Information Society Project
Yale Law School

DIGITAL FUTURE WHITEPAPER SERIES

The Death of Cryptocurrency

The Case for Regulation

Nicholas Weaver

December 2022

Contents

The Death of Cryptocurrency: The Case for Regulation

I. Introduction

Over the past decade, the cryptocurrency space has seen a huge growth in interest. Despite ten years of hype and a largely hands-off approach from regulators, however, the technology has not yet revolutionized payments or other parts of the financial system. The most ambitious attempted integration of cryptocurrency into the economy at-large thus far was a spectacular failure: even when El Salvador adopted Bitcoin as a national currency the project rapidly collapsed. Not only was the currency almost unused among the general population, but when it *was* used it did not actually involve cryptocurrency transactions. Cryptocurrencies will not and cannot form the basis of a revolution in our global financial system.

Despite the repeated failures of major cryptocurrency projects, the space is seemingly inescapable. Immense investments into cryptocurrency projects drive a hype cycle that keeps promising a set of revolutions that are not materializing.

All of which leads to a major question: Why? Why, despite such time and freedom to develop, have cryptocurrencies had so little impact on the financial system?

The answers are surprising. As I will argue throughout this essay, the truth about cryptocurrencies is that they fail to accomplish nearly every objective they purportedly were created to achieve. It may be that in the future, some new purpose for the cryptocurrency ecosystem will emerge that will justify continued investment and development of these technologies. But the catastrophic failures of nearly every major cryptocurrency project—including the recent bankruptcy of cryptocurrency exchange FTX—are not flukes.

Not only is the technology that underlies cryptocurrency not novel, these technologies are deployed in ways that will inevitably result in unstable products that are fundamentally at odds with the stated goals of the cryptocurrency and decentralized finance *raison d'être*: They do not work as currency or a store of value. They are neither trustless nor decentralized. They cannot create a new paradigm for the web, finance, and micropayments. They are less secure in practice and more prone to widespread fraud than our current financial system, and frequently result in irreversible consumer harm that could have been mitigated using traditional financial processes.

This paper argues that the very nature of cryptocurrency technology ensures that current cryptocurrency projects cannot actually succeed at their purported goals. Until and unless the cryptocurrency community develops new objectives, or significantly alters cryptocurrency technology to meet existing objectives, this mismatch between existing means and desired ends will forever relegate cryptocurrency to the novelty, speculative space that it currently occupies—good for a news headline but not for sea change in the financial system.

Behind the veneer of new technology, cryptocurrencies reflect old economic phenomena and paradigms; seemingly novel problems are addressable with existing regulations. Many such existing regulations have explicit "duck tests": if it looks like a duck, quacks like a duck, and swims like a duck, it's probably a duck. In most cases, the harms that cryptocurrencies can cause are directly addressed by these existing frameworks, should regulators both understand the technology and be willing to enforce existing regulations against new fact patterns.

My argument takes place in four high-level sections. I will begin with a discussion of the theory and practice of cryptocurrencies and other forms of "digital money," explaining in particular how cryptocurrencies function and what advantages they purport to have. Our society has used digital money for over a generation. The novelty of cryptocurrency occurs only in its exclusion of explicit intermediaries, creating a cash-like transaction process. At the same time, these same mechanisms make cryptocurrencies fundamentally unsustainable for payment systems.

Second, I will discuss the principle and practice of "decentralized" and "trustless" systems. In decentralized systems, there are purportedly no intermediaries who can exert control over the system. In "trustless" systems, it is presumed that the system is trustworthy without having to trust any individual entity. But these claims do not hold water: in reality, systems are neither decentralized nor trustless. As I will show, a few concentrated entities *must* be trusted for the system to work; these entities in turn can exert significant control over the system.

Third, I will discuss the theory and practice of "programmable money." Advanced cryptocurrencies like Ether (ETH) promise the ability to couple some amount of computation to a transfer, enabling the creation of new financial instruments. However, after two generations of experience in programmable money, it is clear that these products are distinctly inferior to our existing systems.

Finally, I will discuss the social aspects of the use of cryptocurrencies. New structures called "Decentralized Autonomous Organizations," or DAOs, are structurally similar to a joint-stock corporation despite supposedly novel voting mechanisms. The joint-stock corporation is a legal and regulatory structure that has existed for hundreds of years. A DAO which formally incorporates is simply a corporation, while a DAO which does not is a general partnership, complete with joint and several liability. Both can be and should be regulated under well-established corporate law rules.

