

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

The Metaverse: Economic and Social Values and Risks of new Cryptocurrencies and Blockchain Technologies

Dr Petar Radanliev

Department of Engineering Science, University of Oxford, United Kingdom: petar.radanliev@eng.ox.ac.uk

Abstract: The aim of the article is to present a snapshot in time, of the current state in cryptocurrencies, the values and risks associated to blockchains. With emergence of over 20,000 crypto projects, the first objective of this article is to present the stage as it is in 2023, with historical overview since Satoshi presented the first paper on decentralised blockchains, until today. Second objective of the article is to review the values and risks associated to cryptocurrencies, and to clarify the differences between cryptocurrencies from blockchain technologies. The research questions that drive this article are related determining if the blockchain technology an innovation or its already obsolete technology? Are there any significant risks from cryptocurrencies? And are the potential values to society and economy worth pursuing? Would developed or developing countries benefit more from these technologies? And which blockchain projects will survive in the long run? In other words, where is the money and is there money or just hype. The review discusses the high probability that some crypto projects will fail, and given the vast number of cryptos, the article acknowledges that many of these projects are nothing more than ponzi's. These are discussed and acknowledged, then the focus is shifted to the real-world use cases of blockchain projects.

Keywords: Blockchain Technologies; Cryptocurrencies; Risk; Value.

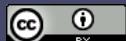
1. Introduction

Cryptocurrencies are digital assets used as virtual currencies, based on cryptography for security and privacy, and often decentralised. The main characteristic of a cryptocurrency (crypto) is that they cannot be controlled by governments, or institutions, but this is debatable, because if one government (e.g., USA) or one institution (e.g., Black Rock) decides to take controlling stake in a crypto, this characteristic can be deceitful. The most popular crypto is Bitcoin, but there are many other cryptos. Crypto can be used to purchase goods or services, and can be traded on many online platforms, but none of these platforms is fully regulated. This opens an opportunity for countries like the UK, that are looking to find their place in the international stage, especially after the recent setbacks from Covid and Brexit. One argument for pursuing this solution is '*that the main indicators to improve financial development should enhance the process of bank lending and equity market development*' [3] Second argument is that smart contracts and metaheuristic can help with securing the quality-of-service and even help with the '*cost-efficient scheduling of medical-data processing*' [4], which seems of crucial importance for the medical systems in the UK – after the Covid shock to the NHS [5]–[7].

1.1. Brief History of Cryptocurrencies

Cryptocurrencies (crypto) are digital assets, or more precisely a set of digital currencies that emerged with the release of Bitcoin in 2009¹. As of January 2021, there are over 4,000 in circulation, some cryptos with very little trading volume (or not at all). Cryptocurrencies are traded as digital 'tokens' or 'coins' that exist on a distributed and decentralised ledger. Bitcoin leads on market capitalisation, but other cryptos are trying to break

¹ <https://bitcoin.org/en/>



in the market by providing different and improved services to Bitcoin. Some of the other cryptos - also known as 'altcoins' i.e., all cryptocurrencies other than Bitcoin – are used to create a decentralised financial system e.g., Ethereum², with the ability to handle more transactions e.g., Dogecoin³, or just use different consensus algorithms e.g., Cardano⁴. Cryptocurrencies remain highly volatile, and without a central control a single statement by Elon Musk has been sufficient to trigger a spike in interest in search trends (as seen in **Error! Reference source not found.**), and to attract a significant interest in news media.

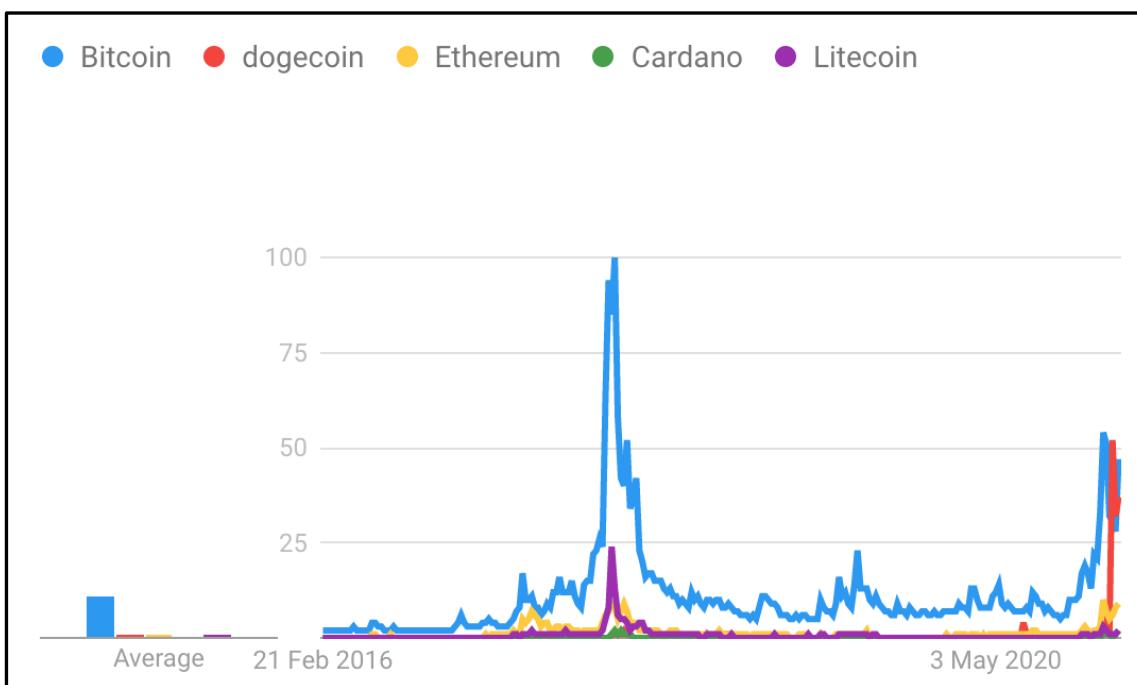


Figure 1. Comparison of search trends on some of the most popular cryptos (data from 2020 – before the last major bull run in crypto).

