Cryptic Regulation of Crypto-Tokens

Joshua S. Gans[1]

May 2023

This paper investigates the alignment of existing securities regulations with the emerging landscape of crypto-tokens and blockchain technology. By examining the features of these digital assets, including decentralization, consensus mechanisms, and programmability, we analyze how they interact with existing financial rules. We compare approaches to regulation across countries, considering potential impacts on innovation. Furthermore, we explore the issues that may arise with blockchain networks, such as payment efficiency and market safety. The study aims to contribute to discussions about balancing innovation within the blockchain sphere and ensuring investor protection and market security, underlining areas that may necessitate regulatory improvements.

JEL Classification Numbers: K22, O38

Keywords: crypto-token, regulation, securities, stablecoins, regulatory uncertainty

[1] University of Toronto and NBER. Thanks to Christian Catalini, Richard Holden, Josh Lerner, Eric Talley and participants at the NBER Entrepreneurship and Innovation Policy and the Economy Conference (2023) for helpful comments. All views here are my own.

Introduction

The fast growth of blockchain technology and the increasing number of crypto-tokens have changed the world of finance in recent years, leading to a need to reconsider existing regulations (Halaburda, Haeringer, and Sarvary, 2022). Crypto-tokens are unique because they are often not controlled by one central authority, can be used across borders, and can be programmed to do specific tasks, like transferring value or executing smart contracts (Nakamoto, 2008; Swan, 2015). This paper looks at the current regulations for crypto-tokens, focusing on rules related to securities, and asks if these rules are a good fit for cryptocurrencies and blockchain technology.

Securities rules have developed over time to make sure financial markets are fair, open, and protect investors. However, crypto-tokens can sometimes have features of both securities and commodities, making it difficult to apply traditional rules (Zohar, 2015). In the United States, the Securities and Exchange Commission (SEC) has tried to classify many crypto-tokens as securities using the "Howey Test" (SEC, 2017). Some people say this approach might hold back innovation because it does not fully consider the special features of blockchain-based assets. On the other hand, some countries, like Switzerland and Singapore, have created specific rules for crypto-tokens that try to balance supporting innovation and protecting investors (FINMA, 2018; MAS, 2020). These countries realize that one set of rules might not work for all the different types of crypto-tokens out there (Watch, 2016).

To regulate crypto-tokens appropriately, it is important to understand how they work and how their features affect finance. This paper will look at the main features of cryptocurrencies and blockchain technology, like decentralization, consensus mechanisms, and programmability (Mougayar, 2016). We will also discuss how these features interact with current rules and point out any areas that might need improvement, especially when it comes to supporting innovation.

By looking closely at the current rules for crypto-tokens, this paper hopes to add to the ongoing discussion about how to find the right balance between supporting new ideas in the blockchain world and keeping investors and financial markets safe.

The paper is organized as follows. First, we look at the features of crypto-tokens and how they work. Next, we discuss possible issues that might come up with crypto-tokens on blockchain networks, like payment efficiency, information gaps, and market safety. Then, we explore different types of rules, including bans, securities law, and banking regulations. Finally, we examine the effect of these rules on innovation in the blockchain space.

What are Crypto-Tokens?

Crypto-tokens are digital assets that, while comprised of pure information, are *rival* in nature as more than one agent cannot hold them at any given time. In this regard, they stand in contrast to many digital items that, in principle, can be consumed by many agents simultaneously without diminishing the value anyone receives from that consumption. The combination of rivalry and digitisation means that crypto-tokens offer the potential to associate (i.e., program) rights that can be associated with or granted to the holder of those tokens.

The most famous crypto-tokens are those designed to be a form of money. Such cryptocurrencies grant a single right to their holder – the ability to transfer ownership of the digital asset to other agents.[2] This gives them the potential to be used as a form of payment for goods and services or to be exchanged with other currencies, including notably, fiat currency issued by governments. Of course, as such tokens are designed to be fungible – i.e., the rights granted to the holder are symmetric across all token units – their value as a payment instrument requires that they are scarce (Fama, 1980). Thus, cryptocurrencies have coded rules that regulate the supply of tokens. For instance, the first and most famous cryptocurrency, Bitcoin, 'minted' an initial quantity of tokens and then required new tokens to be issued via a computational contest (Nakamoto, 2008). The Bitcoin protocol code has algorithmic measures that ensure that the total supply of bitcoins remains scarce and growing at a diminishing rate over time, eventually coming to a halt at 21 million bitcoins, to be achieved in over a century's time. The combination of transferability and scarcity implies that bitcoins can serve as a payment mechanism of the type first modelled by Kocherlakota (1998).

Precisely because crypto-tokens were maintained in digital code, it became natural to see those tokens being made interoperable with other software systems. In the blockchain environment, the most famous development in this regard is Ethereum. Ethereum has a cryptocurrency called Ether that is used for payments, including to those who are engaged in tasks to keep the network operational, but importantly, along with the record of who controls a particular token at any given time, it also holds the state of a virtual machine that can, in principle, be programmed to execute any code a classical computer can handle – that is, the virtual machine is what is called Turing complete. This functionality has given rise to the notion of programmable money. Rather than rely on the actions or approval of a token-holder to initiate a transfer of the token to others, transfers can be made contingent on the state of the virtual machine. For instance, the virtual machine might read weather conditions and initiate transfers in the event that there are poor weather conditions. This allows insurance contracts to be coded and executed on the blockchain. Other so-called smart contracts may be used to complete real-world trades (Gans, 2021), while there has been considerable activity to provide more sophisticated financial contracts (so-called DeFi) and even to house cryptocurrency exchanges (e.g., Uniswap).

An important form of more sophisticated financial contracting arises around stablecoins. Stablecoins are digital assets designed to maintain a stable value, typically by pegging them to a reserve of assets or employing algorithms to manage their supply. There are three primary types of stablecoins:

1. Fiat-collateralized stablecoins: These stablecoins are backed by reserves of fiat currency, such as the US dollar, euro, or other national currencies. For every stablecoin issued, there is an equivalent amount of fiat currency held in reserve by the issuer. Examples include Tether (USDT) and USD Coin (USDC).
2. Crypto-collateralized stablecoins: These stablecoins are backed by a reserve of other cryptocurrencies, often requiring over-collateralization to account for the price volatility of the underlying assets. Smart contracts are used to manage the collateral and ensure the stability of the stablecoin's value. MakerDAO's DAI is an example of a crypto-collateralized stablecoin.

