UNIVERSITY OF CAMBRIDGE

Bennett Institute
for Public Policy
Cambridge

POLICY BRIEF

Crypto, web3, and the Metaverse

Sam Gilbert

March 2022

1. Introduction

This brief aims to give policymakers an overview of crypto's core concepts, and highlight some of the policy questions raised by its increasing adoption by citizens and organisations.

It begins with a short explanation of the crypto movement's ideological origins, offers basic primers in cryptocurrencies, blockchain, web3, NFTs, and the metaverse, and concludes with a discussion of the policy implications and suggestions for further reading. Short case studies and a glossary of crypto terminology (denoted by italics) are interspersed throughout. References are made by means of hyperlinks.

2. Ideological origins

The crypto movement originates in 1970s libertarian critiques of the state, which see central banks as illegitimate and government taxation as a protection racket. In the 1990s, the diffusion of digital technology gave rise to hopes among libertarians that the state's power over the individual could finally be transcended in cyberspace. Subsequent technical development of crypto has – at least in part – been an attempt to realise this vision of individual liberation from perceived state tyranny.

Two texts have been particularly influential: Neil Stephenson's novel *Snow Crash* (1992) and *The Sovereign Individual* (1997), a non-fiction book by James Davidson and William Rees-Mogg. Both these works imagine a future of extreme inequality in which nation-states have largely withered away. In their place, small, private city-states compete to attract the wealthiest and most talented individuals, who choose the jurisdiction with the mix of currencies, laws, and security arrangements that suits them best. In *Snow Crash*, those outside the self-sovereign elite spend much of their leisure time in a virtual world called the metaverse, which offers conditions that are more benign than reality.

It is common to hear echoes of these texts in the words of leading figures in the contemporary crypto movement, such as Balaji Srinivasan, Elon Musk, and Naval Ravikant. It would be wrong to assume that crypto technologies are inherently libertarian, or that all advocates of crypto share these ideological commitments. Nevertheless, crypto's origins help explain why ideas of radical decentralisation, disintermediation of institutions, and individual empowerment are held to be self-evident goods.

GLOSSARY

Fiat currency – conventional currencies such as USD or GBP, which are backed by government decree

Coin – a synonym for cryptocurrency

3. Cryptocurrencies primer

Cryptocurrencies were originally conceived as a replacement for the *fiat* currencies issued by central banks. However, actually existing cryptocurrencies do not fit most accepted definitions of currency or money. Too few things can be bought with them for them to be useful as a unit of exchange – at least in the formal economy. At the same time, they are too volatile to function as a store of value. As such cryptocurrencies are more accurately categorised as financial assets or securities, and are hence sometimes described by the label “crypto assets”.

The first and best-known cryptocurrency is Bitcoin (BTC). At the time of writing 1 Bitcoin is worth ~$42,000, and there are ~18.9m coins in circulation, implying a market capitalisation of ~$795bn. The total supply of Bitcoin cannot exceed 21m coins – a deflationary feature built in by its pseudonymous creator, Satoshi Nakamoto.

Bitcoin can be obtained by exchanging *fiat* currency at cryptocurrency exchanges like Coinbase and Binance and trading apps like eToro, or by *mining* it. Bitcoin mining involves solving computational puzzles. As the complexity of the puzzles increases, more and more computing power is required. Based on today’s prices, the value of Bitcoins still to be mined exceeds $88bn, creating strong economic incentives for mining. Bitcoin mining has become highly professionalised: miners use specialised *rigs* and routinely migrate to locations where electricity is cheapest, implicating Bitcoin in energy crises in places like Kazakhstan.

Why do people buy Bitcoin? As it operates outside the financial system and offers a degree of anonymity, Bitcoin is useful for illegal transactions (for example, purchasing drugs), and for laundering the proceeds of crime. It can also be useful for circumventing foreign exchange controls, and for hedging against hyperinflation and currency devaluations in emerging market economies. But for UK investors, the main non-criminal rationale for purchasing Bitcoin is to speculate on short-term movements in its price, or to buy-and-hold in the expectation of long-term appreciation (known in crypto parlance as *hodling*). While an estimated 114m people globally own Bitcoin, the majority of holdings by value belong to hedge funds and other professional investors.