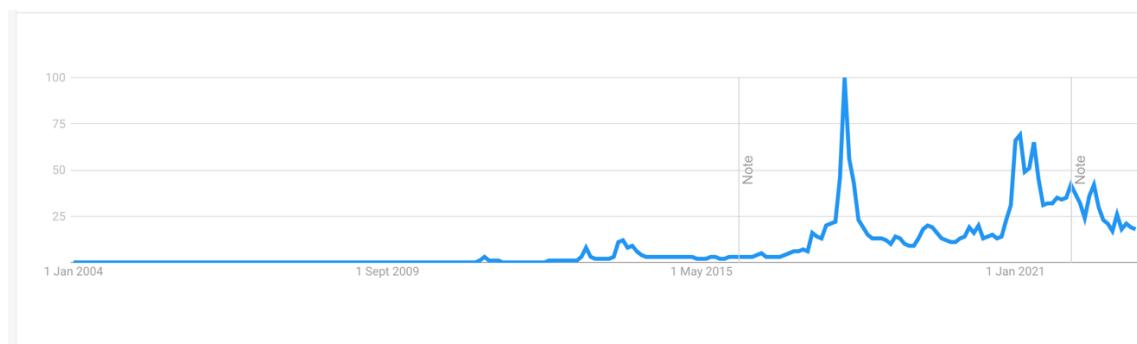
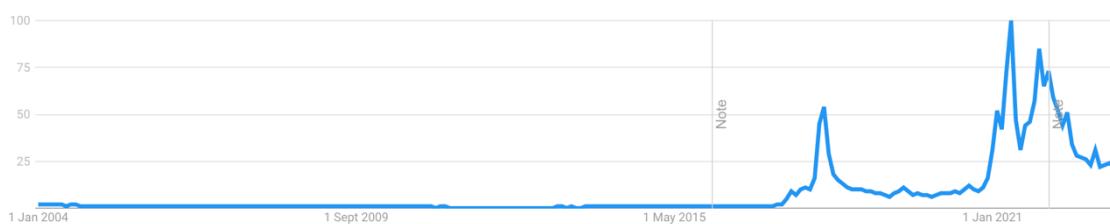
Although the search trends can spike about specific cryptos i.e., Bitcoin and Dogecoin in **Error! Reference source not found.**, a dynamic equicorrelation [8] shows a contagious correlation (a mutual relationship or connection) effect between cryptocurrencies (i.e., when Bitcoin crashes, altcoins follow), and the same effect is also related between Bitcoin and NASDAQ. This disincentivises diversification into multiple cryptocurrencies, but a more robust analysis with a value-at-risk and expected shortfall need to be computed to confirm this. Looking at the spikes in search trends after the announcement from Elon Musk on Bitcoin purchase and comparing them to the price cap of Bitcoin and Dogecoin, it almost resembles a certain behaviour in crypto markets. The user behaviour in some crypto (e.g., Ethereum) appears more stable, while the behaviour of users in Bitcoin appears more speculative, with fluctuations based on market trends, followed by larger sell out when market is down [9]. This is not to say that influential people cannot manipulate the stock market, but the point here is that stock market investors are protected by regulations, which don't yet exist in crypto markets.

In **Error! Reference source not found.** we can clearly see that 'interest over time' has changed for Bitcoin and Cryptocurrencies in general – including Altcoins. While the interest in Google Trends for Bitcoin has reached its peak in the 2018 bull run, the interest in cryptocurrencies as a search trend, has increased (to a new 100%) in the 2021 bull run.

² <https://ethereum.org/en/>

³ <https://dogecoin.com/>

⁴ <https://cardano.org/>

Bitcoin: Interest over time – 1st of January 2004 until 7th of March 2023Cryptocurrencies: Interest over time – 1st of January 2004 until 7th of March 2023**Figure 2.** Interest over time: Bitcoin vs Cryptocurrencies (including Altcoins).

Crypto users can be categorised according to their actions and resources e.g., fortune hunter, idealist [10], but the bigger question is, can we categorise cryptocurrencies into taxonomies, and forecast the future success or failure of individual Altcoin categories? Another important topic discussed in this article is related to cryptocurrencies, the idea of Central Bank Digital Currencies (CBDCs), and the Friedrich von Hayek's theory of private money, which some experts argue it could lead to national currencies being replaced by '*the currency of the digital platform*' [11]. Another point on centralisation is that even cryptocurrencies that are meant to be very decentralised, such as Ethereum (ETH), and stablecoins such as UDSC, can be (in reality) very centralised, and potentially controllable.

1.2. Research questions and structure

The research aims, objectives, and questions motivating this article include **Aim**: To present the current and future values and risks associated to blockchain projects. **Research questions**:

1. Is the blockchain technology a driving force for innovation for the future versions of the internet and Web3 or is it the technology already obsolete?
2. What are the risks from cryptocurrencies?
3. What are the values from cryptocurrencies?
4. Which blockchain projects will survive in the long run?
5. Which blockchain projects can help further development in already developed countries?
6. Which blockchain projects can help developing countries?
7. Can cryptocurrencies and blockchain projects be regulated? And are national regulations or international regulations the correct solution?

The article follows a traditional (standard) structure, starting with chapter one (1) Introduction, chapter two (2) Methodology, then (3) the research engages with a Case study review of secondary data sources, and complements the case study with a new

chapter (4) that comprises a survey review. The article ends with a chapter (5) discussion, and (6) Conclusion.

2. Methodology

This article applies the case study method, in combination with survey review, and literature review. Since the initial search on the Web of Science and Scopus didn't result with a significant number of records, the search was expanded into a wider review of Google Scholar, IEEE, and other libraries. Although in the initial stages the focus was on new technologies, after the initial search, the review expanded into literature on ethics, trading, gambling, decentralised finance, and the Metaverse.