[2] Note that this right distinguishes crypto-currencies from other digital assets such as airline loyalty points. Such points can be exchanged but there is a limit on who and for what purpose those rights are transferred. A closer analogue are casino tokens that can be exchanged for fiat currency at a fixed rate. See Halaburda and Gans (2015) for a more extensive discussion.

3. Algorithmic stablecoins: These stablecoins are not backed by any collateral. Instead, they employ algorithms to automatically adjust the stablecoin's supply based on market demand, aiming to maintain a stable value. Examples include Ampleforth (AMPL) and Basis Cash.

Such stablecoins overcome a significant issue with other crypto-currencies, exchange rate variability. By pegging to a fiat currency or basket of such currencies (as was proposed by the Diem Association), agents can hold and trade in crypto-currency without the associated exchange rate risk. However, as we will discuss below, there have been issues with regard to whether stablecoins can really be stable without a regulatory structure to ensure compliance and other practices related to banking in general.

Crypto-tokens can have associated rights, in addition to transferability, that allow for interactions between agents. Decentralized Autonomous Organizations (DAOs) give token-holders rights over the functioning of a smart contracting environment. Commonly, these are policy proposals and voting approval mechanisms where participation rights are conferred on token-holders. Such DAOs can, therefore, be governed without the need for a centralised intermediary. The MakerDAO, mentioned above, serves as a notable example of a DAO in action, which governs the creation and management of the DAI stablecoin. By employing a decentralized network of participants who collectively vote on decisions, MakerDAO ensures that DAI maintains a stable value pegged to the US dollar. This innovative approach not only mitigates the risks associated with centralized decision-making but also empowers the community to actively shape the direction and future of the project. More recently, a broader set of rights associated with tokens have given rise to web3 applications. These are applications that promote user privacy, data ownership, and equitable value distribution. Uniswap, a decentralized exchange (DEX) built on the Ethereum blockchain mentioned above, is an illustrative example of a web3 application. It enables users to trade cryptocurrencies and tokens directly from their wallets without the need for a centralized intermediary. In this way, Uniswap affords potential security and privacy benefits.

A final class of crypto-tokens that have emerged are non-fungible tokens or NFTs. These are tokens that involve rights that are not equivalent across tokens. While these include a right to transfer, an NFT often has an associated right that can be evoked in the real world to represent ownership, authenticity, and provenance of a wide range of items such as art, collectibles, virtual goods, and more. NFTs can provide a decentralized and tamper-proof way to verify an item's uniqueness and ownership. Each NFT has a distinct identifier and cannot be exchanged on a one-to-one basis like cryptocurrencies.

A real-world example of NFTs is the digital art market, where artists create and sell their artwork as NFTs. One famous instance is the artwork *Everydays: The First 5000 Days* by digital artist Beeple, which sold at a Christie's auction for a record-breaking $69 million. By tokenizing their art as NFTs, artists can potentially ensure their works' provenance and retain royalties from future resales. At the same time, collectors gain verifiable proof of ownership and the ability to trade these unique assets on various NFT marketplaces. That said, most NFTs confer rights to digital content without necessarily excluding others from consuming that context. In that sense, they are a certificate of ownership, and it is only that certificate that is scarce. Broader applications of NFTs look to extend rights to other activities – such as club membership or concert tickets – that may provide a more secure contractual foundation (Kaczynski and Kominers, 2021).

For crypto-tokens to have a rival and scarce nature, they are all generated on blockchains. Blockchains are a form of distributed ledger where a set of nodes both holds the record of ledger entries as well as updates those entries as rights are exercised. In principle, such ledgers need not be distributed and can be held by a single entity. This is actually what technically banks and other financial institutions do. However, it is argued that blockchains can provide transparency as to the protocol rules and also a greater level of immutability so that the ledgers and protocol rules cannot be tampered with by any actor or a relatively small subset of actors. Thus, while a centralised ledger may technically be subject to attack through a single point of failure, blockchain ledgers require an attack that targets many nodes simultaneously.

Not surprisingly, the major attack that needs to be thwarted in the context of blockchains issuing crypto-tokens is an attack that diminishes the right to transfer those tokens. A double-spend attack involves someone transferring a token and then denying the recipient the ability to exercise a similar right by returning the token to the control of the original holder. It is the equivalent of handing someone a counterfeit dollar bill or paying with a check that will bounce. While for fiat currencies, these issues are resolved via centralised legal institutions, many blockchains are designed to simply make it too costly to mount a double-spend attack in the first place. For Bitcoin, such an attack requires, at a minimum, that one single agent controls more than half of the nodes in the network. But even there, such attacks are less likely the longer agents wait to finalise transactions involving payments in bitcoin. Thus, in practice, transactions are not considered final immediately as they are, say, in the Visa and Mastercard networks. It may take from ten minutes up to a few hours, depending on the crypto-token, before agents consider a transaction final and free from the threat of a double-spend attack.[3]

If blockchains are more difficult for an attacker to take control of, the cost of this security is that effort must be expended to ensure that all of the different nodes in the network agree with one another over the state of the distributed ledger, a virtual machine (if any) and the underlying protocol code. Blockchains attain consensus through a communication game (Abadi and Brunnermeier, 2018; Halaburda, He and Li, 2021). This usually involves transactions or messages being publicly broadcast by agents and then assembled into blocks by nodes. One node is selected to become the block proposer, and then other nodes accept this proposal or not. In a network with a fixed number of known nodes (a permissioned network), it is possible to create protocols that allow consensus to be reached relatively quickly. When any agent can become a node on the network (i.e., in a permissionless network), achieving consensus is more difficult. However, Nakamoto (2008) proposed the longest chain rule to achieve coordination across nodes, while others use a technique from computer science based on Byzantine Fault Tolerance (Buchman, 2016). The details need not concern us here except to note that achieving consensus while trying to ensure a network is secure generally means that individual transactions both take more time and are costlier to process than their centralised counterparts.