GLOSSARY

Altcoin – a cryptocurrency other than Bitcoin

Memecoin – an altcoin derived from an internet meme, such as Dogecoin

Stable coin – a cryptocurrency whose value is pegged to one or more fiat currencies

Shitcoin – an altcoin of negligible value

Nocoiner – a rejector of cryptocurrencies

Mining – validating cryptocurrency transactions in exchange for cryptocurrency

Rigs – powerful computers used to mine cyptocurrencies

Hodling – holding cryptocurrency, usually in the context of adverse price movements

Wallet – a secure electronic repository for cryptocurrency and other crypto assets

The next largest cryptocurrency after Bitcoin is Ethereum ($377bn market cap). Importantly, Ethereum’s platform can be used to create new cryptocurrencies (see Blockchain Primer), which has led to a proliferation of *altcoins*, including Dogecoin ($20bn market cap). The use-cases for altcoins are identical to Bitcoin. *Stable coins* are a subcategory of cryptocurrencies which are pegged to fiat currencies (typically the US Dollar), and exist to offer investors a haven from market volatility and facilitate the exchange of cryptocurrencies back into fiat currency. The best-known stable coin is Tether ($78bn market cap), which has drawn regulatory attention due to its low dollar reserves (see Policy Implications).

Cryptocurrencies are held in cryptographically-secured electronic repositories called *wallets*. Nevertheless, the trade in cryptocurrencies is prone to scams, fraud, and market manipulation (see Table 1).

Table 1: Varieties of crypto scam

Type	Description	Example
Rug pull	The originators of a crypto project take the capital raised from a token sale and disappear	In January 2022, the creators of the Big Daddy Ape Club NFT collection took $1.3m in payments from investors but provided no NFTs in return
Pump-and-dump	A particular crypto asset is hyped – typically in group chats for crypto speculators on Telegram or Discord – leading to a short-term spike in the asset's price as buy orders flood in. The instigators then sell off their holdings, triggering a crash, with other investors left "holding the bag".	In November 2021, the creators of Squid Coin, an altcoin based on the Netflix series Squid Game, sold their holdings for $3.3m and abandoned the project
Wash trading	Artificially inflating the price of a crypto asset by repeatedly trading it between wallets controlled by the same individual or group	Almost 90% of the reported $9.5 billion worth of trading through the NFT marketplace LooksRare appears to be wash trading.
Ponzi scheme	Capital from later investors in a crypto asset is used to pay returns to earlier investors	In 2018, investors in the cryptocurrency Bitconnect lost a total of > $2 billion when it collapsed
Hacking	Protocols or wallets are hacked and owners' crypto assets stolen	Hacks exploiting smart contract issues in the DeFi protocol Cream Finance totalled $148m in 2021
Phishing	Attackers use social engineering techniques to trick a target into revealing information that can be used to gain access to their crypto assets	In December 2021, digital art collector Todd Kramer had 15 NFTs, valued at $2.2m, stolen from his wallet following a phishing attack

4. Blockchain primer

Blockchain is a distributed database technology. Rather than being stored on a particular machine (for example, on a cloud server belonging to Amazon Web Services), blockchain data is distributed across a network of machines. The individual machines in the network are referred to as *nodes*.

Advocates of blockchain claim it offers three key benefits over conventional database technologies:

- Decentralisation – there is no single point of failure and no reliance on a trusted central authority to validate transactions (hence blockchain is sometimes described as "trustless")
- Immutability – once written to the blockchain, transactions cannot be undone or altered
- Transparency – all transactions are a matter of public record

However, blockchain is slow and energy-intensive compared to conventional database technologies. This is a function of the *consensus mechanisms* used to update the database, which involve multiple nodes in the network validating each new transaction.

There are two types of consensus mechanism: *proof-of-work* and *proof-of-stake*. Bitcoin mining is an example of a proof-of-work mechanism, in which nodes compete for the right to add a transaction to the blockchain, with the winner receiving a reward in cryptocurrency (see Cryptocurrencies Primer). Proof-of-stake mechanisms simply reward nodes in proportion to their existing cryptocurrency holdings, meaning that they use less energy than proof-of-work mechanisms.