The Internet-of-Things (IoT) is already used in Blockchain 3.0 as open-source distributed ledger (e.g., IOTA, NEO, EOS) and has presented many unique alternatives for storing transactions with a potential for higher scalability (by using Tangle) over Blockchain 1.0 based distributed ledgers (such as Bitcoin). However, the interest in some of the early crypto projects seems to be dying down. As we can see in **Error! Reference source not found.** the research interest in some of the most promising projects from the pre-2018 bull run, seem to has almost completely died out – comparing to interest in cryptocurrencies in general.

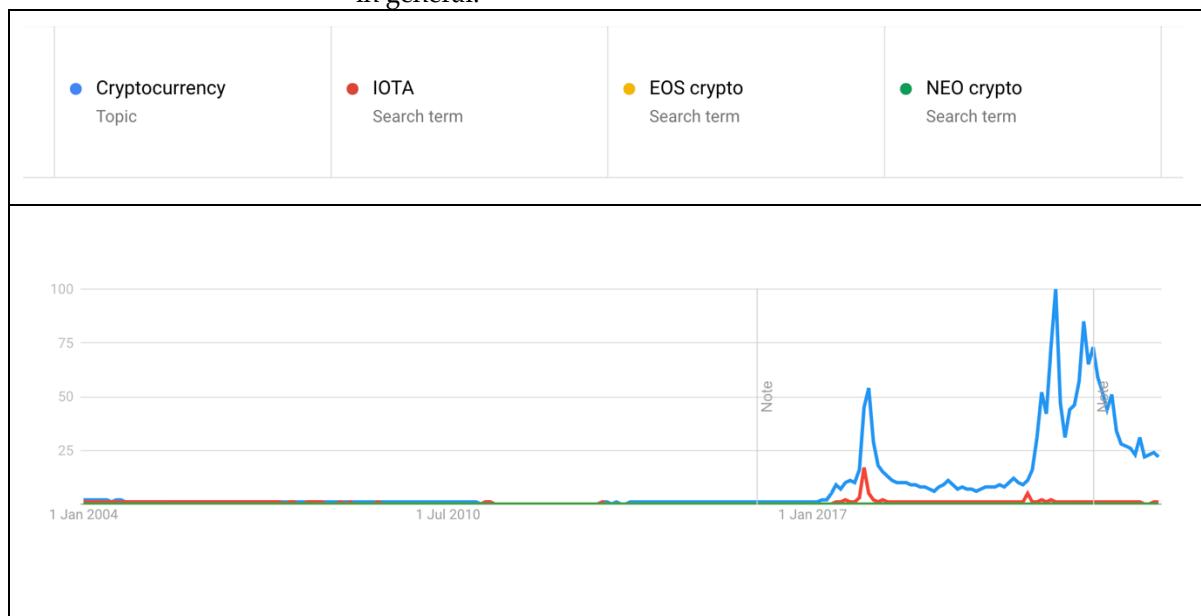


Figure 3. Trends in interest for early (pre-2018) crypto projects vs interest in cryptocurrencies in general.

One solution that seem to be under consideration is to rename existing projects (e.g., NEO is renamed to N3 – with a promise of a better Blockchain)⁵, and IOTA is keeping its name, but evolving into a new blockchain called Crysallis⁶. Although the idea of IoT based crypto is undeniably valuable, further research is required to determine how IoT technologies would resolve the main problem of Blockchain 1.0, namely the (i) speed of transaction, and the (ii) security risk from quantum computers. For the first part of the objective, the IOTA project can process around 500-800 transactions per second. There are much faster blockchains, such as Solana that can process 50,000 transactions per second.

1. Case Study review

⁵ <https://neo.org/>

⁶ <https://chrysalis.iota.org/status>

The first version of Blockchain (Bitcoin) combined cryptography with distributed computing, both of which are decades old technologies. Blockchain 1.0 is a database maintained by combining a network of computers that collaborate and share data, creating a new class of information technology (Distributed Secure Database).

2.1. *Blockchain solutions*

IoT for healthcare

The increased adoption of IoT in health services seems inevitable, because IoT offers increased efficiency at reduced amount of time spent, which seems exactly what the NHS needs. To reduce costs and provide the support required, the NHS must automate some of the basic data collection and monitoring, which would free skilled staff to focus on patient safety and patient service. One of the main crypto projects that could benefit NHS is the 'VeChain' project, which resolves many of the existing supply chain issues. The 'VeChain' project is already running and operational, but in the future, it would be interesting to have even more automated, machine controlled supply chains, and for that, we have a very different set of Blockchain solutions – based on IoT systems.

Decentralised finance – DeFi

Decentralised finance is based on automated protocols for providing financial services. The DeFi solutions have many advantages over traditional finance, some include faster and improved transparency, interoperability, immutability, operations across borders. However, these strengths are also the main weaknesses. In other sections of this review, we discuss that processing transactions across borders at speed is not a difficult task, but the challenges are in the money laundry compliance process. The speed of DeFi is often at the cost of non-compliance, and although some day, this will be resolved, at present, it is still a major challenge for large scale adoption – on a national level, as in El Salvador. Some of the big DeFi protocols in 2023 include Aave, Compound, Curve Finance, Synthetix, PancakeSwap, Kyber Network, Uniswap, and many other protocols. Although new protocols are gaining ground, Uniswap remains the most popular decentralised exchange. The collapse of FTX and other centralised exchanges, has opened a new market potential for decentralised exchanges, but many questions remain on how decentralised some of the decentralised exchanges are.

Centralized exchanges

Centralized exchanges have been hit hard in 2022 and without centralised regulations, it seems like centralized exchanges will continue to make the same mistakes. Although centralized exchanges that survived the storm (e.g., Binance, Coinbase, Kraken, KuCoin, among others) claim to be compliant, this compliance is not overseen, except in some cases in the US, Australia, and New Zealand. Some of the major exchanges that are regulated (although not to the same level as stock exchanges and banks), in Australia and NZ are also ATO and AML compliant, KYC. Coinbase in the US is also regulated to a similar level. In a different article, we will review how effective is this compliance, but in this article, we focus on the level of compliance that is required for crypto assets to be considered as truly compliant. Because partial compliance can be confusing, and by classifying such risky assets as compliant, opens the possibility for fund managers to combine these risky assets in a relatively safe financial products (e.g., pension funds) and that is one potential scenario for a future version of the 2008 sub-prime mortgage crisis.