This white paper concludes with a series of recommendations to policymakers, mostly focused on how existing regulations can apply, should apply, and in some cases have *already* applied to the space of cryptocurrencies. This includes regulating new issues of cryptocurrencies, the existing cryptocurrency exchanges, and the stablecoins. Such regulations should be imposed without fear of stifling innovation. As I will argue, there is, at root, no true innovation currently present to stifle.

II. The Theory of Cryptocurrency Payments and Digital Money

Our modern economy runs on digital money: our "money" consists of entries in ledgers maintained by trusted and regulated institutions. For decades we have used electronic

payments on a daily basis, using payment systems maintained by these regulated intermediaries.

We trust these institutions because they are regulated and backed by explicit government backstops like the Federal Deposit Insurance Corporation (FDIC). There are extensive regulatory frameworks that act to protect consumers and, in the end, the government and the national economy as well. In our existing system, consumers are strongly protected against fraudulent payments and against failing institutions.

These regulations also serve to protect the financial institutions themselves. Bank runs on regulated banks effectively no longer happen, as there is no need for a consumer to rush to the bank. So although the 2008 financial crisis resulted in many failing banks and cascading crises, consumers were largely protected from failures by regulated institutions. It was only the lesser-regulated shadow banks, such as the Reserve Money Market Fund or AIG, that experienced bank runs.

These trusted intermediaries also provide reversibility. In case of fraud or other problems, transactions can be undone for at least a limited period of time. This enables error mitigation, as a human can intercede and fix what would otherwise be a potentially catastrophic loss of funds.

There does exist a disadvantage to these regulated systems in that they require trusted intermediaries. Especially for payments, these intermediaries both collect transaction fees (for example, the net fee on a credit card purchase is roughly 1%-2%[1]) and also enforce numerous regulations about what is allowed or disallowed.

The major exception to this regime is physical cash. Cash can be passed from person to person without a third party needing to participate, collect fees, or enforce rules. But at the same time, cash has significant disadvantages: the lack of reversibility means that theft or errors are often unrecoverable, and the physical nature of cash places inherent limits on the medium.

Cash both requires physical counterparty presence and takes up a considerable amount of space. One million dollars in $100 bills weighs roughly 10 kilograms (22 pounds). So

although a million dollars can (just barely) fit in a briefcase, the resulting briefcase is heavy and needs to be exchanged in person.

Although we still think of cash as money, it is remarkably divorced from our primary payment channels. A business depositing cash has to invest in security, armored cars, and other expenses not present in other forms of payments. A bank will commonly charge 0.25% just for processing cash due to the physical inconvenience.[2] Our financial system is also rife with cash-specific regulations to protect those who use it and deter crime: for example, cash deposits over $10,000 are specifically reported by financial institutions who must file Currency Transaction Reports.[3]

The idea behind Bitcoin, the first major cryptocurrency, was to enable electronic payments that behave more like cash. In Bitcoin there purports to be no need to rely on trusted intermediaries. Bitcoin transactions, like cash, are irreversible—but unlike cash, they are electronic in nature.

Bitcoin, like any other electronic payment system, starts with a ledger of participants and their balances. But unlike a conventional payment system, the participants are only identified by their cryptographic public keys. This public key corresponds to a user's private key, which is simply a long random number. In Bitcoin's case, it is 76-digits long.[4] The private key is then used to create a corresponding public key, a random-looking number that is also some 76-digits long.

These two keys allow the creation of a "public key signature." The holder of the private key, who we might call Alice,[5] can take an arbitrary message and "sign it," producing yet another random looking, 76-digit-long number. Anyone else, who we might call Bob, can then take that original message, signature, and public key and use this to validate the signature. This validation confirms that the signature is applied to the original message and that only someone who knew the private key could create the signature.

This forms the foundation of a Bitcoin transaction, which is effectively a digital check signed by the sender. Thus for Alice to transfer 1.24 Bitcoin to Bob, Alice creates a digital check: "I, Alice's public key, pays Bob's public key the sum of 1.24 Bitcoin, with a transaction fee of 0.01 Bitcoin" and then cryptographically signs it. Now Bob can check the public ledger to see if the check is good and then seek to get it published in the ledger.

