Crypto and digital currencies — nine research priorities

Article

Accepted Version

Urquhart, A. ORCID: https://orcid.org/0000-0001-8834-4243 and Lucey, B. (2022) Crypto and digital currencies — nine research priorities. Nature, 604 (7904). pp. 36-39. ISSN 0028-0836 doi: https://doi.org/10.1038/d41586-022-00927-5 Available at https://centaur.reading.ac.uk/104521/

Crypto and digital currencies – 9 research priorities

Researchers must advise governments and central banks how best to regulate this financial frontier to avert privacy breaches, scams and environmental damage.

Andrew Urquhart and Brian Lucey

Money 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, criminals can easily launder vast sums unseen, and whether the benefits of finance can be extended to the X billion people globally who lack access to banks.

Cryptocurrencies --- private monies that use encryption to perform and verify transactions --- have been around since Bitcoin was developed in 2008[1]. Now over 11,000 cryptocurrencies are in circulation, with a market value exceeding $2 trillion (Source: Coinmarketcap.com).

Institutional investors are accumulating them. MassMutual, JP Morgan, Paul Tudor Jones, Microstrategy and Tesla have all seen publicly in this market. Over 150 cryptocurrency hedge funds have sprung up to invest billions of dollars solely in these new assets. The financial system is also adapting with Bitcoin futures, options and exchange-traded funds (ETFs) are now available. Coinbase, the leading exchange, is listed on the New York Stock Exchange (NYSE).

Cryptocurrencies can perhaps hedge against inflation with the maximum supply of Bitcoin fixed at 21 million. Inflation fears are being stoked by the falling value of conventional currency. Governments and central banks have expanded the money supply to invigorate economies during the 2009 Global Financial Crisis and COVID-19 pandemic.

Cryptocurrencies can also offer the promise of 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 youthful president, Nayib Bukele, is an enthusiast who believes that cryptocurrencies can deepen financial inclusion and reduce economic dependence on the US. Last year, El Salvador deposited $30-worth of Bitcoin in each citizen's digital wallet, one tenth of the average monthly wage. Technical issues plagued the launch, however, including hacked accounts, verification difficulties, poor IT infrastructure and delays.

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. Bitcoin alone has a carbon footprint equal to Kuwait and an electricity footprint of Thailand, producing as much

electronic waste as the Netherlands (Source" Digiconomist.net). To get around this, El Salvador uses geothermal energy to decrypt its Bitcoin.

Lack of regulation worries bankers and policymakers. For all these reasons, China banned the mining of Bitcoin in July 2021. In January, the UK's Financial Conduct Authority (FCA) expressed concern over its inability to control cryptocurrency exchanges. The chair of the US Securities and Exchange Commission (SEC) warned that cryptocurrency platforms need regulation to survive.

In parallel, several economies including China and the European Union are developing other forms of digital assets over which they do have control. Central bank digital currencies (CBDCs) are an electronic record of the official currency, and might replace physical banknotes and coins within a decade **.** China is already testing a digital version of its Yuan/Renminbi, where customers can make payments over their mobile phones. In July 2021 the EU launched a digital Euro project to investigate feasibility of a digital Euro over the next 2 years. Later this year, the US Federal Reserve will release a discussion paper on a digital dollar.

Although the growth of research in this area has been substantial[2], research is urgently needed on 4 fronts: legality, scalability, usability and acceptability. All of these are interconnected; solutions in one area may exacerbate problems in another. Here we set out 9 priorities.

9 priorities

1. Curb criminality

The anonymity of cryptocurrency transactions appeals to criminals. Cryptos are used to launder money, fund terrorism and fuel corruption[3] with up to half of Bitcoin transactions may support illegal activities[4]. Solving this problem is nigh impossible --- cash has been used to conduct all the crimes for which cryptocurrency is blamed for. But options could be considered. Cryptocurrencies could monitor users and introduce 'know-your-customer' forms of authentication, a feature absent to now. But that would go against their privacy and ownership principles, lowering their uptake. Researchers need to examine such tradeoffs.

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

2. Regulate digital assets

Regulation around cryptocurrencies is fragmented. At one extreme, they are banned, as in China, Iraq and Egypt. At the other, they are mainstream, as in El Salvador. In the majority of

other countries, they are permitted yet not seen as legal tender. Trading is unregulated and they are treated as just another (lightly regulated) asset. Scams and mis-selling are rife.

Major global regulators such as the SEC in the US and FCA in the UK 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 throughout history. Economists speak of "graham's law" which is that bad (unsound, prone to inflate) money drives out good. Partially as a counter to this, such private monies were legislated and regulated out of existence..

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?

3. Minimize energy use

Cryptocurrencies are computationally intensive. Creating ('mining') some cryptocurrency's requires solving difficult cryptographic puzzles. Adding transactions to a digital ledger, such as the blockchain, demands verifications by algorithms. All those calculations consume energy. Bitcoin is more energy hungry than a medium-sized country like Norway. Processing one transaction consumes over $100 in electricity (Source: https://fortune.com/2021/10/26/bitcoin-electricity-consumption-carbon-footprin/) , and contributes 1 tonne of CO2 emissions. The next most popular cryptocurrency, Ethereum, consumes less energy but still adds 90kg of CO2 per transaction per submissions to the US Congress.

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 user 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), to 6.25 in 2022 for each block created. Lots of miners compete for the reward, hiking energy use.