While it was invented to support Bitcoin and continues to support all cryptocurrencies, blockchain can also be used for other purposes, typically in conjunction with *smart contracts* – contracts programmed in computer code, that can self-execute based on predetermined triggers.

Smart contracts are said to be important because they remove the need for trusted intermediaries such as lawyers, banks, and brokers, paving the way for peer-to-peer transactions. However, the corollary is that transacting parties must be capable of reading the smart contract code themselves: if bugs or fraudulent features in the code result in losses, they have no recourse. Malicious smart contracts are the means by which many crypto frauds and scams are perpetrated.

GLOSSARY

Block – groups of transactions, which, when "chained" together, constitute a blockchain

Node – one of the individual machines in the network used to validate transactions before they are appended to the blockchain

Consensus mechanism – the means of validating blockchain transactions via consensus among the nodes

Proof-of-work – a consensus mechanism where nodes compete to solve complex computational puzzles, incentivised by a reward paid in cryptocurrency

Proof-of-stake – a consensus mechanism where nodes are rewarded proportionate to their cryptocurrency holdings

Hash rate – in the context of proof-of-work, a measure of the computing performance – either of a nodes, or of the whole validator network

Smart contract – a self-executing contract, written in computer code

Gas – fees payable by parties transacting on the Ethereum blockchain

Many real-life uses of blockchain involve Ethereum. In addition to issuing its own cryptocurrency, Ethereum operates an open-source platform which makes it easy for software developers to create:

- dApps – distributed applications running on blockchain

- Protocols – sets of standardised rules determining how different categories of applications should operate
- Distributed autonomous organisations (DAOs) – an organisational form governed by smart contracts rather than a central authority, which some see as a digital successor to co-operatives and trade unions

Access to the Ethereum platform has resulted in a proliferation of blockchain-based projects (see web3 Primer).

5. web3 primer

The term *web3* refers to the putative next generation of the web's technical, legal, and payments infrastructure – including blockchain, smart contracts and cryptocurrencies. For its advocates, the peer-to-peer character of web3 means it represents a more equitable vision for the web than its current iteration, Web 2.0, which is dominated by powerful intermediary platforms (Facebook, Amazon, Apple, Google and other big tech companies).

However, some cryptocurrency advocates – notably Jack Dorsey – believe web3 is simply a narrative invented by opportunistic venture capital investors, whose profit motives are incompatible with the political project of radical decentralisation (see Ideological Origins).

Most existing web3 projects fit into one of three categories:

- Decentralised Finance or *DeFi* – peer-to-peer, blockchain-based financial services including savings, borrowing, payments, and credit-scoring. Many (although not all) DeFi apps run on Ethereum.
- Digital Services – decentralised internet service provision, cloud storage, web infrastructure, data analytics, and identity management
- Collectibles – digital artwork, sports memorabilia, and virtual goods

Current examples of web3 unicorns (companies valued at > $1bn) include:

- Ripple, an international payments provider
- Aave, a protocol for borrowing and lending crypto assets that runs on Ethereum
- Chainalysis, a data analytics platform for compliance, risk management, and cybercrime investigations
- Forte, a gaming infrastructure platform
- OpenSea, a digital collectibles marketplace
- Sorare, an Ethereum-based fantasy football game in which virtual player cards can be bought and traded

WEB3 SLANG

gm / gn – stand for "good morning" / "good night"

wagmi / ngmi – stand for "we are all going to make it" / "not going to make it", expressing respectively optimism or pessimism about the future

FUD – people who are critical of web3 may be accused by its advocates of spreading "Fear, Uncertainty, and Doubt"

hfsp – stands for "have fun staying poor"; typically levelled at someone thought to be spreading FUD

The web3 community is to be found in group chats (known as *servers*) on the messaging platform Discord, and on Twitter, where members can often be recognised by one or more of:

- Hexagonal profile pictures
- Profile names with ".eth" extensions (referring to the Ethereum equivalent of domain names)
- Use of web3 slang

Capital for new web3 projects is typically raised not by selling equity, but by selling *tokens* to prospective users of the product or service, and/or to financial investors who believe the value of the tokens will rise in future. The process is known as an *initial coin offering, token-generating event*, or simply *token sale*. A proportion of the tokens is usually reserved by the founding team so they continue to have a stake in the project, and can incentivise staff and contributors (similar to share options in conventional startups).