Once published, everyone now knows that the balance associated with Alice's key is now decremented by 1.25 Bitcoin and Bob's incremented by 1.24 Bitcoin.

The major difference between Bitcoin and previous systems is how the ledger itself is managed. In conventional electronic payments, the ledger is managed and validated by the trusted third parties: the bank, the payment processor, or other intermediary keeps a copy of the ledger and can validate and include transactions.

But Bitcoin seeks to eliminate the costs and benefits of the trusted third parties by instead managing the ledger publicly and collectively through what is known as the mining process.

Anyone can theoretically become a Bitcoin miner. Miners gather up the currently unvalidated checks, ensure that each check meets the rules,[6] and assembles a block of new checks. This block includes a pointer to the last block, creating the "blockchain" structure.

This system is not impenetrable: in particular, the system could be vulnerable to "double spending" attacks, where someone replaces an already recorded check with a new valid one. For example, instead of Alice's check to Bob, Alice could have the miners change history to instead include a check to herself.

The solution to this for Bitcoin is the proof-of-work system, which is designed to make the cost of double-spending significantly more than the potential benefit. Each block includes a large amount of useless work, but it is very easy to verify that the useless work was done. The amount of useless work is automatically tuned, so it takes roughly ten minutes for some miner to create the next valid block.

Anyone attempting to rewrite the last N blocks of history needs to do an equivalent amount of useless work to rewrite history. While this doesn't eliminate all possible double-spending, it does economically eliminate all double-spending where the benefit of the attack is less than the (time-consuming, expensive) work done in the interim.

The resulting system is a payment network where Alice and Bob no longer depend on an identified intermediary. Instead, they rely on the collective work of the miners to update the ledger. As a consequence, there is no single identifiable third party able to reverse or

block disallowed transactions. This is what cryptocurrency advocates mean when they speak about a "decentralized," "trustless" system.

III. The Practice of Cryptocurrency Payments

The irreversible design and volatile nature of most cryptocurrencies makes them unsuitable for use as a payment channel for either domestic or international payments. The inherent volatility of cryptocurrencies such as Bitcoin means that the recipient will, at some point, need to convert from the cryptocurrency back to local currency, which in practice is a huge drawback to the potential everyday use of a decentralized financial system. A receiver seeking to minimize this risk will conduct the conversion almost immediately.

The conversion to a government-backed currency to avoid volatility is why, although many companies have claimed to accept cryptocurrencies over the years, most do not actually accept cryptocurrency in practice. Instead they use a service that allows them to price their goods in dollars with an automatic conversion to present the price in Bitcoin or other cryptocurrency.[7] Then, when a payment is received, it is automatically converted to dollars.

This means that the counterparty has to convert dollars to Bitcoin for the system to balance. We will see later why irreversibility makes Bitcoin hard to buy, but even in the best case, this means that a real-word cryptocurrency transaction requires two currency conversion steps. Such currency conversion is generally expensive, as there are inevitably fees incurred in such conversions.

Transactions with two currency conversion steps can become significantly more expensive than conventional payment methods. Today, even an international transaction tends to at most involve one currency conversion, rather than the two that are demanded by the use of Bitcoin.

The irreversibility of cryptocurrencies also creates an incompatibility that makes cryptocurrencies hard to buy due to increased cost of transaction between buyer and seller necessary to increase safety where there are no trusted intermediaries. The normal financial system relies on trusted intermediaries being capable of reversing transactions to mitigate

problems. Thefts, bugs, and other problems can be undone if detected in time. Cryptocurrencies lack this critical feature. This is why cryptocurrency thefts, as a fraction of the available currency, are orders of magnitude more common and severe than thefts in the normal financial system.

The largest significant electronic bank heist, targeting the Bank of Bangladesh, managed to steal roughly $100 million.[8] Cryptocurrency hacks of similar magnitude are almost a monthly occurrence; indeed, in the largest cryptocurrency hack on record, of Axie Infinity's "Ronin Bridge," hackers stole over $600 million.[9]

This ease of theft is inherent in the very nature of cryptocurrency. Stealing $10 million in physical cash requires that someone break into a secure location and move 100 kilograms of physical paper. Stealing $10 million in a traditional bank transfer requires both breaking into the bank's computer and also quickly moving the money through a series of accounts to hide its origin, such that the victim's bank cannot undo the theft. Stealing $10 million in cryptocurrency controlled by a computer, on the other hand, requires compromising the computer but—critically—the victim can't recover the money.[10]

This creates significant friction in buying cryptocurrencies. Someone who wishes to sell cryptocurrencies cannot accept a conventional electronic payment. Instead they either have to have an established relationship with the buyer (to know the buyer poses an acceptable credit risk), accept cash, or accept an electronic payment and then wait for a few days.[11] This drives up the price of buying cryptocurrency as all three options (validating credit risk, accepting cache, or waiting) incur additional expenses not present in other payment systems.