Market Failures

Interestingly, much of the policy discussion with respect to the regulation of crypto-tokens has taken place without the specific identification of market failures such regulation would be

[3] The potential limits in security are explored by Budish (2022) and Halaburda et.al. (2022). See Gans (2023) for a more comprehensive overview.

designed to address. For this reason, it is appropriate to consider potential market failures surrounding crypto-tokens.

Payment efficiency

The main use case thus far for crypto-tokens is as a means of payment via crypto-currencies. In that respect, comparisons have been drawn between the payment efficiency of blockchain-based networks versus traditional payment networks. In terms of convenience, Bitcoin can only process 4.6 transactions every second, while the Visa network can process over 1,700 transactions per second.[4] Moreover, according to the Cambridge Center for Alternative Finance (CCAF), Bitcoin currently consumes around 110 Terawatt Hours per year, or roughly equivalent to the annual energy draw of small countries like Malaysia or Sweden.[5] This amounts to around $8 billion spent per year.[6]

Many point to such electricity consumption as a potential market failure due to the carbon pollution that is associated with electricity generation. However, it should be noted that this is associated with most electricity generation, and Bitcoin consumption is 0.55% of the global amount. As Bitcoin mining involves the voluntary choices of miners to consume electricity, it does not seem appropriate to distinguish Bitcoin mining from other electricity-consuming activities. That is, the market failure is broader than Bitcoin alone and in of itself does not provide a rationale to intervene to suppress Bitcoin mining. Moreover, Bitcoin mining is not location specific as it can be provided almost anywhere in the world and, therefore, will be located to minimise mining costs. Thus, Bitcoin and other cryptocurrencies based on Proof of Work play a role in arbitraging local differences in electricity prices. This means that if Bitcoin mining were prohibited, then global electricity consumption would fall but not to the full extent of that used by Bitcoin mining as other lower-value uses of electricity will become economic again in many areas.

What is of more interest as a potential market failure is whether the market for payments works to ensure that payment processing costs are at the lowest possible level. One reason why this might not be the case is due to network effects. If merchants (or conversely, consumers) favour one form of payment, it can be difficult for other payment networks to emerge and compete for those transactions. In this situation, it is entirely possible that a new payment network that could be built on a new, more efficient technology may be unable to gain traction due to the network effects that drive merchants and consumers towards incumbent networks. Thus, in the crypto-currency space, if, say, Proof of Work is less efficient than newer protocols based on Proof of Stake (which consume very little electricity), network effects may prevent merchants and consumers from coordinating their transactions on a more efficient network.

That said, in 2022, the Ethereum network moved from Proof of Work to Proof of Stake without any downtime for the network. This was a planned and coordinated change by a set of individuals that might be called ‘movers and shakers’ on that network (Akerlof and Holden, 2016). This suggests that it is possible for individual cryptocurrency networks to change their protocols to move towards more efficient payment processing. This was achieved without any government

[4] Visa vs. Cryptocurrency: Which Is Better? - MUO. https://www.makeuseof.com/visa-vs-crypto/ Accessed 3/21/2023.

[5] Electricity needed to mine bitcoin is more than used by 'entire .... https://www.theguardian.com/technology/2021/feb/27/bitcoin-mining-electricity-use-environmental-impact Accessed 3/21/2023.

[6] Using a rate of 5 cents per kilowatt hour.

intervention. It is unclear whether the same move might be possible for networks without a referent source of leadership (such as Bitcoin).

Information asymmetries and market safety

Another set of market failures in the context of crypto-tokens might arise from information asymmetries in markets for crypto-tokens. Information asymmetries may lead to markets with thin transactions or to other behaviour that may make transacting unsafe. These factors are known to make it challenging to create markets compared to a situation where information asymmetries are not present (Roth, 2008).

Interestingly, at one level, crypto-tokens, when they reside on public blockchains, might be less susceptible to the consequences of information asymmetries. The code is disclosed so that anybody can run it, and the ledger of transactions is kept public and, by design, is difficult or impossible to change after the fact. Thus, information asymmetries that arise because a provider has a hidden balance sheet or ledger of transactions would not be present in public blockchains. In this respect, there is potential for blockchains to reduce the costs of verifying aspects of transactions taking place there (Catalini and Gans, 2020).

Earlier, it was noted that crypto-tokens could be minted and also transferred. With respect to each of these activities, information asymmetries can create inefficiencies. Perhaps the clearest act of minting tokens arises when a crypto-token is first introduced and are allocated to agents. This was most apparent in the fundraising model termed initial coin offerings (or ICOs). In an ICO, a business creates tokens with rights that include transferability but also other aspects – for instance, a promise that purchases of goods and services supplied by the business will only be possible using those crypto-tokens. The idea is similar to a pre-sale of products as occurs in crowdfunding platforms such as Kickstarter. As with those platforms, it is often the case that the initial tokens allocated are in exchange for a price significantly lower than the price expected to emerge in subsequent exchanges. However, for ICOs, this creates a potential issue as the promise to create a venture and products that would be priced in the market at a high value is difficult to evaluate. The promise might not be fulfilled. Or alternatively, the market potential of the resulting goods and services might be over-claimed (Catalini and Gans, 2018). This is the same set of issues that arise in the ICO's inspired traditional funding model, the initial public offering (or IPO). Put simply, the issuers of either coins or shares may have more information than purchasers. The net effect of such information asymmetries is, in theory at least, a reduction in the total amount of funds that can be raised in this manner.

A distinct set of issues can arise with respect to the exchange of crypto-tokens. When exchange markets are thinly traded, they can be subject to various tactics whereby sellers of tokens engage in coordinated activities to convince potential purchasers that tokens have a higher value than their current market price. Factors such as wash trades or pump-and-dump schemes, are short-term, costly actions that some holders of tokens might engage in to convince others that the price of tokens is set to or will continue to rise (Halaburda et.al., 2022). In traditional securities markets, such activities are prohibited by exchanges and may impact the ability of participants to trade on them. The same can be true of crypto exchanges. However, these exchanges often conduct trades that are off-chain and, therefore, are potentially not as transparent as examining those trades taking place on a public blockchain. Once again, the fact that some agents on one side of an exchange market may have more information as it relates to price signalling can make exchange markets unsafe for other agents.