There are several different types of token, including:

- Utility tokens, which grant rights of access to a product or service
- Governance tokens, which grant voting rights on decisions

web3 UK case study: Pool

Founded in 2021 and based in London, Pool is building technical infrastructure for data unions – organisations allowing groups of individuals to be directly compensated when data about them is used for digital advertising or other commercial purposes. To date, Pool has raised $3.7m to build its product through sales of Ethereum-based $POOL tokens.

According to Co-Founder & CEO Shiv Malik, there are several advantages to Pool being structured as a web3 project.

Firstly, the amount payable to an individual when data about them is used is typically a small fraction of a penny. Tokenisation overcomes this operational problem by enabling micropayments to individual data union members.

Secondly, tokens can be used to democratise the governance of Pool's platform. Enabling token holders to vote on key decisions should mean that the interests of the platform's users (data unions and their members) are not secondary to the interests of the organisation's board and executive management – a common criticism of Web 2.0 platforms.

Thirdly, issuing tokens rather than equity makes the process of raising startup capital easier, as investors benefit from greater liquidity – they are able to sell their tokens in the secondary market more or less immediately, rather than having to wait for a subsequent investment round or IPO.

Malik adds: "Issuing tokens also allows for the equity in the company to remain protected. This is important to our current and future stakeholders because we need to protect the ownership of the IP we are creating to stop any potential buyout by big tech now and in the future. It's like Ulysses tying himself to the mast. At the same time, those tokens allow stakeholders to benefit in the increased value they are helping to generate."

- Non-fungible tokens (NFTs), which grant ownership rights over unique items of digital property, such as imagery, videos, and audio files

All such tokens are financial assets which can be traded in secondary markets. They are therefore more liquid and more volatile than startup equity or options, and can be used for the same forms of financial speculation as cryptocurrencies. Some consumer brands have financialised their loyalty programmes through token sales, notably a number of Premier League football clubs (in partnership with the web3 company Socios).

6. NFTs primer

NFTs have played a key role in building mainstream consumer awareness of web3. NFTs of digital artworks such as Beeple's *Everydays – The First 5000* Days, collectibles such as Bored Ape Yacht Club avatars, and parcels of virtual land have sold for millions of dollars, both through traditional auction houses and on web3 marketplaces like OpenSea.

Like cryptocurrencies, NFTs are held in wallets. Technically, an NFT is not the digital file itself, but a database entry on the blockchain that attributes ownership to a particular wallet.

GLOSSARY

Drop – the release of a collection as NFTs

Minting – the process of creating an NFT for a digital file on the blockchain

Air drop – the distribution of an NFT or other token to a wallet for free

The provable scarcity of individual NFTs means they can function as digital status symbols, helping to explain why they are sometimes compared to Rolex watches and Lamborghini sports cars. Various consumer brands, including Coca Cola, Nike, and McDonalds, have sought to capitalise on the craze by issuing (or *dropping*) their own NFT ranges, as have football clubs such as Manchester City and Glasgow Rangers.

Celebrity endorsements are a common means of promoting high-profile NFT projects. Some wealthy celebrities like Reese Witherspoon and John Terry appear to be enthusiastic collectors, while others including Paris Hilton and Floyd Mayweather seem to engage with them in a more straightforwardly transactional way.

However, not all NFT drops are extravagantly priced or associated with a well-known brand or celebrity (see, for example, The Pluto People or the case study on Les Éléfants Terribles). NFTs are said to offer digital artists a new way of selling their work directly to the public, without having to pay commission to agents or galleries, as well as the potential to earn ongoing royalties from future sales of their work in the secondary market. The same benefits are said to be available to musicians and creators of video content, whose products (respectively audio and video files) can also be represented by NFTs.

NFT case study: Les Éléfants Terribles

Les Éléfants Terribles is a digital art collection co-created by the London-based artist and illustrator Guillaume Cornet. It consists of 2,754 images of elephants, programmatically-generated from 373 hand drawings of references to “enfant terribles” from the worlds of literature, art, fashion, and music.

