

# Comment



Bitcoin is now a legal currency in El Salvador.

JOSE CABEZAS/REUTERS

## Crypto and digital currencies – nine research priorities

Andrew Urquhart & Brian Lucey

To avert privacy breaches, scams and environmental damage, governments and central banks need to know how best to regulate this financial frontier.

**M**oney is at a crossroads. A race is on to decide who creates it, who can access it and how, who controls it, and to what degree and how it is regulated. The outcome could decide whether governments have access to all our financial data, whether criminals can easily launder vast sums unseen, and whether the benefits of finance can be extended to the billions of people globally who lack access to banks.

Cryptocurrencies – private monetary systems that use digital encryption to perform and verify transactions – have been around

since Bitcoin was developed in 2008 (ref. 1). Now, nearly 20,000 cryptocurrencies are in circulation, with a total market value of around US\$2 trillion.

Institutional investors are accumulating them. In the United States, many have dabbled publicly in this market, including: life-insurance company MassMutual; investment bankers JP Morgan Chase; hedge-fund manager Paul Tudor Jones; business-intelligence company MicroStrategy; and electric-vehicle manufacturer Tesla. More than 150 cryptocurrency hedge funds have sprung up to invest billions of dollars solely in these assets. The

financial system is adapting, with bitcoin futures, options and exchange-traded funds now available. Coinbase, the leading exchange, is listed on the NASDAQ stock exchange.

Cryptocurrencies can potentially be used to hedge against inflation. Inflation fears are being stoked by the falling value of conventional currency. Governments and central banks deliberately expanded the money supply to invigorate economies during the 2008 global financial crisis and the COVID-19 pandemic. By contrast, the maximum supply of bitcoins is fixed at 21 million bitcoins.

Cryptos can offer financial independence. In 2021, El Salvador became the first nation to accept Bitcoin as a parallel official currency to the US dollar. The country's president, Nayib Bukele, thinks that cryptocurrencies can deepen financial inclusion and reduce economic dependence on the United States. Last year, the nation deposited US\$30-worth of bitcoins into each citizen's digital wallet, around one-tenth of the industrial minimum monthly wage. Technical issues plagued the launch, however, including hacked accounts, verification difficulties, poor information-technology infrastructure and delays. In the past month, Ukraine has begun accepting donations in cryptocurrency to fund its defence against the Russian invasion.

Yet, in our view, great challenges need to be addressed before electronic currencies can become mainstream.

Bitcoin's value is notoriously volatile: 2021 saw swings of 50–100%. Vast amounts of energy are needed to run the complex computer codes that underpin cryptos. Currently, Bitcoin alone has an estimated annual carbon footprint equal to that of Kuwait and an electricity footprint equal to Thailand's, and produces as much electronic waste as the Netherlands. To get around this, El Salvador uses electricity generated by geothermal power near a volcano to decrypt its bitcoins. Lack of regulation also worries bankers and policymakers.

For all these reasons, China banned the mining of bitcoins last July. That August, the chair of the US Securities and Exchange Commission (SEC) warned that cryptocurrency platforms need regulation to survive. And in January this year, the UK Financial Conduct Authority (FCA) expressed concern over its inability to control cryptocurrency exchanges.

In parallel, several economies, including China and the European Union, are developing forms of digital assets over which they do have control. Central bank digital currencies (CBDCs) are an electronic record of the

## Key terms

### A money glossary.

**Blockchain.** A distributed database that registers information electronically in a digital form. Data are structured into blocks that are linked to previous ones through cryptographic codes.

**Cryptocurrencies.** Digital assets secured by cryptography. Many, including Bitcoin, use blockchain technology to store transactions.

**Central bank digital currencies.** The virtual format of a fiat (official) currency: an electronic record, governed and regulated by state or federal monetary authorities.

**Fiat currency.** A national currency that is not pegged to the price of a commodity such as gold or silver. Central banks or governments control how much is issued. The US dollar is one example.

official currency, and might replace physical banknotes and coins within a decade. China is already testing a digital version of its yuan, with which customers can make payments over their mobile phones. Last July, the EU launched

## “Bitcoin alone has an estimated carbon footprint equal to that of Kuwait.”

a project that will examine the feasibility of a digital euro over the next two years. Later this year, the US Federal Reserve will release a discussion paper on a digital dollar.