It was for these reasons that the class of cryptocurrencies called stablecoins emerged. A stablecoin is a crypto-currency that is designed to trade at a fixed rate with respect to a fiat currency. The goal is to create a digital asset that is less volatile than traditional cryptocurrencies like Bitcoin or Ethereum, making it more suitable for use in transactions, remittances, or as a store of value. One type of stablecoin achieves this parity by keeping one hundred percent of fiat currency given to it in exchange for tokens as a reserve. The difficulty, however, is that the promise to keep one hundred percent reserves may not be transparent to market participants or auditors. This may make it difficult to maintain the value of stablecoins as a lack of confidence can lead to a run on those stablecoins (just as there might be a run by depositors at a bank). Moreover, even when subject to audit, reserves are often held in interest-bearing accounts at traditional banks or in the form of holding of government bonds. In 2023, however, when there were concerns over the health of Silicon Valley Bank, the stablecoin, USDC, lost its peg to the US dollar briefly, as many of its reserves were held as deposits in that bank. Moreover, even government bonds can be an issue if too many stablecoin holders want to exchange back into fiat currency at a time when those bonds may be trading lower because of temporary changes in interest rates. In this respect, there is a fragility that, while related to informational issues, is also something that often accompanies banks (Diamond and Dybvig, 1983).

Another type of stablecoin is one that maintains its peg to fiat current through the use of an algorithm. These stablecoins use algorithms and smart contracts to adjust their supply in response to market fluctuations automatically. This is achieved by having a stablecoin pegged to, say, one US dollar, another token held as collateral or as a reserve and smart contracts that control the minting, burning and adjustments for the stablecoin and the other token. The algorithms adjust the stablecoin's supply by either increasing or decreasing it based on the price deviation from the target peg. If the stablecoin's price is below the peg, the algorithm may contract the supply (burn tokens) or introduce incentives to buy and hold the stablecoin. If the price is above the peg, the algorithm may expand the supply (mint new tokens) or incentivise users to sell the stablecoin. The problem here is that there is the potential for a destabilising spiral that makes it impossible to maintain the peg (Catalini et.al., 2022). One example of an algorithmic stablecoin failure is the collapse in May 2022 of LUNA token, a native token used to collateralise the Terra (UST) stablecoin (supporting an ecosystem that was the third largest behind Bitcoin and Ethereum). As LUNA's price began to fall, a negative feedback loop was created, with users selling their Terra and LUNA tokens, causing the prices to plummet even further. This eventually led to the collapse of the Terra stablecoin's peg and the rapid decline in the value of the LUNA token. As is often the case with these things, it was likely smaller holders and those with less financial knowledge that incurred the largest losses (Liu, Makarov & Schoar, 2023).

One final issue with respect to market safety arises with respect to the exchange of crypto-tokens. This is the issue of front-running. One form of front-running occurs when traders take advantage of lags between the time a transaction is proposed and when it actually is confirmed to a block to front-run the trade on crypto-exchanges (Daian et.al., 2020). This involves a contest for priority that is potentially captured by nodes in the form of higher transaction fees. Such arbitrage front-running creates a challenge for those trading crypto-currencies. Of more concern is so-called liquidation front-running. This impacts smart contracts when bots can front-run requests for payment associated with smart contract performance, substituting their own address and draining smart contract wallets before legitimate claimants can do so. Absent changes to the smart contracts themselves or the use of encryption, such as front-running, can completely eliminate smart contract viability (Gans and Holden, 2023).

Solutions to such problems are often left to more centralised exchanges that impose and enforce certain trading rules that may make the exchange of crypo-tokens safer. However, while there are several examples of exchanges that have emerged to process a significant volume of crypto transactions, like many of the other elements of the crypto-token sphere, these have not been subjected to regulation that covers the exchange of securities (for instance, by locating in jurisdictions with weaker regulatory oversight). The end result, perhaps most emphasised by the collapse of the FTX exchange and associated entities in 2022, is that exchanges do not appear to solve these issues of market safety organically.

Criminal activity

Finally, it is important to mention an aspect of crypto-currencies that is the opposite of market safety – its potential use as a means of payment for illegal or criminal activities. One challenge criminals have in conducting transactions is that there is a lack of contract enforcement. Consequently, transactions usually need to use cash as a means of payment which is difficult when payment quantities become large. Crypto-currencies offered a potential way of transacting without the need for cash. Moreover, their perceived anonymity was seen as a way to launder money without a trace. This has made them an attractive payment instrument for hackers placing ransomware in computer networks (and demanding cryptocurrency payments to avoid that software causing major damage). However, the public nature of the blockchain has more recently turned out to be a hindrance to such activities (e.g., with the deployment of Chain Analytics). Nonetheless, this form of market safety is itself a challenge for law enforcement and consequently could be argued to be a source of social inefficiency arising from crypto-currency exchanges.

Regulatory Instruments

Having examined potential market failures associated with crypto-tokens, we can now turn to examine the regulatory instruments that are available to mitigate their harmful impacts, if any.

Prohibition and Taxation

One obvious regulatory instrument is to ban cryptocurrencies. Several countries have done this, most notably China but also Algeria, Bangladesh, Egypt, Iraq, Morocco, Nepal, Qatar and Tunisia. Other countries have implicitly banned cryptocurrencies by prohibiting banks and financial institutions from dealing in them.[7] The rationales for such prohibition usually have to do with the use of crypto-currencies for illegal or criminal purposes, and competition with fiat currency (see Gorton and Zhang, 2022). That said, because many crypto-currencies operate on open and permissionless blockchains, it is not clear how effective the prohibitions are (Chen and Liu, 2022).

Relatedly, several jurisdictions, including those above, have opted to prohibit the mining of crypto-currencies. The rationale for this is a combination of environmental concerns arising from carbon and other pollution as well as a desire to keep electricity prices for other consumers low. In May 2023, the US White House proposed a 30 percent tax on the electricity bills of crypto-mining.[8] This tax was a blanket one and was not targeted, say, at mining operations using

[7] Countries Where Crypto is Legal (and Illegal) | Money.com. https://money.com/cryptocurrency-legal-status-by-country/ Accessed 3/22/2023

[8] https://www.whitehouse.gov/cea/written-materials/2023/05/02/cost-of-cryptomining-dame-tax/

electricity generated more intensively via fossil fuels. Consequently, it is unclear whether such arrangements will lead to significant changes in global pollution from crypto-mining (unless enacted globally) or what the incidence might be. For instance, energy producers have proposed using crypto-mining to under-write new developments in renewable energy production (Carter, 2021). A blanket tax might deter these investments.

