2. As reported by CNBC, the value of Bitcoin **fell by more than 60%** in 2022, and 60% of surveyed Americans now consider digital currency investments "highly risky," up from 45% the year before.
3. There were 198 reported crypto thefts in 2022, according to research from Comparitech. This represents a 45% increase compared to 2021 (136).
4. **North Korean hackers are responsible for the majority of crypto thefts**, with crooks linked to the country stealing an estimated $1.7 billion in cryptocurrency in 2022.
5. There were 57 cryptocurrency thefts in the first quarter of 2023. At this rate, there may be a record 228 incidents in the year.

2 Bitcoin Price Trajectory

FIGURE 12-4 Cryptocrime report introduction



https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction//

Cryptocurrency theft statistics

6. October 2022 was "the biggest single biggest month ever for cryptocurrency hacking," with 32 attacks and more than $775 million lost.
7. In November 2022, the cryptocurrency exchange FTX spiraled into bankruptcy, creating a wave of crypto crime. Its users were subjected to a scam offering a refund, $415 million of crypto was stolen in a series of cyber attacks, and another $3.1 billion was wiped from the market.
8. Three of the five biggest crypto heists of all time were on exchange platforms. The largest of these was a cyber attack at Binance, in which $570 million was stolen.
9. DeFi protocols were the most common target for crypto hackers in both 2021 and 2022. They accounted for 82.1% of all attacks in 2022, up from 73.3% the year before.
10. The ten biggest crypto scams of 2022 were all fake investment opportunities. The most successful of these was Hyperverse, which attracted almost $1.3 billion in bogus revenue.

Biggest cryptocurrency heists of all time

Ronin Network ($620 million stolen)

- In March 2022, Ronin Network disclosed that it had fallen victim to a social engineering scam in which a senior engineer had downloaded a PDF file containing spyware.
- This gave the attacker control of four of the network's private validator keys, which helped them steal more than 173,000 Ethereum, worth $595 million at the time, plus another $25.5 million from a bank account.
- Ronin Network, a blockchain platform created by Sky Mavis for the online game Axie Infinity, said that its DAO validator nodes had been compromised and the funds had been drained in two transactions.
- The US Treasury Department later attributed the attack to North Korea's Lazarus group. Meanwhile, the Ronin Network relaunched three months later and began compensating those affected.

Thank You for your attention!