Furthermore, the actual cryptocurrency transactions themselves can be surprisingly expensive.[12] In order to act as a limit on spam transactions, where someone creates a huge number of useless transitions that need to be validated, slowing down the transaction verification process, any given cryptocurrency allows only a limited number of transactions per block in the blockchain. When the desired number of transactions is below this threshold, transactions are nearly free. But if the desired transaction rate exceeds this threshold, then prices can spiral as a fee auction is used to select which transactions to process due to the inelastic supply of available slots.

Bitcoin is particularly limited in this respect. Due to an early decision to limit spam by restricting the block size to just one megabyte, the Bitcoin network can only process somewhere between three and seven transactions per second worldwide. In comparison, the typical load on the VISA network is 1,700 transactions per second, and VISA has tested the system up to 64,000 transactions per second.

During times of congestion, this can lead to the price for Bitcoin transactions reaching $50 or more. Other cryptocurrencies may have higher limits, which naturally leads them to be more vulnerable to spam. High congestion fees ensure that Bitcoin transactions can never be used for everyday, low-value payments. It is inconceivable that consumers would be willing to pay an extra $50 at the grocery store because they went shopping on a Saturday or Sunday afternoon.

Cryptocurrency advocates will insist that "layer-two solutions" exist for this problem. They will often point to the Bitcoin "Lightning Network," a protocol implemented on top of the underlying cryptocurrency, as an example of a solution. Unfortunately these don't solve the fundamental problem of limited transaction capacity.

Lightning works by creating a pre-funded payment channel between the user and a central relayer.[13] From there the user can issue or receive payments that pass through a chain of relayers to the recipient. Eventually, a user may close the channel and receive the Bitcoin back onto the main blockchain. Thus, the internal payments no longer need to be recorded on the central blockchain.

In creating, adding funds, and closing the channel, the user still needs to conduct a normal Bitcoin transaction. The Lightning network's ability to create or close channels is limited by Bitcoin's own transaction limitations. Therefore, Lightning cannot provide scaling as there is still a substantial limit on the number of channels that can be created, funded, or closed per second.

The one example where Bitcoin did scale to a significant number of transactions was in El Salvador, though it scaled, ironically, by not actually using Bitcoin to process payments.[14] The dictator of El Salvador, President Nayib Bukele, passed a law mandating that Bitcoin, along with the US dollar, would now be considered official currencies and merchants were

obligated to accept it. Along with the mandate came a phone application, the "Chivo Wallet," to enable El Salvadorian citizens to accept and spend Bitcoin payments.

Users were given 30 US dollars in Bitcoin when they signed up for a Chivo Wallet as a way of attempting to drive usage.[15] The system also included deep subsidies on gasoline when purchased with Bitcoin.[16] Critically, although there was an initial flurry of Bitcoin transactions, the resulting transactions didn't actually use Bitcoin's ledger or even the Lightning network.

Instead, Chivo acted like a decades-old centralized payment network: user balances were simply updated in Chivo's internal ledger, and Chivo acted as a trusted third party which processed transactions. In sum, the one attempt to deploy a cryptocurrency payment system on a national basis specifically did *not* use the cryptocurrency for most payments.

There was nothing decentralized or trustless about El Salvador's Bitcoin experiment. For the reasons described above, it is simply not conceivable for there to be a decentralized or trustless system that is capable of handling payments at-scale. Increased frictions inherent in the nature of cryptocurrency as alternative mechanisms to promote safety and security will inevitably make any cryptocurrency-based system worse at handling transactions than our current system—at least on an economy-wide scale.

There is one potential exception to this rule: the "stablecoin." A stablecoin purports to maintain a 1-to-1 value relationship with a conventional currency. There are actually three different types of stablecoins, which I will discuss in detail in section VIII, but the only viable sort, a "backed stablecoin," requires a trusted intermediary—the very thing cryptocurrencies are supposed to eliminate.