Securities Law

A significant amount of discussion has been centred around the use of existing securities law to regulate crypto-tokens. This has been spurred on by regulators such as the SEC, who have sought to bring crypto-currencies under existing laws. But there is a broader issue of whether new laws need to be drafted to deal with the specific characteristics of crypto-tokens.

Securities law is aimed at overcoming the problems arising from information asymmetries. These laws achieve this by establishing rules and regulations that ensure the disclosure of relevant, accurate, and timely information about financial instruments and the companies that issue them. It is instructive to note that securities law is often a complement to other laws, such as those that criminalise fraud. Fraud laws are often only triggered when there are claims from securities issuers that are false or when key information is omitted, which results in others taking actions that are harmful or damaging to them. By contrast, securities law identifies a class of assets that are required to make certain disclosures and to do so truthfully. In this way, securities law can be enforced at the point claims are made rather than ex post after damage, if any, is realised. From this perspective, they can be seen as directly confronting the existence of information asymmetries rather than being reactive.

The main question with respect to crypto-tokens is whether they should be registered as securities at the point at which they are created. Not only would this require disclosures to be made at the time crypto-currencies are issued (both initially and perhaps through ongoing minting), but it would also prevent further tokens from being issued in a manner that might devalue the tokens already held by token-holders. That said, in principle, the total quantity of tokens can be managed by transparent code on blockchains. Thus, the focus has been on the information provided by token issuers.

From this perspective, when tokens are offered to the general public as part of an ICO, as the purpose of that offering is to raise funds for a venture, this would appear to make them a security in the eyes of security law – at least, at that stage. That is, they are covered by the Howey Test as they represent securities covered by an investment contract.

The Howey Test is a legal framework used in the United States to determine whether a particular financial instrument or transaction qualifies as an "investment contract" and, therefore, falls under the purview of securities law. The test originated from the U.S. Supreme Court case,[9] which established a set of criteria to assess whether a given transaction constitutes a security subject to SEC regulation. The Howey Test comprises four main elements, and all must be met for a transaction to be considered an investment contract:

1. Investment of money: The transaction involves an investment of money or assets by the investor.

[9] SEC v. W.J. Howey Co., 328 U.S. 293 (1946),

2. Common enterprise: The investment is made in a common enterprise, meaning that the investor's funds are pooled with those of other investors, or the success of the investment depends on the efforts of a group or third party.
3. Expectation of profit: The investor has a reasonable expectation of profit from the investment, which may include capital appreciation, dividends, or other forms of financial returns.
4. Profits derived from the efforts of others: The investor's profit is primarily dependent on the efforts of a promoter, third party, or other individuals responsible for the success of the enterprise, rather than the investor's own efforts.

If an asset satisfies the Howey Test this triggers registration, disclosure, and other regulatory requirements. More specifically, those assets that satisfy the test are ones where there are advantages to ensuring that information asymmetries are dealt with upfront. In so doing, market safety is preserved and so this can actually promote transactions and investment.[10]

The difficulty of applying the Howey Test with respect to crypto-tokens is that once those tokens are used as a means of payment for goods and services or are used to exercise certain control rights, they may cease to satisfy the conditions of the Howey Test. Most notably, there may be no single or small group of agents that could be characterised as promoters of the token by supplying effort that, if expended, could increase the value of that token. Indeed, the SEC specifically identified bitcoins and ether as tokens that were not securities after 2018. The argument was that the network was sufficiently decentralised.

> *But this also points the way to when a digital asset transaction may no longer represent a security offering. If the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract. Moreover, when the efforts of the third party are no longer a key factor for determining the enterprise's success, material information asymmetries recede. As a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful.*[11]

For Bitcoin, by this argument, it was apparently never a security while Ethereum was when it was part of the first ICO in 2015 but not by 2018. Interestingly, the argument seems to really be that the network is not centralised, and there is no active promoter or promoters that have sufficient impact on value that can be identified. Without that, there is no agent that has information that others do not have or if they do, that information cannot be used to disadvantage others.

In reality, there is a large set of factors that might determine whether a token is a security or not.[12] To the untrained legal eye, it appears that if a token is used to transact for goods or services,

[10] The Reves Test arises from a more recent court case than Howey (Reves v. Ernst & Young, 494 U.S. 56 (1990)) and may also have an impact on the classification of crypto-tokens.

[11] https://www.sec.gov/news/speech/speech-hinman-061418

[12] When you read through the SEC's staff advice (https://www.sec.gov/files/dlt-framework.pdf) there is a sense in which whether a token is a security or not depends on, what Australians would call, "the vibe of the thing."

then it is not a security. Otherwise, it might well be. This might mark the change at the point where the token is first used for purchases of those goods and services.

However, what is harder to assess is the notion that a token might morph from being a security to not being a security. That is, the sale of a token at one time might require registration and disclosures by an active participant, but the sale of the same token at another time might not. Where the change in legal status occurs might be difficult to assess. That said, perhaps taking a market failure approach, one sale might involve information asymmetries that are consequential while another might not.[13] Regardless, the SEC view is yet to be fully tested in the US courts, so uncertainty remains.

Banking Regulation

Stablecoins emerged as a counter to the highly volatile nature of crypto-currency exchange rates. For non-algorithmic stablecoins, what made them stable was that they were purported to be one hundred percent backed by deposits in traditional banks and holdings of government bonds. This was also the principle behind the stablecoin proposed by the Diem (formerly Libra) Association backed by a number of businesses and organisations.[14] However, Diem sought regulatory approval prior to launching their stablecoin. Having not received that approval, that stablecoin was never launched and the Associated disbanded.

It is unclear why regulators were loath to provide conditions under which a privately launched stablecoin could be given official sanction. The benefits of this would give such tokens what Gorton and Zhang (2021) refer to as a "no questions asked" (or NQA) property. This is a property that most fiat (or sovereign) currencies have as well as deposits issued by banks and other financial institutions. This property also is argued to apply for holding of government bonds. When users hold such assets, they do not need to investigate or form beliefs over the stability of their value. They can safely hold and accept such assets without asking questions about them.