### Nine priorities

Although there's been much progress<sup>2</sup>, research is urgently needed on four fronts: legality, scalability, usability and acceptability. These are interconnected; solutions in one area might exacerbate problems in another. Here we set out nine priorities.

**Curb criminality.** The anonymity of cryptocurrency transactions means that they appeal to criminals and bad actors. Cryptos are used

to launder money, fund terrorism and fuel corruption<sup>3</sup> – it's been estimated that up to half of bitcoin transactions could support illegal activities<sup>4</sup>. Cryptocurrencies might be used to bypass financial sanctions, such as those currently imposed on Russia.

Solving this problem is close to impossible – cash has been used to carry out all the crimes for which cryptocurrency is blamed. But options could be considered. Cryptocurrencies could monitor users and introduce 'know-your-customer' forms of authentication, a feature absent up to now. But that would go against their principles of privacy and ownership, lowering their uptake. Researchers need to examine such trade-offs.

CBDCs have the opposite problem. They could allow central banks and governments to track everyone's transactions – a digital panopticon. However, if implications for privacy and rights were addressed, such transparency might deter and expose crime, as well as increasing tax revenues and diminishing black-market trade.

**Regulate digital assets.** At one extreme, cryptocurrencies are banned, as in China, Iraq and Egypt. At the other, they are mainstream, as in El Salvador. In most other countries they are permitted, yet not seen as legal tender. Trading is unregulated and they are treated as just another asset. Scams and misselling are rife.

Researchers need to ask: what is the optimal regulatory framework for digital assets to prosper in? And, how can regulators work in this space to the benefit of all?

Major global regulators such as the SEC in the United States and the FCA in the United Kingdom would like to see cryptos regulated much like other financial assets. Only qualified investors and authorized brokers should trade. Again, that would make cryptos less attractive, potentially crashing the market. Private currencies have existed before. In medieval times, and in nineteenth-century United States, Sweden and Australia, for example, individuals and banks could issue currency. These were all regulated out of existence.

**Cut energy use.** Cryptocurrencies are computationally intensive (see 'Bitcoin balance sheet'). Creating ('mining') some cryptocurrencies requires solving difficult cryptographic puzzles. Adding transactions to a digital ledger, such as the blockchain (see 'Key terms'), demands verifications by algorithms. All those calculations consume energy. A report from the UK financial site MoneySuperMarket.com found that bitcoin is more energy



ALESSANDRO BIANCHI/REUTERS

Employees work on bitcoin-mining computers in a Bitminer factory in Italy.

hungry than Norway. The report found that processing one transaction consumes more than \$100 worth of electricity, and generates more than 800 kilograms of carbon dioxide (see [go.nature.com/3wzhkmw](https://go.nature.com/3wzhkmw)). The next most popular cryptocurrency, Ethereum, consumes less energy but still adds 62 kilograms of CO<sub>2</sub> per transaction.

These high rates stem mainly from the choice of ‘consensus mechanism’ – all miners must agree on the computed solution to verify a transaction. Bitcoin uses a proof-of-work (PoW) system. If a miner is successful, they can propose a new block of transactions to the blockchain, and receive a reward. The reward diminishes in value but is still high: it started out at 50 bitcoins and halves every 210,000 blocks (roughly every 4 years), reaching 6.25 bitcoins for each block created in 2022. Lots of miners compete for the reward, hiking up energy use.

Shifting to an alternative consensus process – proof of stake (PoS) – could reduce energy consumption one-million-fold. Miners compete instead on the basis of their holdings of the coin. Ethereum is moving to PoS during 2022. But regulation and taxation risk disincentivizing PoS coins.

More research is needed on how incentives and sanctions can reduce energy needs. Options range from outlawing profligate protocols to nudges towards more efficient ones through regulatory or tax favouritism.

**Speed up transactions.** To replace existing systems of payment, cryptocurrencies will need to challenge retail and commercial banking settlement systems (such as SWIFT). These process payments in seconds and handle quadrillions of dollars per year. By contrast, Bitcoin handles 250,000 confirmed transactions per day, with a market value of \$1 billion to \$2 billion. Its transactions can take tens of minutes – much too slow for global market needs. Researchers need to find ways to speed them up.