The images were minted as NFTs on the Tezos blockchain, which is seen by many digital artists as an energy-efficient alternative to Ethereum because of its proof-of-stake consensus mechanism (see Blockchain Primer).

In common with many NFT projects, Les Éléfants Terribles conceives of its owners as a community and offers them additional benefits. There is a dedicated Discord server, and rewards (in the form of new limited-edition artworks) are randomly distributed to owners through regular *air drops*.

Cornet previously sold work through commercial galleries, but he sees much greater earning potential in minting artworks as NFTs – not least because they can easily be sold without the need to pay the high commission rates galleries typically charge. In the secondary market, the floor price for an Éléfant Terrible is currently 22 XTZ (~$85).

There are, however, significant barriers created by current UK taxation rules and UK banks’ interpretation of anti-money laundering regulations. According to Cornet, the proceeds of his NFT sales are treated as ordinary income, giving rise to an immediate tax liability in GBP, calculated using the XTZ:GBP exchange rate at the time of the transaction. At the same time, banks will not accept payments into business accounts from cryptocurrency exchanges. He is therefore more exposed to exchange rate volatility, and less able to manage his business's tax position and cashflow than with conventional sales in fiat currencies. In addition to the financial costs, Cornet says this is a major cause of occupational stress among digital artists.

Meanwhile, establishing NFT marketplaces as DAOs (see Blockchain Primer) has been proposed as a means of pre-empting the emergence of a new generation of dominant intermediaries – the web3 successors to Spotify, Youtube, TikTok et al. The idea is that creators would have the opportunity to co-own the platforms through which their work is traded, and to determine their decision-making via governance tokens.

As with cryptocurrencies, NFT prices can be volatile, while trade in NFTs is prone to fraud and market manipulation. When NFTs are initially issued (or *minted*), the underpinning smart contract may be designed to siphon cryptocurrencies and other tokens from buyers’ wallets. Meanwhile, prices in the secondary market can be artificially inflated by wash-trading – that is, the trading of an NFT between wallets controlled by the same individual or group. The pseudonymity offered by the web3 facilitates both practices.

7. Metaverse primer

The term *metaverse* refers to the open, persistent, real-time, interoperable, virtual world that could be built using web3 technologies. NFTs, blockchain, smart contracts, and cryptocurrencies are said to provide the payments and legal infrastructure needed to complement virtual reality (VR) capabilities, meaning that the vision presented in *Snow Crash* – or more optimistically, *Ready Player One* – can be realised.

However, it is important to note that the metaverse does not yet exist. Mark Zuckerberg's presentation on the metaverse at the 2021 Connect conference and the re-branding of Facebook, Inc. to Meta Platforms, Inc. have encouraged commentators to describe existing VR applications – including those available through Meta's Oculus headsets – as manifestations of the metaverse. This is incorrect, as such applications are neither persistent (because they reset when users quit them), nor interoperable (because they are siloed and it is not possible to move seamlessly between them). So, unlike the other concepts and technologies described in this paper, the metaverse can only be discussed in terms of its potential.

While widespread participation in the metaverse may seem implausible to some, the scale achieved by massively multiplayer online games (MMOs) such as Fortnite, Call of Duty, and Minecraft hints at the potential. More than a billion people regularly play MMOs, with an estimated $93 billion of economic activity happening inside them each year, in electronic currencies native to each game (for example, Fornite's in-game currency is called V-Bucks).

The main driver of these virtual economies is the sale of "skins" – virtual goods which allow players to change their in-game appearance. It is claimed that the interoperability of MMOs in the metaverse, the replacement of in-game currencies with cryptocurrencies, and the minting of skins as NFTs, would lead to significant growth in the market for virtual goods. Skins could supposedly be taken from one game to another; sold, rented or gifted to other players; used as collateral; and so on.

The blockchain-based game Axie Infinity, offers a glimpse of the opportunities and risks that might be created by the development of a metaverse economy. Operating on a pay-to-play-to-earn model, Axie Infinity requires an up-front investment of ~$1,000, but rewards play with an Ethereum-based in-game token, which can be spent on NFTs of virtual assets, or exchanged for fiat currency. The majority of players live in The Philippines, where some rely on it as their main source of income. The sustainability of such income depends on the willingness of more affluent players to continue making in-game purchases with fiat currencies, which some have argued amounts to the reproduction of colonial power relations.