That said, the NQA property is an equilibrium property. For fiat currencies and financial institution deposits alike, there can be reductions in value. Even for government bonds, if there is a tightening of monetary policy, the liquidation value of bonds can fall. What supports the equilibrium is that governments and central banks stand ready to support the value of such assets should there be a loss in confidence. For the banking sector, this support comes as a quid quo pro for regulations that require those institutions to hold reserves of cash, deposits with the central bank and even government bonds. In other words, their ability to create NQA assets comes with a check on the quantity of those assets that can be created.

Stablecoins, to achieve the NQA status, have self-regulated to, in many cases, holdings of one hundred percent reserves. Thus, they represent assets that are not part of fractional reserves but are potentially fully backed. All that stands between them and other NQA assets is government sanction. This might resolve issues of compliance with their own self-regulation that has plagued

[13] The SEC statements also leave open the possibility that a token might morph back from a non-security to a security. For instance, as already noted, Ethereum in 2022 made a significant change from Proof of Work to Proof of Stake. That move was planned for, worked on and then promoted and coordinated by a relatively small group of people each of whom likely had some significant holdings of ether. Moreover, by making Ethereum less reliant on energy, it might be more attractive for use by others and so there would be some expectation that it would have a high value following the change and certainly a lower value if the change was mismanaged.

[14] More precisely, Diem proposed to hold reserves in a manner that would have been akin to a narrow bank (Catalini et.al., 2022).

many stablecoins. Nonetheless, there appears to be no reason, in principle, that stablecoins could not become part of the official monetary sector (Gorton and Zhang, 2021). However, to date, governments have been unwilling to admit them into the official sector.[15]

Tax Treatment

A final class of regulatory instruments that impact crypto-tokens is their tax treatment when such tokens are exchanged. For standard fiat currency exchanges, if the currency is held for the purpose of purchasing goods or services (say, while visiting another country), any appreciation is not subject to income or capital gains tax. If foreign exchange is held for speculative reasons, it is subject to taxation.

For crypto-currencies, the same distinction applies in many countries. However, there is some uncertainty in this regard because so few transactions involving crypto-currencies involve the purchase of goods and services. Thus, if fully enforced, the tax treatment of crypto-currencies can have a substantial impact on the transaction costs associated with trading. As with the grey areas regarding whether a crypto-currency is a security or not, uncertainty over tax treatment creates issues for the development and use of crypto-tokens.

Innovation Impact

The 2023 *Economic Report of the President* reviewed the state of the digital asset industry which includes crypto-tokens of the type examined here. They concluded that:

> *Although the underlying technologies are a clever solution for the problem of how to execute transactions without a trusted authority, crypto assets currently do not offer widespread economic benefits. They are largely speculative investment vehicles and are not an effective alternative to fiat currency. Also, they are too risky at present to function as payment instruments or to expand financial inclusion. (p,277)*

For a set of technologies actively developed since 2008, this is a somewhat damming conclusion. That said, they did not rule out future developments. They wrote, "it is possible that their underlying technology may still find productive uses in the future as companies and governments continue to experiment" with distributed ledger technologies. Somewhat ironically, they also believed that some crypto-tokens were here to stay despite their apparent lack of utility.

The lack of applications that have been developed and seen adoption at scale leaves open the issue of whether this is driven by some fundamental limitations of the technology or instead as a result of regulatory issues. To that end, it is useful to remind ourselves of the features of crypto-tokens on distributed ledgers that so many have seen as a likely foundation for innovation.

1. *Security*: while various hacks and missteps by ventures using the blockchain suggest that it is insecure, the fact that, for the most part, well-designed blockchain protocols have proven very secure in protecting the ledger itself from attack and disruption. In that regard, the security provided, while not necessarily inexpensive, is readily available to entrepreneurs to utilise without having to construct and invest in secure

[15] Gorton and Zhang (2021) suggest that an alternative would be for stablecoins to be issued by banks themselves.

information technology systems or having an established reputation for security. Thus, security is a feature open to entrants at a level only incumbents generally are able to have available. This provides avenues for innovation and competition.

2. *Interoperability*: for blockchains that provide a virtual machine, there is significant interoperability between payments or accounting rails and other information technology services. While many have postulated coding smart contracts as a potential route to innovation, the more basic notion of programmable money can allow for the development of simpler and more direct forms of payment that themselves can be made contingent on other digitised events. Once again, this offers the potential for innovations that take advantage of this interoperability, and in particular, its consequent transparency can allow code links between different organisations.
3. *Incentives*: having an accounting mechanism at the core of blockchains allows the provision of incentives directly in code. This enables a commitment to mechanisms that is often lacking in other centralised and non-transparent systems – such as those that govern, say, digital markets for advertisements. This would allow for innovations in the design of markets, the establishment of novel mechanisms to enhance trade possibilities and the use of incentives at a larger scale than is currently possible. This avenue has already been exploited by DeFi applications that seek to construct mechanisms for sophisticated financial transacting without the requirement for intermediaries to complete trades.

Therefore, it is important to recognise that, despite the potential lack of progress, the fundamental features of the blockchain that generated innovative enthusiasm and a plethora of experiments have not changed. Those opportunities largely remain.

Ultimately, regulation will impact innovation in the use of crypto-tokens. It should mitigate the risks and costs of financial innovation while promoting the benefits. Thus, it is instructive to examine the ways in which regulation might be impacting certain key aspects of innovations that may be contemplated or advanced.

Raising funds

Entrepreneurs face many challenges in financing their ventures, especially in the early stages. The uncertainty surrounding their ideas may force them to part with higher equity to outside funders, including angel investors and venture capitalists. It is perhaps for this reason that when entrepreneurs realised that they could mint and sell tokens upfront as a way of funding their ventures, ICOs became, for a time at least, a preferred path for entrepreneurs.

One set of advantages ICOs had for entrepreneurs is that they could market their venture to a wider set of investors without requirements for standard regulatory disclosures or even the use of legal counsel. While this did not necessarily mean that ICOs could be launched without any details of the potential use of funds acquired, it did mean that many of the purchasers of tokens were not sophisticated investors. It is for these reasons that eventually the seeming regulatory advantages were removed when securities law enforcers turned their attention to ICOs.