Layer 1s and 2s, Non-Fungible Tokens (NFTs), and the Metaverses

In a decentralised terminology, a Blockchain (e.g., Bitcoin, Ethereum) is referred to as a Layer 1, and protocols that can be used in conjunction with a Blockchain are known as Layer 2 (e.g., Arbitrum, Optimism). Most Metaverses are Layer 2 protocols on existing Blockchains, for example, Decentraland (MANA), ApeCoin (APE), Axie Infinity (AXS), the Sandbox (SAND), Enjin Coin (ENJ), Gala (GALA), Render (RNDR), and Metahero

(HERO) are all powered by the Ethereum (ETH) blockchain. Theta (THETA) started as an ERC-20 token but converted to native THETA. Uses two tokens THETA for governance and TFUEL for utility. Stacks (STX) is one of a very few layer-1 blockchains in the Metaverse ecosystem. Non-Fungible Tokens (NFTs) are assets that represent a unique piece of art, digital content, or media. NFTs can be used for trading and storing value in the Metaverses, but majority of the NFTs have proven to be less valuable than some investor hoped.

Crypto Bridges and Oracles

Blockchain bridges enable the movement of assets from one Layer 1 to another Layer 1, or from a Layer 1 to Layer 2, and the reverse. Some of the most popular bridges in 2023 include Hop Exchange, Orbiter, Rango Exchange, cBridge, xPollinate, AllBridge, and many other names. Worth mentioning that many of the major hacks that resulted with a significant loss of Crypto in 2022, were based on cyber-attacks on Crypto bridges. While Bridges resolve the issues of interoperability across chains, Oracles (such as Chainlink) enable cross-chain communication and enable smart contracts to execute on different Blockchains.

Crypto Wallets

Cryptocurrency digital wallets can be classified in three categories, first is safe storage hard wallets where crypto is stored on a personal device (e.g., Ledger, Trezor), second category is hot wallets (such as Metamask, TrustWallet), and exchange wallets (e.g., Coinbase Wallet). Given the recent collapses of centralised exchanges, it is hard to see why people still keep Crypto in exchange wallets, and it could be that users simply prefer someone to run the day-to-day management of their savings and finances. If that is taken as a postulate, then the regulations of such centralised exchanges become of a paramount importance.

2.2. Lessons to be learned from the errors in FTX and Terra Luna

FTX was a centralised cryptocurrency exchange, providing services such as crypto derivatives and leverage trading, but the main use for centralised exchanges is to enable customers to buy and exchange different cryptocurrencies. The main problems that resulted with the collapse of FTX also apply to all other centralised cryptocurrency exchanges that are currently in operation. Cryptocurrency exchange are not regulated, which leads to individuals taking risks without the approval of the asset owners. Which is an oversimplified description of why centralised cryptocurrency exchange should not be allowed to operate without regulations. Individual savers are not always keen on keeping their assets on a USB drive or writing the private keys on a piece of paper, which if lost, would result with the loss of their savings. Hence, many small crypto savers use centralised cryptocurrency exchanges (such as FTX) to store their crypto savings and earn interest – similarly to the traditional banking system. Despite all the warning signs, individual savers are still locking their crypto savings in unregulated centralised exchanges.

This presents three options to the UK government and all other governments in the world.

1. First is to create standards and regulations for cryptocurrencies, because as of today (08 Jan 2023), we have 22,228 different cryptos (i.e., crypto projects) and 534 crypto exchanges, with a market cap of \$824,468,428,103, and 24h trade volume of \$16,374,071,351[15], and none of the trades are regulated in the UK, nor in most of the other countries in the world.
2. Second is to ban all use of cryptocurrencies, including the ownership and trading, but this is unlikely to be effective, because most crypto projects are run from outside of the UK, and some (e.g., Bitcoin) are decentralised. Hence, even if a global taskforce could be created to track and trace cryptocurrency projects and exchanges, it would be ineffective against decentralised crypto, and it will only serve to push the trade and ownership into the dark

economy. In addition, it is unlikely that the legal mechanisms can cope with persecuting all cryptocurrency projects and exchanges, because as we can see from the case of the XRP legal proceedings, just one case can take years to resolve. The US Government has proven that it can be effective in banning crypto projects, in August 2022, the U.S. Treasury sanctioned the virtual currency mixer Tornado Cash [16]. The Tornado Cash DAO was shut down and its lead developer Aleksey Pertsev was arrested, but what this translates to is that the mixer's code itself is banned for use, and it does not mean that the code has been disabled and cannot be used. To simplify this further, it means that the Tornado Cash U.S. crypto customers are not allowed to use the mixer, at least not without a permission from the U.S. Treasury. The mixer is blacklisted in the US because of its use in money laundering. However, the Tornado Cash app will continue to operate on the Ethereum blockchain exists, the key point is that it is impossible to shut down such technology without shutting down the entire Blockchain. Given that some Blockchains are decentralised, this will prove difficult, and even, if possible, there are many new Blockchains emerging all the time. Hence, sanctioning and banning is unlikely to serve as a valid too for completely closing all operations.