This trusted intermediary accepts conventional payments and issues a corresponding amount of the stablecoin. The stablecoin instruments can circulate on their own until someone else returns to the intermediary to receive the original amount of deposited money. Mechanistically it resembles nothing more than a nineteenth century "free-bank era" bank, just with cryptocurrency tokens instead of physical paper.

Of course, now that you have such a trusted intermediary, why can't that trusted intermediary simply maintain a trusted ledger to track everybody's balance?

If cryptocurrencies are inferior to and more costly than our traditional financial systems, what activities tend to occur with their use? Beyond speculation, cryptocurrencies serve as an effective payment channel for items which would not be processed by the normal payment channels, or where physical money is simply too bulky or restrictive to use.

Initially the primary use of Bitcoin for actual payments (rather than speculation) was the purchase of drugs on the Silk Road (launched in 2011) and subsequent hidden-service based markets. These markets at their peak conducted over $600,000 in sales a day.[17] Since annual US illicit drug sales are measured in the tens of billions, this means that the dark-net markets only represented a couple percentage points of the total sales in the US, showing that Bitcoin, even for illicit substances and with a decade of consumer experience, is not a significantly useful alternative to cash.

Currently, the primary illicit use for cryptocurrency payments is multi-million-dollar ransoms extorted by "big game ransomware" gangs. These criminal syndicates, commonly operating out of Russia or North Korea, are estimated to obtain billions of dollars in payments while doing perhaps ten times that in damage to the global economy.[18] These actors are blocked from conventional payment systems so Bitcoin and other cryptocurrencies represent the only method available to collect these ransoms. As such, I've previously described the ransomware problem as really a Bitcoin problem.[19]

In the end, despite a decade of hype and speculation, cryptocurrency has never served as a viable alternative for payments that the existing system processes. The problems inherent in volatile cryptocurrencies are simply fundamental to the design, while any viable stablecoin requires a trusted intermediary, the very actor cryptocurrencies were supposed to eliminate.

IV. The Theory of Decentralization and Distributed Systems

Cryptocurrency advocates claim that the underlying technology offers a huge advantage over existing systems through "decentralization," with hundreds or thousands of systems all acting independently but creating and maintaining a common view of the world.[20] They also claim that the result is "trustless" systems where you don't need to trust particular actors, but instead only the resulting system.

For a generation we have successfully built distributed (also sometimes termed federated) systems. In a distributed or federated system, we have a collection of named and identified actors. Within the system, these actors are explicitly trusted within their limited sphere of operation. In some cases, we only need to trust that a subset of the actors are honest, but in others we delineate where each entity is trusted, with authority within their bailiwick but no authority outside of it.

As an example, modern payment systems are a distributed system. In the Automated Clearing House system, each bank maintains its own set of customer balances and is trusted to act on behalf of those customers. Participating banks can then send messages to other banks, and because the banks are pre-identified and trusted, the system can efficiently transfer money between these known actors. Distributed systems critically expose the trust relationships: you have to trust your bank, the recipient's bank, and the intermediate payment processor for the system to work. These systems can scale to immense size.[21]

The major difference between decentralized and distributed systems is that decentralized systems forgo identifying and restricting who can participate. In a distributed system, the entities are all vetted and trusted to at least some degree, and these entities are also therefore identifiable and identified and have various rights and responsibilities. In a decentralized system, anyone can participate without needing to confirm their identity with some trusted party. This also contributes to claims that such decentralized systems are "trustless": a participant can be assured that the system will work even if some fraction of the unknown participants are bad actors.

V. The Practice of Decentralization

In the end, all decentralized systems rely on some form of a voting scheme to decide the current state of the world. Indeed, all such systems have some notion of the state of the world. If one party thinks "Alice paid Bob" is what should be recorded, but another thinks "Alice paid Carol" should be recorded, there needs to be a mechanism for all participants to end up agreeing. And in the end this usually requires some sort of vote: All the participants effectively vote on the question "Who did Alice pay?" and the majority vote wins.

The biggest problem faced by decentralized systems is thus the threat of what are known as "Sybils." A Sybil is simply a fake participant, where a single actor creates hundreds or even millions of fake participants to gain a larger share of any "one man, one vote" type system using a "vote early, vote often" strategy. Distributed systems do not face the same problem as the identification of the participants implicitly eliminates the possibility of Sybils.