Beyond gaming, the metaverse promises experiences of remote work and socialising which improve on what is currently possible with software like Zoom, Slack, Miro, and Microsoft Teams. Assuming conditions of pandemic and the goal of Net Zero continue to reduce long-distance travel significantly, remote interactions are set to remain a fact of life. It is at least plausible that they could benefit significantly from taking place in the metaverse – imagine, for example, visiting a geographically-distant family member in a virtual representation of their real home, rather than seeing them on Zoom. VR treatments have also been shown to alleviate chronic pain, PTSD, and phobias, suggesting that the metaverse may eventually have clinical applications.

8. Policy implications

In the UK, crypto regulation is already in progress. What follows is a non-exhaustive list of outstanding policy questions raised by recent developments in cryptocurrencies, blockchain, web3, NFTs, and the metaverse. In some cases, the contours of possible policy responses to the different risks and opportunities are sketched out.

Anti-money laundering

The risk of money laundering through cryptocurrencies is well understood; the way in which this is exacerbated by the DAO form perhaps less so. Cryptocurrency exchanges which are structured as DAOs such as the popular Uniswap DeFi protocol do not – and in fact are technically unable to – perform KYC checks.

Business and innovation

web3 presents opportunities as well as risks. Adapted versions of the Seed Enterprise Investment Scheme (SEIS), Enterprise Investment Scheme (EIS), and Enterprise Management Incentives scheme (EMI) may merit consideration as a means of increasing the supply of capital and talent available to early-stage web3 ventures. Encouraging DeFi projects to apply for the FCA's Regulatory Sandbox might help the UK consolidate its position as a global fintech centre. Meanwhile artists, musicians, and video content creators would benefit from clearer guidance on and revisions to the tax treatment of NFTs.

Central Bank Digital Currencies (CBDCs)

CBDCs are digital versions of bank notes, which can be used for retail and wholesale payments. As such, they can be seen as competitors to cryptocurrencies. Nigeria and The Bahamas have launched CBDCs, and a number of other countries are piloting them – including China and Sweden. Meanwhile, the Bank of England is advancing with its own exploration of a CBDC.

The rationale is twofold. Firstly, if the money system were to become fully digitalised, CBDCs would be needed to ensure that citizens retained access to fiat currencies. Otherwise, they would have no alternative to cryptocurrencies, and would therefore be exposed to the risks described earlier in this brief. Secondly, CBDCs have the potential to make cross-border payments faster and cheaper, and to improve the effectiveness of certain monetary policies. For example, a central bank could issue financial stimulus payments in a CBDC designed to devalue quickly, encouraging recipients to spend stimulus funds immediately rather than saving them.

Climate

Proof-of-work consensus mechanisms have a significant carbon footprint, with Bitcoin now consuming more energy than Sweden. When Bitcoin's price rises, it creates incentives to expend more energy on mining. The expansion of any systems relying on proof-of-work is therefore clearly in tension with Net Zero goals (in addition to accentuating energy security risks). Ethereum plans to move from proof-of-work to the less wasteful proof-of-stake mechanism, but for now, there is a significant environmental externality to the majority of web3 projects by virtue of their dependency on Ethereum.

Competition

Proof-of-stake consensus mechanisms are less environmentally damaging, but as they operate on the Matthew Principle they also compound inequalities. The market participants with the largest existing holdings are able to stake the most tokens – they therefore receive the largest block rewards, meaning their holdings grow at a faster rate. Proof-of-stake-based blockchains therefore tend towards oligopoly: the dominant nodes in the network end up with the power to change protocols in a way that is detrimental to the interests of other participants (for example, by raising prices). In this scenario, anti-trust would not be an effective policy lever, as there would be no organisational entity that could be held to account.