3. Third option is to create fully centralised, Government run Blockchains, upon which open crypto projects and exchanges can be built. In this scenario, Governments would be able to control the type of projects and impose regulations and standards upon the developers and the user community. In such fully centralised Blockchains, the government could allow the development of centralised and decentralised crypto exchanges, and fund or encourage the development of CBDCs (Central Bank Digital Currencies) and regulated Stablecoins (cryptocurrency with a pegged value to another currency, commodity, or financial instrument). By enabling the development of a fully regulated Stablecoin, the UK Government would prevent one of the main risks for individual crypto savers, which is the collapse of another Stablecoin – which is what happened to the UST Algorithmic Stablecoin in 2022. Many of the current stablecoins are highly speculative, and at present most stablecoins are not audited or regulated – at least not in any meaningful way. Although Tether (USDT) has announced that it is preparing to be audited by a large accounting firm to prove the transparency of Tether, at present USDT market reserves are not audited, and as of today, the market cap of Tether is \$66,268,895,618., with around \$11,106,992,770 of the cryptocurrency stablecoins being traded in the last 24 hours alone. Tether (USDT) is just one of many stablecoins on the many crypto exchanges that exist today. In the top 10 cryptocurrencies by market cap, apart from USDT, we also have the USDC (market cap of \$43,922,152,193), and BUSD (market cap of \$16,377,185,225), while on the 11th place we have DAI (market cap of \$5,790,436,026), on the 41st place we have USDP (market cap of \$876,254,775), on 43rd place TUSD (market cap of \$846,271,617), on the 52nd place is USDD (market cap of \$707,743,989) and so on – data from 8th of January 2023 [15]. From the above listed stablecoins, USDC has reserves regularly attested, but not audited, in fact, none of the stablecoins are audited. This creates a systemic risk for all cryptocurrencies and regulating the stablecoins will not only prevent future loss of savings for individual users and savers (hodlers), but it would increase the confidence in the market, and if combined with a regulated crypto exchange, it would provide security and quick exit for investors during times of volatility. Final comment on CBDCs, we must point out that the view emerging from this article is not sympathetic with the values to society and economy from CBDCs. Although CBDCs would resolve many issues related to fluctuations in price of all cryptocurrencies, the stablecoin solution could be a preferred version of a Blockchain based currency, more specifically,

decentralised stablecoins. However, the collapse of UST – LUNA has exposed vulnerabilities in some of the decentralised algorithmic stablecoins. We need new solutions that would address some of the vulnerabilities that got exposed in 2022.

4. The main lesson that we must learn from FTX is that without taking regulatory action, the cases of corporate malfunction and malfeasance will continue to dominate the cryptocurrency ecosystems. Even if governments around the world decide to embrace the concept of complete monetary decentralisation (which seems highly unlikely), there are elements of the crypto markets that still need to be regulated, just to ensure that self-governance is not replaced again with malfeasance. The collapse of FTX (which was considered as one of the safest exchanges because of the public display of approval from various high-profile politicians), has proven that corporate malfeasance exists in cryptocurrencies on a much greater level than we are aware. To put this into a perspective, if users start withdrawing large volumes from any of the above listed stablecoins, it seems questionable if they will survive. That is not to say that the concept of stablecoins should be abandoned, or that the currency should be pegged to the gold and not to the USD. Stablecoins provide crucial service in the crypto markets, and USD is the most traded currency. The concept seems sound, but the regulations, standards and accountancy audits are missing.

These three scenarios could be seen as the opportunities for the UK Government to intervene and take advantage of the situation to establish the UK as the leading country in the world, that is providing a highly demanded service (which is also highly profitable), but also highly regulated, standardised, and audited according to international standards. Would this expose the UK economy to unnecessary risk? That depends on how this process is undertaken. If the UK develops a new Blockchain that provides the services that are used by companies to build crypto projects, then the risk to the UK is minimal, because even if the crypto markets collapse and the value of Bitcoin drops to its all-time lows from year 2009, the Blockchain would still charge transaction fees until the market cap goes down to zero, at which point, there won't be any transactions, and there won't be any cost, because there won't be any need for maintaining the new Blockchain. Similar arguments can be made about the development of a UK crypto exchange, regardless of the level of centralisation, the code for Uniswap and many other exchanges is open and can be copied to create a new exchange without building a new code. In fact, that is exactly what SushiSwap did, and it gained a significant market cap and trading volume almost instantly.

3. Survey of Crypto use cases

The use case for crypto projects depends largely on the specifics of the project features and characteristics. Some of the most popular use cases come with questionable motives. For example, the idea that bitcoin can be considered as digital gold, or as a store of value, and that bitcoin can be used to preserve wealth and hedge against inflation, this use case is very debatable. There are many use cases for crypto, and below I list some realistic use cases, but the idea that a digital asset with no other purpose or a use case can replace gold, is not very convincing. It seems more likely that Bitcoin will need to be wrapped and transferred to a different chain, where cost of transactions is much lower, and be used as a payment system, similar to SWIFT. That could be a real-world use case, and we already have the Algorand Blockchain, which is capable of handling wrapped Bitcoins, and the cost of transactions is very low, while security is high. Algorand could even enhance the security of Bitcoin. There will be many other Blockchains that can do the same function. Hence, the bitcoin community needs to start innovating, because back in 2009, Satoshi presented the most innovative and secure technology, but surely, he didn't expect this to remain the same forever.

Some of the real-world use cases include:

1. Borderless payments without any centralised entities acting as an intermediary,

Decentralised finance, for lending and borrowing, accessible to anyone and everyone that has internet connection and knows how to use the specific blockchain – crypto project,

2. Security and privacy of products (and services) as they move through different supply chains,

3. Authenticity verification for products and services,

4. Ensuring payments are processed fairly in supply chains- with the use of smart contracts,

5. Buying and owning digital assets, such as gaming and collectibles that can be owned as non-fungible tokens (NFTs).

6. Crypto transactions can be designed to help with privacy and anonymity, creating added value to users that prefer to keep their finances private.

7. Crypto can be used for crowdfunding, where new funds can be raised by issuing initial coin offerings (ICO) or token generation events (TGEs).

8. Crypto can be used by creatives to monetise their work, for example, digital content creators can accept payments for premium content, and this can open a safer and cheaper environment for a variety of artists, from dancers, tutors, painters, to fitness instructors, digital consultants and education providers.

9. Charitable donations, crypto can be used as a fast and secure method for transferring wealth to people in need.

Worth mentioning that new use cases will continue to emerge with the increased adoption of the decentralised blockchain technology. One way to compare the current state of crypto, is to think of web one, vs web two, and the emergence of web three. Web one was just a collection of data and information, that was made available for free online. Web one was called the ‘information highway’, and despite its amazing potential, it was soon replaced by the web two, which is the current version of the interactive internet, where we can click likes, and talk to people on the other side of the planet. But as we can see today, there are some major concerns in regards to the web two version, and many social platforms have been criticised for exploitation of users privacy. This will inevitably lead to a new version of the web, which is predicted to be based on the Blockchain technology. Hence, the blockchain technology, has already found its main use case - the adoption of blockchains in the web3.