Shifting to an alternative consensus process, Proof of Stake (PoS), could reduce energy consumption a million-fold. Miners compete instead based on holdings of the coin. The second largest cryptocurrency, Ethereum, is moving to PoW during 2022. But, regulation and taxing risk disincentivizing PoW 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 via regulatory or tax favouritism.

4. Speed up transactions

To replace existing systems of payment, cryptocurrencies will need to challenge commercial banking (such as SWIFT) and retail settlement systems. These process payments in seconds and handle quadrillions of dollars per annum. Bitcoin by contrast handles 250 thousand confirmed transactions per day, with a market value of $1-2billon (source: https://www.blockchain.com/charts/n-transactions) . Its transactions can take tens of minutes --- far too slow for global market needs. Researchers need to find ways to speed them up.

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

Volatility adds complications. In any monetary transaction, both sides want certainty in the value of an asset[4]. 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 way. 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, whilst the transactions are logged.

5. Manage volatility

Cryptocurrency prices can have massive swings[5]. In 2021 Bitcoin rose from $37k in January to $64k in April, falling back to $37k by July then rising again to $67k in November. In June 2021, a midsized coin (Iron Titatium) collapsed from $51 to $0.0004 in 24 hours. There are many reasons, including the assets' immaturity, decentralised trading and limited supply.

Mainstream currencies don't fluctuate so much because central banks buy and sell currency to moderate swings. Other financial products like options and futures also smooth price paths since these products allow investors to hedge future risks. The introduction of these instruments for cryptocurrencies has not reduced volatility[6] and cryptocurrency exchanges lack stop limits and halts in trading which halt trading when prices rise (or fall) more than a set percentage over a period, which act as emergency brakes 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 also needs attention. Regulators should provide warnings to investors about price swings.

6. Boost security

Cash can be lost, credit cards stolen and bank fraud committed. Sometimes the holder is insured or compensated by an insurance scheme. By contrast, 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 (https://www.cryptovantage.com/news/ask-cryptovantage-how-much-

bitcoin-has-been-lost-forever/) suggest that up to 25% of all Bitcoin ever mined, or hundreds of billions of dollars' worth, are irretrievably lost.

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 Bitcoin were stolen.

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

7. Manage fees

Cryptocurrencies charge fees for transactions. The user sets the amount and naturally want to work on those with the highest fees. Competition drives up these fees (varying from $0.01 up to over $50) and these fee spikes are common when many transactions are in the queue needing to be verified.[7] This happens when prices tumble and users are trying to offload Bitcoin like in early 2018 when the price of Bitcoin was plummeting.

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

8. Educate users

A 2021 study by the FCA found that 78% of UK consumers have heard of cryptocurrencies. Far fewer know how they work. Around 10% believed 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 and ownership proclivity was concentrated among younger ages Most finance experts lack training in the intricacies of 'fintech'. Universities have only recently started offering modules on cryptocurrencies and the blockchain.

Media coverage is off-putting. Stories tend to be negative, focused on lost wallets, criminality, volatility and energy use. Few merchants accept cryptocurrencies, leaving them as novel instruments for speculators[8]. Businesses and educators should do more to improve customers' understanding and build trust.

9. 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 off privacy for convenience in their financial transactions[9].

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 figure out what this brave new world of money will look like.

TEXT BOX

KEY TERMS

[Please can you pin down these definitions a little more but without introducing many more words; these should be very short (say 2 sentences each)]

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 are digital assets secured by cryptography. Many, including Bitcoin, use blockchain technology to store transactions.

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

Fiat currency is 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 printed with US dollar is one example.

Authors:

Professor Andrew Urquhart, Professor of Finance and Financial Technology, ICMA Centre, University of Reading, Henley Business School Whiteknights, Reading RG6 6BA, United Kingdom a.j.urquhart@icmacentre.ac.uk

Professor Brian Lucey, Professor of International Finance and Commodities, Trinity Business School, Trinity College, Dublin 2, Ireland; Institute of Business Research, University of Economics Ho Chi Minh City, 59C Nguyen Dinh Chieu, Ward 6, District 3, Ho Chi Minh City,

Vietnam; Institute for Industrial Economics, Jiangxi University of Economics and Finance, 169, East Shuanggang Road, Xialuo, Changbei District 330013 Nanchang, Jiangxi, China ; blucey@tcd.ie

[1] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

[2] Corbet, S., Lucey, B., Urquhart, A., Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis*, 62, 182-199.

[3] Teichmann, F. M. J., Falker, M.-C. (2020). Cryptocurrencies and financial crime: solutions from Liechtenstein. Journal of Money Laundering Control, 24, 775-788.

[4] Foley, S., J. R. Karlsen, and T. J. Putninš, (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies 32(5), 1798–1853.

[5] Shen, D., A. Urquhart, P. Wang, (2020). Forecasting the volatility of Bitcoin: The importance of jumps and structural breaks European Financial Management, 26, 1294-1323.

[6] Corbet, S., B. Lucey, M. Peat, and S. Vigne. (2018). Bitcoin futures—what use are they? Economics Letters 172, 23–27.

[7] Easley, D., O'Hara, M., Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. Journal of Financial Economics, 134, 91-109.

[8] Baur, D. G., K. Hong, and A. D. Lee (2018). Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money 54, 177–189.

[9] Agur, I., A. Ari, and G. Dell'Ariccia (2021). Designing central bank digital currencies. Journal of Monetary Economics .