Another area of focus for competition policymakers should be the rise of new intermediary platforms with gatekeeping power. Running counter to the decentralising ideals of the crypto movement is increasing demand from consumers for trusted intermediaries who can perform useful market functions like verifying that smart contracts are bona fide, freezing misappropriated crypto assets, or reversing accidental transactions. The more mainstream cryptocurrencies and NFTs become, the greater this demand will be. In the context of the worldwide web and Web 2.0, similar dynamics produced dominant intermediaries like Spotify and the App Store. It therefore seems likely that web3 markets will develop in the same way – for example, OpenSea may emerge as the dominant intermediary for NFT sales.

Consumer protection

The accessibility of trading apps and cryptocurrency exchanges mean the entry barriers for consumers to crypto investing are very low. At the same time, the level of technical understanding required to read and understand smart contracts is very high. Together with celebrity endorsements of NFTs, above-the-line advertising campaigns for cryptocurrencies, and commercial partnerships between web3 firms and football clubs, this creates the conditions for widespread financial mis-selling. Compounding this risk is the prevalence of fraud – globally some $14 billion was lost to crypto scams in 2021 – and the potential for the collapse of Tether to result in systemic failure and large losses for holders of cryptocurrencies.

In the UK, HM Treasury has recently brought advertisements for crypto assets within the scope of the Financial Conduct Authority's financial promotion rules. Meanwhile, regulatory proposals by the European Commission (EC) would require exchanges to comply with standards designed to protect consumers from losses arising from cyberattacks, fraud, and technical malfunctions. The same proposals would also require web3 projects wishing to raise capital through token sales to incorporate, and to submit their white papers to regulators. Modest entry barriers like these might disincentivise some fraudulent projects and help identify serial scammers.

A possible additional mitigation would be to require trading apps and exchanges to implement questionnaires designed to test a customer's financial sophistication before allowing them to invest in crypto (as with equity crowdfunding platforms). When it comes to web3 projects, there is also scope to go further than the EC proposals by requiring white papers to explain to potential investors the distribution and vesting schedule of tokens. In both cases, the trade-off would be eroding the advantage tokens have over equity as a means of raising capital for new ventures.

Cybersecurity

The existence of cryptocurrencies is an enabler of ransomware attacks, in that they make it much easier for attackers to receive large payments without revealing their identity. Ransomware attacks cost $11.5bn in 2019, with a $1.9m average cost of recovery for each organisation affected. Recent examples of UK organisations affected by ransomware attacks include NHS England, Redcar and Cleveland Borough Council, and KP Snacks.

Financial stability

The scale and growth rate of the crypto asset market ($2.3 trillion, +200% in 2021) is sufficient to pose a risk to the overall stability of the financial system, with the potential for knock-on effects to damage the real economy.

As there is material institutional investment in crypto – not least from hedge funds with leveraged positions – a severe market correction could result in a sell-off of other assets to meet margin calls. This would have adverse consequences for the amount of liquidity in the financial systems and could result in contagion if general investor sentiment was affected. The risk will be compounded if the crypto derivatives market continues to grow.

Online safety

The immutability of the blockchain might mean instances of revenge porn and doxxing (maliciously publishing information that identifies an individual so as to facilitate harassment) become indelible. The ability to air drop NFTs into crypto wallets could be used malevolently to give ownership of illegal imagery or video to individuals against their wishes. In such cases, the individuals would only be able to remove the files by sending them on to a different wallet. Meanwhile, VR environments bring with them new dimensions to online harms like cyberbullying and sexual harassment.

It seems likely that forthcoming online safety legislation will soon need to be updated to mitigate these risks. Furthermore, the decentralised nature of web3 may mean that the threat of sanctions against big tech companies will lose its effectiveness as a policy lever.

9. Concluding remarks

There is no shortage of writing about the topics discussed in this policy brief; the trouble is that it tends towards boosterism on the one hand, and polemic on the other. My aim has therefore been to provide as balanced and objective an overview as possible. However, I am going to set aside that detachment in these concluding remarks.

I do not think policymakers need to concern themselves unduly with speculation in crypto assets by institutional investors and sophisticated retail investors. It seems likely that the reported size of the market is inflated by wash trading, which would lessen the magnitude of risks to overall financial stability. Publicity around criminals' difficulty laundering and spending large amounts of cryptocurrency seems likely to have a deterrent effect on ransomware attacks and scams. Meanwhile, an intervention which triggered a sharp fall in crypto asset prices might damage the legitimacy of regulatory authorities. Provided taxes can be collected and anti-money laundering rules enforced, these sections of the market can probably be left to manage themselves – at least for now.