We could consider the Bitcoin emergence in 2009, to the first web browser – AOL. Although AOL was the most popular browser when it first emerged, it was soon replaced by Hotmail. We could compare Hotmail to Ethereum, and this is the current state of the art in 2023. Since Ethereum is dominating the crypto world, with the new and emerging layer 2 projects, such as Optimism and Arbitrum, and the upgraded blockchain, from proof of work to proof of stake, we can easily argue that Ethereum is all the rage in 2023. The real question is, would Ethereum be as popular in 5-10 years’ time, or would the project be taken over by another crypto. One thing that comes to mind is that at its final days, Hotmail was experimenting with quite a few features that were very similar to the competitors (e.g., Hotmail live), and the users still decided to leave Hotmail and move to other projects. The most puzzling is that the current version of WhatsApp is very similar to the old MSN chat. The design is similar, the functions are similar, and WhatsApp is still very popular among the older generations, while MSN lost many of the users, and the project was abandoned. Although some WhatsApp users would argue that the platform is based on the mobile signal, that is false, the WhatsApp platform uses the personal mobile number as a username, not as a method for communications. Without internet connection, WhatsApp won’t work, hence, one could argue that the MSN was much safer application, because you could create a new and random username, instead of using your personal mobile number. This example is just to build the argument that when we have multiple platforms, providing similar services, it is very unpredictable which platform will prevail in the long run. Unless crypto projects are uniquely positioned to provide a specific service to users, their long-term viability is entirely dependent on the preferences of the user community. If Ethereum becomes the MSN, then who is WhatsApp? The answer is not a single platform, because NEAR, SOL, and at least few doused other projects can do almost

everything that Ethereum does. The real question is, which project will be the next Google, or even the new ChatGPT, and would Bitcoin pull another revival with the Lightning network, because when transmitted using the Lightning network, there is no real difference between layer 1s and 2s. Bitcoin has also been increasing the level of renewable energy use, and maybe it's just a nostalgia of an old Satoshi fan, but if Bitcoin can improve speed, energy use, and become more user friendly for every day shopping, maybe the new Blockchain innovations will come from Bitcoin.

The Buterin's trilemma

This review article would not be complete without discussing the Buterin's trilemma and how that fundamentally captures the trade-offs between security, decentralisation, speed, and the attendant risks. Some blockchains (e.g., Sol) clearly go for speed, but are more centralised; others are less centralised, but often more secure. One study suggested a solution called '*The Blockchain Quadrilemma*', but also recognised that for basic Blockchain operations '*Algorand can often be the right choice*', but Ethereum is recommended for '*more sophisticated computations*' [17]. Another research study recommended '*a dichotomy of algorithms between leader-based and voting-based consensus algorithms*' based on '*tradeoffs ... for a given distributed system*' [18]. It is worth mentioning that some experts recommend a '*incentive-based role in the governance of DeFi as opposed to an enforcement-oriented role*', because we need to build new tools that enable new '*policy options in a transnational environment hostile to formal state intervention*' [19].

4. Discussion

Crypto is still a subject to many risks, for investors and for users. One of the main risks for investors is that the value is extremely volatile and fluctuates significantly in short periods of time. This makes crypto price and value extremely difficult to predict, and can lead to significant losses when the value drops significantly. Since crypto is also a speculative asset, investors cannot be certain that the value of their investment will ever recover, or go to zero.

Another risk is that crypto is not regulated by anyone, not by a government, nor by any financial institution. This is the clearest indicator that there won't be any protection or oversight from fraud, mismanagement or financial malfeasance. In other words, crypto investors need to be aware that if something goes wrong, they will have very little recourse.

Apart from these risks, one commonly discussed risk is the safety and security of the blockchain technology. The common topic in media is that the underlying blockchain technology is not as secure as it was thought to be. The rationale for this assumption is the fact that in the past, we had some very high profile hacks that managed to result with the theft of large amounts of crypto from exchanges and wallets. Although the latest is correct, the first is not. Bitcoin and other secured blockchains have never been hacked, the hacks happen on crypto exchanges, on digital wallets that do not apply appropriate security, and most of the theft has been on crypto bridges, pools, and other instruments that are not really related to the blockchain technology itself. To explain this in other words, the Blockchain is as secure as it has been described in the first paper written by Satoshi, but the new projects are bypassing the security requirements, often because there are no cybersecurity standards, and the hacks are increasing, but this does not mean that the blockchain technology is not secure, it means that we need cybersecurity standards for projects that use blockchain technology.

4.1. The good

Traditional finance has also been slow in developing new faster and more secure solutions. The SWIFT network is very slow comparing to some of the crypto solutions, and the idea of tokenised USD does seem appealing to many users, most specifically to traders. Cryptocurrencies can also solve much of the banking problems in developing countries. The ability to make payments and transfer tokens that are pegged with the value of USD,

could provide solutions to much of the developed world that is still lacking the basic banking services. Since existing payment methods like Visa or Mastercard charge service fees, it is reasonable to expect that some small fee would be considered acceptable to users. However, there is no evidence of crypto being adopted as a method of payment in developing countries. Although some countries like El Salvador have adopted Bitcoin, its use for everyday payment has not been adopted. Another point to make here is related to the value of Bitcoin (BTC), and the value of private money and wallets. Although decentralised cryptocurrencies don't hedge against short term inflation, Bitcoin has massively outperformed gold over a decade in the face of monetary easing/printing.

4.2. . The bad

Bitcoin emerged from the financial chaos in 2008, and it was presented as a solution to the centralised banking system and the high-risk practices of a few greedy financial firms that only care about profits. The long-term economic utility is also questionable. Why would one coin that is created out of code be valued in thousands of pounds, and another coin that is also created out of code be worth zero. For crypto to be seen as a long-term value, it must provide economic utility, and at present, crypto is not providing such utility. Another problem is that in technological terms, crypto is old technology, the first block was created in 2009, and we have seen a rapid technological change since then. Most of the mobile phones from 2009 are now considered old and almost obsolete. We are still waiting for some extraordinary use case for crypto, but since it hasn't really materialised until now, the question is when it will, and would it ever happen.