**“Transactions can take tens of minutes – much too slow for global market needs.”**

A handful of cryptocurrencies can handle large volumes of transactions. EOS, for example, can manage 50,000 transactions per second. But it is a centralized cryptocurrency, less private than Bitcoin.

Volatility adds complications. In any monetary transaction, both sides want certainty in the value of an asset<sup>4</sup>. Yet bitcoin values can vary by 10% in minutes. Few will sell goods if they lose a big chunk of value between sale and settlement.

Bypassing some of the cumbersome blockchain technology goes part of the way to

solving the speed problem. Adding a second layer to a network can enable transactions off the blockchain. Bitcoin, for example, introduced such a ‘lightning network’ in 2018, although it has only recently become popular. It allows two parties to make or receive payments swiftly off-chain, while the transactions are logged.

**Manage volatility.** Cryptocurrency prices can have massive swings<sup>5</sup>. Last year, Bitcoin rose from \$37,000 in January to \$64,000 in April, falling back to \$37,000 by July then rising again to \$67,000 in November. That June, a mid-sized coin (Iron Titanium) collapsed from \$51 to \$0.0004 in 24 hours. There are many reasons for volatility, including these assets’ immaturity, decentralized trading and limited supply.

Mainstream currencies don’t fluctuate so much because central banks buy and sell currency to moderate swings. Other financial products such as options and futures also smooth price paths because these allow investors to hedge future risks. The introduction of these instruments for cryptocurrencies has not reduced volatility, however<sup>6</sup>. Cryptocurrency exchanges lack limits and rules to halt trading when prices rise or fall more than a set percentage over a period; such rules act as an emergency brake to slow price crashes or bubbles.

Researchers should study factors driving

cryptocurrency volatility and how to manage it. The relationship of cryptocurrencies to other assets in diverse investment portfolios needs attention, as does the impact of price volatility and policy uncertainty on Bitcoin<sup>7</sup>. Regulators should provide warnings about price swings to investors.

**Boost security.** Cash can be lost, credit cards stolen and bank fraud committed. Sometimes the holder is insured or compensated by an insurance scheme. But if the electronic keys to a cryptocurrency wallet are lost, there's no way to gain access and no central body to help users. Some estimates suggest that up to 25% of all bitcoins ever mined – hundreds of billions of dollars' worth – is irretrievable.

Virtual raids are common. For example, in 2014, the Japan-based bitcoin exchange Mt. Gox was hacked. At the time, it handled 70% of bitcoin trading; \$473 million dollars' worth of bitcoins were stolen.

Researchers need to explore how cryptocurrency can better withstand cyberattacks. State-run CBDCs should be more secure, but keeping them so will require effort. Exchanges should offer education around security on their platforms. More might require user identification.

**Manage fees.** Cryptocurrencies charge fees for transactions. The person making the transaction sets the amount and miners naturally want to work on those cryptocurrencies with the highest fees. Competition drives up these fees (varying from one cent to more than \$50) and fee spikes are common when many transactions are in the queue needing to be verified<sup>8</sup>. This typically happens when prices tumble and users try to offload coins, as happened with Bitcoin in early 2018.

Researchers need to examine how to control and smooth such spikes. They should set out guidelines on how users choose their fees. Miners should be encouraged through regulation and incentives to add transactions to the next block on the basis of the timestamp and not the fee.

**Educate users.** A 2021 study by the FCA found that 78% of UK consumers have heard of cryptocurrencies. Few know how they work. Around 10% understood wrongly that they had consumer protection for their crypto holdings, as they might for bank deposits. More than 40% relied on information from social media; ownership was concentrated in younger people. Most finance experts lack training in the intricacies of 'fintech'.

Universities have only recently started offering modules on cryptocurrencies and blockchain.

Media coverage tends to be negative – focused on lost wallets, criminality, volatility and energy use. Few merchants accept cryptocurrencies, leaving them as new instruments for speculators<sup>9</sup>. Businesses and educators should do more to improve customers' understanding and build trust.

**Protect privacy.** CBDCs come with a big privacy challenge, unlike decentralized cryptos. A move to a cashless society could allow governments to see all our transactions. Given growing interest from central banks, research is urgently needed on the willingness of individuals to trade privacy for convenience in their financial transactions<sup>10</sup>.

Baseline surveys would be a first step. China is already road testing its e-yuan. Since 2020, the People's Bank of China has been randomly gifting customers e-yuan, which they can use to purchase goods and services. A prepaid card and e-banking app was trialled in February at the Beijing Winter Olympics.