By contrast, there is a clear and present danger that consumers will suffer serious losses from the mis-selling of crypto assets, at a scale comparable to secured loans in the 2000s or payday loans in the 2010s. When it comes to cryptocurrency investments and initial coin offerings, advertising campaigns, sponsorship deals with consumer brands, and celebrity social media promotions should be regulated assertively. Entry barriers to investment in cryptocurrencies should be heightened by requiring exchanges (eg Coinbase) and trading apps (eg eToro) to undertake more due diligence on their customers' means and financial sophistication before allowing them to invest. This would in turn raise the entry barriers to DeFi, since cryptocurrency holdings are of course a dependency for participation. Meanwhile, the tokenisation of fan loyalty programmes (eg Socios) and esports (eg Sorare) should be investigated to determine the materiality of consumers' exposure to market volatility.

The risks presented to consumers by NFTs seem to me to be less acute. In contrast to cryptocurrencies, buyers of NFTs receive an object in return, which may give them pleasure regardless of future fluctuations in its market value. In this way, the NFT market has more in common with markets for real-world collectibles like wine, stamps, and fine art than with financial services, and therefore in my opinion does not demand such a robust approach.

The new opportunities tokenisation offers startups and digital artists should not be dismissed out of hand. Tax policy (eg SEIS, R&D tax credits) have played an important role in the successes of the wider UK tech sector over the past ten years, and could likewise help the nascent web3 sector develop. The same goes for the growth potential of the virtual economy, which could see the UK's video gaming sector become a bigger source of jobs and corporation tax revenues – with or without the emergence of a fully-fledged metaverse.

Finally, I think the benefits of decentralisation and disintermediation have been overemphasised. While some market intermediaries are extractive rentiers, many others play value-adding governance roles that cannot be replicated with smart contract code. For example, I suspect few ordinary consumers would regard a bank without a customer services department, or an online marketplace without the ability to escalate a dispute to a human decision-maker as an improvement on the status quo – even if they offered much better prices. For this reason, I expect trusted central authorities to remain a feature of the web. If that is correct, as most of the opportunities described in this brief are not technically dependent on a decentralised solution, it may be possible to realise them without the blockchain's negative externalities.

10. Further reading

Folding Ideas, "Line Goes Up – The Problem With NFTs" (January 2022) [Video]

David Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism*, University of Minnesota Press (2016)

The Crypto Syllabus, "Basics" and "Politics"

The Dig, "Cryptocurrency w/ Edward Ongweso Jr & Jacob Silverman" and "Private Money with Stefan Eich" (December 2021) [Podcast Episodes]

Li Jin, Scott Duke Kominers, and Lila Shroff, "A Labor Movement for the Platform Economy", Harvard Business Review (September 2021)

Joey D'Urso, "Socios 'fan tokens' – what they really are and how they work" and "Sorare: 'An unregulated timebomb' or a fantasy game that will revolutionise football?", The Athletic (2021)

Matthew Ball, "The Metaverse: What It Is, Where to Find it, and Who Will Build It" (January 2021)

a16z, web3 Policy Handbook (October 2021)

11. About the author

Sam Gilbert is an affiliated researcher at the Bennett Institute for Public Policy and the author of *Good Data: An Optimist's Guide to Our Digital Future*. He was previously Employee No.1 and Chief Marketing Officer at the fintech unicorn Bought By Many, and held senior roles at Experian and Santander.

Disclosure: at the time of writing, he is not an investor in any of the crypto assets mentioned in this policy brief.

12. Acknowledgements

The author would like to thank the following people for helpful conversations and feedback during the development of this brief: Charlie Beer, Guillaume Cornet, Professor Diane Coyle, Tony Gjerlufsen, Shiv Malik, and Sofie Stenbøg.

UNIVERSITY OF
CAMBRIDGE

www.bennettinstitute.cam.ac.uk

Bennett Institute
for Public Policy
Cambridge