4.3. The ugly

At present, the crypto market is not connected to the traditional markets, and it is relatively small. If the crypto market gets connected to the traditional finance, the spill-over effect needs to be considered. The main concern is that, if the crypto market is regulated in a way that it would get supercharged, and its allowed to create the connections between regulated finance, and the crypto system, then crypto problems can become much bigger problems. This would mean that people that never invested in crypto, are affected by fluctuations in price, and crypto market risks, in the same way that investors were affected by the mortgage-backed securities in 2008. Hence, the focus in regulations should be on minimising the connections between the crypto market and the regulated financial system.

5. Conclusion

The question that emerges from this review paper is, if we fast forward 10 years, would all the transactions that we perform in our society be in fiat currencies, and the answer is that most probably they won't. With the emergence of Web3, assets, currencies and marketplaces will become interconnected, and some of the cryptocurrencies will form part of these new digital assets, but would that be Bitcoin, or some of the other 22,250 cryptos that are in circulation today, that is difficult to predict.

What also becomes clear is that regulation would eliminate many of the the cases of corporate malfeasance. Regulations will most likely also remove many of the current use cases for crypto. Much of the current hype around crypto is around the lack of regulations, and when regulations are applied, the promise of getting rich from crypto would certainly start to weaken. With regulations, crypto projects will have to start making checks (KYC) on who their customers are, and this argument for regulations killing the crypto is especially strong for cryptocurrencies that are created with no real use case, and based purely on the promise of making a great deal of money for early investors. Once regulations are created, these cryptos will be out of the picture. Most of the crypto projects are almost certainly not compliant with the derivatives or either security regulators. Crypto has been operating in a very grey area, where different crypto project are considered as commodities, and because of that, crypto exchanges do not need to register with the federal government and be subject to regulation. This debate has been ongoing for far too long, the

issue of whether crypto is a commodity or crypto is a security is not really the main point of concern. The main concern is not the naming, but whether crypto is a subject to regulation, and from this perspective, it makes sense to call all crypto assets securities, which will mean that all crypto is subjected to strong oversight. The issue is that, if that happens, most crypto projects won't be able to comply, and that will hurt not only the crypto industry, but also the crypto investors. Given that regulations are designed to protect investors, it is uncertain if such strong approach would serve the purpose it intended to, or would it lead to a significant loss for crypto investors. A more realistic approach would be to regulate crypto exchanges, and to ensure that exchanges are registered as investment dealers. This seems realistic and reasonable, because if crypto investor engages in a contract with a crypto exchange, where the exchange would promise a very lucrative return, or some special benefits that are not very realistic, there are small crypto investors that might fail for such advertisements. This makes crypto exchanges investment deadlier, and they need to be regulated. Regulators need to engage in how these exchanges keep their assets, how do they get the returns, and ensure that exchanges are not taking unnecessary risks that expose investors to risk that they are not aware of, or do not fully understand. The old saying in crypto is 'not your keys, not your crypto', and regulating the centralised exchanges, won't even come with any disagreement from the crypto community.

6. Final comments

Final comment on investing in crypto, despite the remarkable returns some investors have benefited from, the crypto market has not matured yet, and the market – including the technology – is still evolving. There are risks, and investing in crypto comes with serious risks, and investors should approach crypto with caution. In addition, we still cannot use Bitcoin or any other Crypto to buy coffee in Costa or Starbucks, we cannot buy food in Tesco, and transactions come at a cost, while using fiat, doesn't cost. Until we can use crypto as a fiat currency, in every aspect of the use cases, we won't really be able to claim that retail and commerce adoption is increasing, even if the price of crypto goes up (or down), the use case doesn't change much, and this triggers concerns. On the other hand, the claim that Bitcoin is used for crime and money laundry, has been contradicted by blockchain analysis company Chainalysis, which reported that only a very small percentage (0.15% total of \$14bl) of known cryptocurrency transactions conducted in 2021 were involved in illicit activities [23].

Declarations:

Availability of data and materials: all data and materials are included in the article.

Code availability: N/A – no code was developed.

Competing interests: No conflict nor competing interest.

Funding: This work has been supported by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which has been funded by the UK EPSRC [under grant number EP/S035362/1] and by the Cisco Research Centre [grant number CG1525381].

Authors contributions: One author.

Acknowledgments: Eternal gratitude to the Fulbright Visiting Scholar Project.

Short biographical note:



Petar Radanliev is a Post-Doctoral Research Associate at the University of Oxford. He obtained his Ph.D. at University of Wales in 2014 and continued with Postdoctoral research at Imperial College London, Massachusetts Institute of Technology, University of Cambridge, and the University of Oxford. His current research focusses on Blockchain Technologies, Cryptocurrencies, the Metaverse, Cybersecurity, Cyber Risk, Privacy, Ethics, and the Internet of Things. For his research work, Petar has been awarded the Fulbright Fellowship and the Prince of Wales Innovation Scholarship.

1. Abbreviations

Bitcoin – the first decentralised blockchain

Terra Luna – collapsed crypto project

FTX – collapsed crypto exchange

Solana (SOL) – crypto project that got affected by the FTX collapse

Ethereum, Cardano, Dogecoin, Litecoin, Algorand, NEAR – crypto projects that remained popular with investors in the 2021 bull run

IOTA, NEO, EOS – crypto projects that were popular in the previous bull runs, and are still present in the crypto market in 2023

NEFD - new and emerging forms of data

CBDCs - Central Bank Digital Currencies

Tornado Cash DAO – crypto mixer that has been prohibited for use by the USA

UST Algorithmic Stablecoin – collapsed stablecoin

USDT, USDC, DAI, BUSD, USDP, USDD, TUSD - Stablecoins still in existence in 2023 (as of 25th of January 2023)

NHS – National health Service

Uniswap / SushiSwap – decentralised exchanges

NFTs - non-fungible tokens

ICO - initial coin offerings

TGEs - token generation events

ChatGPT – AI based chat designed to replace the Google search engine

M-Pesa - SIM card payment from a mobile phone

We Chat Pay - a QR Code payment

KYC – know your customer

Bibliography

- [1] C. Dierksmeier and P. Seele, "Cryptocurrencies and Business Ethics," *Journal of Business Ethics*, vol. 152, no. 1, pp. 1–14, Sep. 2018, doi: 10.1007/S10551-016-3298-0/TABLES/1.
- [2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.
- [3] A. Mikhaylov, H. Dinçer, and S. Yüksel, "Analysis of financial development and open innovation oriented fintech potential for emerging economies using an integrated decision-making approach of MF-X-DMA and

golden cut bipolar q-ROFSs," *Financial Innovation*, vol. 9, no. 1, pp. 1–34, Dec. 2023, doi: 10.1186/S40854-022-00399-6/TABLES/26.