That said, there are other advantages of ICOs that may suit entrepreneurs and so there is perhaps scope for them within the bounds of securities law. First, ICOs force entrepreneurs to be very specific about the rights attached to tokens issued. The demand for those tokens once the venture's products are launched will, in turn, determine their exchange rates. Thus, the exchange value of tokens is a proxy for the realisation of demand. Thus, funding can be tied to demand conditions leaving costs fully under the control and responsibility of entrepreneurs. Second, ICOs do not necessarily require long-term constraints on a venture. For instance, if a token represents pre-payment for a venture's product, then it will be purchased by consumers in the short-run following commercialisation and then returned to the venture. This means that the payback for tokens could conceivably occur over a much short time frame than returns to equity investing that often require entrepreneurial exits in order to be realised (Catalini and Gans, 2018).

These distinctive features of tokens lead to the possibility that they might represent innovative ways of funding entrepreneurial innovation. In this respect, if regulation were to fully ban ICOs as a possible financing instrument, this may diminish this path for innovation in entrepreneurial financing.

Incentivising co-innovation

One of the uses of tokens is to provide incentives for the development of products and applications on multi-sided platforms (Bakos & Halaburda, 2018; Cong, Li & Wang, 2022). The idea is that when a platform is launched, an entrepreneur will want to have all of the pieces in place to build it through network effects; that is, to ensure one side of the platform is built out, which requires developmental effort and co-innovation by others. By vesting developers with tokens that will appreciate if the use of the platform rises, entrepreneurs can incentivise third-party agents without having to pay them directly upfront.

Seeding ecosystems requires solving difficult coordination problems and can be surrounded by considerable uncertainty. Developers are investing in the platform but are not directly funding the platform. Nonetheless, their success can depend on the platform's active promoter, and their development may be a combination of effort and their own funds. In that respect, there is concern that tokens issued for this purpose may be considered securities. This would represent challenges as the relevant disclosures may not be possible, given the level of uncertainty involved.

Once again, tokens can provide a means of stimulating innovation, but their role may come into conflict with existing laws that were designed to be applied for less novel ends.

Regulatory uncertainty

The operation of blockchain networks tends to be funded by the issuing or allocation of tokens to those performing network tasks. This bootstrapping has allowed those networks to be stood up very quickly.

Regulatory uncertainty, however, remains over the legitimacy of those arrangements. Securities enforcers have recently indicated that certain ways of staking tokens as part of Proof of Stake consensus protocols may violate securities law. This is because those staking tokens can earn additional tokens depending on the performance of network functions such as block proposal and validation. As becoming a node can require a sizeable stake, some nodes are themselves funded by a multitude of agents. In this respect, securities regulators are concerned that the stake and expected return comprise a fund rather than a key part of network operations.

As of the writing of this paper, there is considerable uncertainty with respect to these and related functions. As one possibility is that the staking is not possible, the viability and operation of blockchain networks can be directly at risk. This likely reduces the incentives for innovation in terms of blockchain protocols themselves. While not a novel aspect of issues with regulation, regulatory uncertainty has been considerable in the blockchain space, and there is a need for clarification of what the laws applied to blockchains actually are in many jurisdictions.

Conclusion

It is not unusual for new technologies to be accompanied by what might be charitably called "a mess" because it falls within the cracks of government regulation or, at least in its early stages, is shaped by those who pretend the rules do not apply to them. We saw this with ride-sharing, which eventually morphed its way into new regulatory arrangements. And we are currently seeing this with artificial intelligence, which has come with it, concerns for privacy, copyright infringement to risks that are more existential.

Crypto-tokens, initially just a curiosity for computer scientists, have taken hold since the Global Financial Crisis of 2008, first with a group of enthusiasts looking to break existing institutions and then by many others who saw potential in its underlying blockchain technology or just a new way to make money. Suffice it to say, it captures imagination even if it does not seem to create value that many, including government regulators, can see. Matt Levine (2022) captures a reasonable modal view:

> *I don't have strong feelings either way about the value of crypto. I like finance. I think it's interesting. And if you like finance—if you like understanding the structures that people build to organize economic reality—crypto is amazing. It's a laboratory for financial intuitions. In the past 14 years, crypto has built a whole financial system from scratch. Crypto constantly reinvented or rediscovered things that finance had been doing for centuries. Sometimes it found new and better ways to do things.*
>
> *Often it found worse ways, heading down dead ends that traditional finance tried decades ago, with hilarious results.*
>
> *Often it hit on more or less the same solutions that traditional finance figured out, but with new names and new explanations. You can look at some crypto thing and figure out which traditional finance thing it replicates. If you do that, you can learn something about the crypto financial system—you can, for instance, make an informed guess about how the crypto thing might go wrong—but you can also learn something about the traditional financial system: The crypto replication gives you a new insight into the financial original.*

That said, the crypto-system is beset with scandals, fraud and the consequences of an unregulated free-for-all. This is deeply ironic because at the heart of blockchains is the type of security that usually only comes with the backing of a reasonable size military, and so it should have been its key output. Instead, the actions of people who have sought to use it have left us with a system that is anything but secure. The good news, for now, is that the operations, losses and machinations of the crypto-token ecosystem have very little impact on the rest of the economy.

> *A lot of people who put money into crypto were using their gambling money, and when their bets didn't pay off, they thought, "Ah, well, that was fun, too bad."*

> *Almost everything about the world of crypto screams "high risk" to anyone who knows at all what to look out for. And so, if you do know what to look for, you take your crypto risks with money that you can afford to lose and in ways that account for the risks. You don't take your life savings, lever them up 10 to 1, and invest everything in Dogecoin. (Levine, 2022)*

In that sense, even if what happens likes like good old financial crises being reinvented, they have been able to do that in a sandboxed way.

In the end, crypto seemed to offer many the opportunity to innovate without having to seek permission. But that has turned out to be either an illusion or a lesson depending on your point of view. But what gave so many the perceptions that crypto could just operate outside traditional institutions? Part of that is hubris. However, it is also the case that regulators and others did not pay much attention to crypto. Like those playing it, they saw it as a game others were playing. If it got out of hand, then their eye would be cast upon it.