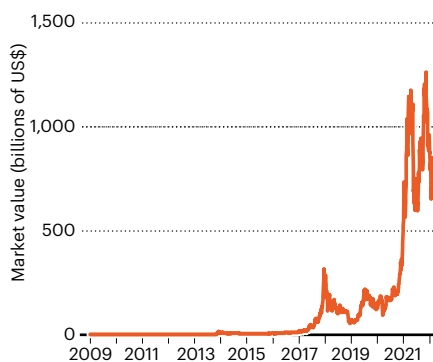
More work on all these aspects will help governments and the public decide what the future of money should look like.

## BITCOIN BALANCE SHEET

Since 2008, the cryptocurrency Bitcoin has blossomed into a virtual global currency. But steps still need to be taken to avoid price spikes and crashes and to lessen the computing power required.

### Trillion-dollar market

In 2021, El Salvador adopted Bitcoin as a parallel official currency.



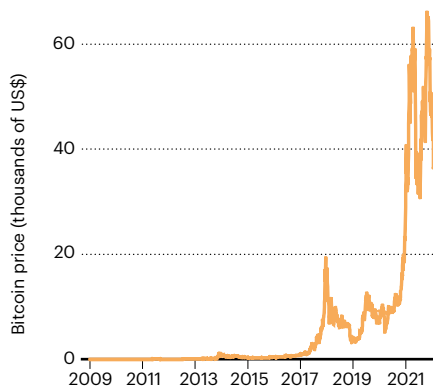
### Rising transactions

Bitcoin exchanges are slow and can take tens of minutes.



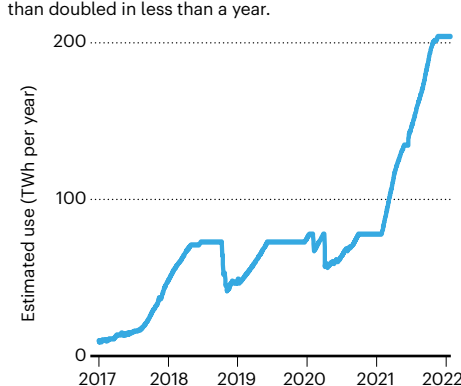
### Volatile prices

2021 saw price swings of 50–100%.



### High energy use

Bitcoin's carbon footprint has more than doubled in less than a year.



## The authors

**Andrew Urquhart** is professor of finance and financial technology at ICMA Centre, University of Reading, Henley Business School, Reading, UK. **Brian Lucey** is professor of international finance and commodities at Trinity Business School, Trinity College, Dublin, Ireland; Institute of Business Research, University of Economics, Ho Chi Minh City, Vietnam; and Institute for Industrial Economics, Jiangxi University of Economics and Finance, Nanchang, China. e-mails: a.j.urquhart@icmacentre.ac.uk; blucey@tcd.ie

1. Nakamoto, S. *Decentralized Business Rev.* 21260 (2008).
2. Corbet, S., Lucey, B., Urquhart, A. & Yarovaya, L. *Int. Rev. Finan. Anal.* **62**, 182–199 (2019).
3. Teichmann, F. M. J. & Falker, M.-C. *J. Money Laundering Control* **24**, 775–788 (2020).
4. Foley, S., Karlsten, J. R. & Putnins, T. J. *Rev. Finan. Stud.* **32**, 1798–1853 (2019).
5. Shen, D., Urquhart, A. & Wang, P. *Eur. Finan. Manage.* **26**, 1294–1323 (2020).
6. Corbet, S., Lucey, B., Peat, M. & Vigne, S. *Econ. Lett.* **172**, 23–27 (2018).
7. Lucey, B. M., Vigne, S. A., Yarovaya, L. & Wang, Y. *Finan. Res. Lett.* **45**, 102147 (2022).
8. Easley, D., O'Hara, M. & Basu, S. *J. Finan. Econ.* **134**, 91–109 (2019).
9. Baur, D. G., Hong, K. & Lee, A. D. *J. Int. Finan. Markets Inst. Money* **54**, 177–189 (2018).
10. Agur, I., Ari, A. & Dell'Ariccia, G. *J. Monet. Econ.* **125**, 62–79 (2022).

The authors declare no competing interests.