- [4] A. A. Khan *et al.*, "QoS-Ledger: Smart Contracts and Metaheuristic for Secure Quality-of-Service and Cost-Efficient Scheduling of Medical-Data Processing," *Electronics* 2021, Vol. 10, Page 3083, vol. 10, no. 24, p. 3083, Dec. 2021, doi: 10.3390/ELECTRONICS10243083.
- [5] M. C. Chang and D. Park, "How Can Blockchain Help People in the Event of Pandemics Such as the COVID-19?," *Journal of Medical Systems*, vol. 44, no. 5. Springer, May 01, 2020. doi: 10.1007/s10916-020-01577-8.
- [6] B. Pranggono and A. Arabo, "COVID-19 pandemic cybersecurity issues," *Internet Technology Letters*, vol. 4, no. 2, p. e247, Mar. 2021, doi: 10.1002/itl2.247.
- [7] D. S. W. Ting, L. Carin, V. Dzau, and T. Y. Wong, "Digital technology and COVID-19," *Nature Medicine*, Nature Research, pp. 1–3, Mar. 27, 2020. doi: 10.1038/s41591-020-0824-5.
- [8] E. Bouri, X. V. Vo, and T. Saeed, "Return equicorrelation in the cryptocurrency market: Analysis and determinants," *Financ Res Lett*, vol. 38, p. 101497, Jan. 2021, doi: 10.1016/j.frl.2020.101497.
- [9] A. T. Aspembitova, L. Feng, and L. Y. Chew, "Behavioral structure of users in cryptocurrency market," *PLoS One*, vol. 16, no. 1, p. e0242600, Jan. 2021, doi: 10.1371/journal.pone.0242600.
- [10] C. F. Breidbach and S. Tana, "Betting on Bitcoin: How social collectives shape cryptocurrency markets," *J Bus Res*, vol. 122, pp. 311–320, Jan. 2021, doi: 10.1016/j.jbusres.2020.09.017.
- [11] A. Y. Mikhaylov, "Development of Friedrich von Hayek's theory of private money and economic implications for digital currencies," *Terra Economicus*, vol. 19, no. 1, pp. 53–62, 2021, doi: 10.18522/2073-6606-2021-19-1-53-62.
- [12] The Federal Reserve, "Central Bank Digital Currency (CBDC)," 2022. [Online]. Available: <https://www.federalreserve.gov/central-bank-digital-currency.htm>
- [13] M. in C. R. (MiCA), "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," 2022.
- [14] HMT, "UK sets out plans to regulate crypto and protect consumers - GOV.UK," *HM Treasury - Gov.UK*, Feb. 01, 2023. <https://www.gov.uk/government/news/uk-sets-out-plans-to-regulate-crypto-and-protect-consumers> (accessed Mar. 06, 2023).
- [15] CoinMarketCap, "Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap." <https://coinmarketcap.com/> (accessed Jan. 08, 2023).
- [16] OFAC, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," *U.S. Department of the Treasury*, Aug. 08, 2022. <https://home.treasury.gov/news/press-releases/jy0916> (accessed Jan. 08, 2023).
- [17] F. Mogavero, I. Visconti, A. Vitaletti, and M. Zecchini, "The Blockchain Quadrilemma: When Also Computational Effectiveness Matters," *Proc IEEE Symp Comput Commun*, vol. 2021-September, 2021, doi: 10.1109/ISCC53001.2021.9631511.
- [18] A. Altarawneh, T. Herschberg, S. Medury, F. Kandah, and A. Skjellum, "Buterin's Scalability Trilemma viewed through a State-change-based Classification for Common Consensus Algorithms," *2020 10th Annual Computing and Communication Workshop and Conference*, CCWC 2020, pp. 727–736, Jan. 2020, doi: 10.1109/CCWC47524.2020.9031204.
- [19] A. Wang, "Rethinking the Rule and Role of Law in Decentralized Finance," *Proceedings - 2022 IEEE 24th Conference on Business Informatics*, CBI 2022, vol. 2, pp. 118–125, 2022, doi: 10.1109/CBI54897.2022.10057.
- [20] H. J. Kim, J. S. Hong, H. C. Hwang, S. M. Kim, and D. H. Han, "Comparison of Psychological Status and Investment Style Between Bitcoin Investors and Share Investors," *Front Psychol*, vol. 11, p. 3230, Nov. 2020, doi: 10.3389/FPSYG.2020.502295/BIBTEX.
- [21] B. Johnson *et al.*, "Cryptocurrency trading and its associations with gambling and mental health: A scoping review," *Addictive Behaviors*, vol. 136, p. 107504, Jan. 2023, doi: 10.1016/J.ADDBEH.2022.107504.

[22] P. Delfabbro, D. L. King, and J. Williams, "The psychology of cryptocurrency trading: Risk and protective factors," *J Behav Addict*, vol. 10, no. 2, p. 201, Jun. 2021, doi: 10.1556/2006.2021.00037.

[23] M. Sun and D. Smagalla, "Cryptocurrency-Based Crime Hit a Record \$14 Billion in 2021 - WSJ," *The Wall Street Journal*, 2022. Accessed: Mar. 08, 2023. [Online]. Available: <https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073>