That strategy was always going to be too little, too late. At the time of writing this review, the notion that the regulation of crypto-tokens is itself cryptic resonates even if the regulators claim that their existing rules and instruments can handle the job. The perception, however, is that the regulators just do not see what the value is from crypto-tokens and so see no harm in taking actions to shut it all down. To be sure, it is actually hard to find significant value thusfar with even the promise of simple disruptions such as international remittances yet to upend traditional ways of sending money. However, it is not about that. It is about what the signals are being sent to those who wish to continue to look for that value and also the signals being sent to anyone seeking to use technology to improve the operations of the financial system. The least controversial view of Nakamoto is that the existing system has room for improvement. Regulators have a duty to work out how to operate so that people feel safe to search for ways to innovate and explore the room.

References

Abadi, Joseph, and Markus Brunnermeier. *Blockchain economics*. No. w25407. National Bureau of Economic Research, 2018.

Akerlof, Robert, and Richard Holden, "Movers and shakers," *Quarterly Journal of Economics*, 131, no. 4 (2016): 1849-1874.

Bakos, Yannis and Halaburda, Hanna, The Role of Cryptographic Tokens and ICOs in Fostering Platform Adoption (June 30, 2018).

Buchman, Ethan. *Tendermint: Byzantine fault tolerance in the age of blockchains*. Masters diss., University of Guelph, 2016.

Budish, Eric B. "The economic limits of Bitcoin and anonymous, decentralized trust on the blockchain," *University of Chicago, Becker Friedman Institute for Economics Working Paper* 83 (2022).

Carter, Nic (2021), "Bitcoin Mining Is Reshaping the Energy Sector and No One Is Talking About It," *Coindesk*, 11 October 2021.

Catalini, Christian, and Joshua S. Gans, *Initial coin offerings and the value of crypto tokens*. No. w24418. National Bureau of Economic Research, 2018.

Catalini, Christian, and Joshua S. Gans. "Some simple economics of the blockchain," *Communications of the ACM*, 63, no. 7 (2020): 80-90.

Catalini, Christian, Alonso de Gortari, Nihar Shah, "Some Simple Economics of Stablecoins," *Annual Review of Financial Economics* (2022) 14:1, 117-135.

Chen, Conghui, and Lanlan Liu. "How effective is China's cryptocurrency trading ban?" *Finance Research Letters* 46 (2022): 102429.

Cong, Lin William, Ye Li, and Neng Wang. "Token-based platform finance," *Journal of Financial Economics* 144, no. 3 (2022): 972-991.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. "Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability," In *2020 IEEE Symposium on Security and Privacy (SP)*, pp. 910-927. IEEE, 2020.

Diamond, Douglas W., and Philip H. Dybvig. "Bank runs, deposit insurance, and liquidity," *Journal of Political Economy*, 91, no. 3 (1983): 401-419.

Fama, Eugene F. "Banking in the Theory of Finance," *Journal of Monetary Economics*, 6, no. 1 (1980): 39-57.

FINMA (Swiss Financial Market Supervisory Authority). (2018). Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs). Retrieved from https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/

Gans, Joshua S. (2021), "The Fine Print in Smart Contracts," in *Smart Contracts Technological, Business and Legal Perspectives*, Marcelo Corrales Compagnucci, Mark Fenwick & Stefan Wrbka (eds.), Hart Publishing: London, Chapter 2.

Gans, Joshua S. (2023), *The Economics of Blockchain Consensus*, Palgrave-McMillan: London, forthcoming.

Gans, Joshua S., and R. Holden, "A Solomonic Solution to Blockchain Front-running," *American Economic Association: Papers and Proceedings*, 2023.

Gans, Joshua S., and Hanna Halaburda. "Some economics of private digital currency," *Economic Analysis of the Digital Economy*, (2015): 257-276.

Gorton, Gary B. and Zhang, Jeffery, Taming Wildcat Stablecoins (September 30, 2021). *University of Chicago Law Review*, Vol. 90, Forthcoming.

Gorton, Gary B. and Zhang, Jeffery, Protecting the Sovereign's Money Monopoly (July 14, 2022). U of Michigan Law & Econ Research Paper No. 22-031.

Halaburda, Hanna, Zhiguo He, and Jiasun Li. *An economic model of consensus on distributed ledgers*. No. w29515. National Bureau of Economic Research, 2021.

Halaburda, Hanna, Guillaume Haeringer, Joshua S. Gans, and Neil Gandal. "The microeconomics of cryptocurrencies," *Journal of Economic Literature* 60, no. 3 (2022): 971-1013.

Halaburda, Hanna, Guillaume Haeringer, and Miklos Sarvary. *Beyond Bitcoin*. 2nd Edition, Springer International Publishing, 2022.

Kaczynski, Steve, and Scott Duke Kominers. "How NFTs create value," *Harvard Business Review*, 10 (2021).

Kocherlakota, Narayana R. "Money is memory," *Journal of Economic Theory*, 81, no. 2 (1998): 232-251.

Levine, Matt, "The Crypto Story," *Bloomberg Businessweek*, 13 October, 2022.

Liu, J., Makarov, I., & Schoar, A. (2023). "Anatomy of a Run: The Terra Luna Crash," *Working Paper*, No. w31160, National Bureau of Economic Research.

MAS (Monetary Authority of Singapore). (2020). A Guide to Digital Token Offerings. Retrieved from https://www.mas.gov.sg/regulation/guidelines/guidelines-on-digital-token-offerings

Mougayar, W. (2016). *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. John Wiley & Sons.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Roth, Alvin E. "What have we learned from market design?" *Economic Journal*, 118, no. 527 (2008): 285-310.

SEC (U.S. Securities and Exchange Commission). (2017). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Release No. 81207. Retrieved from https://www.sec.gov/litigation/investreport/34-81207.pdf

Swan, M. (2015). *Blockchain: Blueprint for a New Economy*. O'Reilly Media, Inc.

Walch, Angela. "The path of the blockchain lexicon (and the law)," *Rev. Banking & Fin. L.* 36 (2016): 713.

Zohar, A. (2015). Bitcoin: Under the Hood. *Communications of the ACM*, 58(9), 104-113.