Thus a cryptocurrency needs to rely on "proof of something" in order to limit Sybils by imposing a cost on each vote. The method pioneered by Bitcoin is "proof of work": the approval of a set of transactions includes a cryptographic hash.

Cryptographic hash functions take an arbitrary message and produce a smaller number, in this case a number that appears to be randomly chosen between 0 and approximately 10^{76}, so another 76-digit number. A key property of the hash function is that although it is deterministic (the same input will always produce the same output), if you change just a single letter in the input the output looks like a completely different random number.

So if a bunch of participants take an input, add on a little message, and repeatedly hash the value until one finds a combination of the input and their additional message where the hash ends with 18 zeros in base 10, this shows that the system as a whole probably had to compute one quintillion hashes just to find one that matched. While the operation of finding a matching hash is costly, anyone can verify that the resulting input and message match by conducting just a single hash.

This is used by Bitcoin to protect history or "the state of the world." If someone wants to present an alternate history as valid, they have to do at least as much (otherwise useless) work as was used to create the initial record of history. The implication is that would be so costly as to make creating that alternate history unworthwhile for an attacker. Unfortunately, this is not an efficient means of dealing with Sybils.

If an attacker can spend X over a fixed period of time to change history to gain Y dollars, they will do so if $X < Y$ and won't if $X > Y$. But the defenders have to be consuming X in that period of time whether or not they are under attack. As a consequence, proof of work can never be both efficient and effective: if X is low the system is vulnerable to attack, and if X is high there is simply a huge amount of wasted work needed to protect the system

24/7/365. There have been many variants on "proof of wasting X" in terms of cryptocurrencies but all end up suffering from the same flaw: proof-of-waste systems cannot be both efficient and secure.

Proof-of-work systems also inevitably converge into a system where a few entities control the majority vote of the network. This is due to basic economic competition: the more efficient entities (where wasting X resources is cheaper) will quickly dominate the market, expanding the share of resources they are wasting until they account for most of the available profit.

As of this writing, five entities control 75% of the vote on the Bitcoin blockchain.[22] These entities need to be trusted for the system to work properly as they possess an absolute veto over any transaction they might not desire to occur.

The largest proposed alternative, proof-of-stake, instead seeks to formally enshrine a plutocracy, as one's voting share is proportional to one's holdings of the underlying cryptocurrency. Although this doesn't have the efficiency issues with proof of work, it does make the system explicitly dependent on the trustworthiness of the biggest participants.

This problem is further compounded by the strong inequality in most cryptocurrencies. In the end a few participants, either early participants and/or major cryptocurrency exchanges, hold most of the available cryptocurrency. Thus in practice only a few participants, taken together, have the majority vote in such "decentralized" systems. Ethereum, which successfully transitioned to proof-of-stake, has over 50% (and thus the majority vote) of the network controlled by just four entities.[23]

Finally, a lot of "decentralized" cryptocurrencies actually are not decentralized in practice. Instead they use a structure where there is some set of trusted validators created at the start and these validators are the ones responsible for maintaining a coherent state of the world. Such systems are really just distributed systems, using the term "decentralized" to hide their actually centralized nature.

As discussed above, in all of these decentralized systems, trust relationships continue to exist but are hidden and obscured. Cryptocurrency participants need to trust the code that runs their wallets, the exchanges where they trade their cryptocurrencies, the miners who

maintain the public ledger, and the developers who code the cryptocurrency itself. In short, the number and type of trusted entities is actually *greater* than a conventional system, though each actor has *less* accountability due to a lack of formal regulation of these actors and the deliberate obfuscation of these actors' roles.

These actors have shown themselves unworthy of trust in the past. Flaws and bugs in cryptocurrency wallets regularly result in theft or loss.[24] Cryptocurrency exchanges have a long history of failing with little recompense for customers.[25] Cryptocurrency miners have deliberately distorted the process to the detriment of other participants,[26] and developers will change the code in ways that favor the developers over other users.[27]

The repeated bad behavior of actors necessary to a decentralized system results in systems that aren't actually "trustless." Most cryptocurrencies have a small cartel of miners or validators which can effectively control the system. Is there an actual benefit in "decentralization" when four to ten identifiable entities have a supermajority vote and can completely control the system?

VI. The Theory of "Smart Contracts" and Programmable Money

Another promise of the cryptocurrency space is to enable "programmable money": instead of simply having our money be a passive ledger, we can program actions to occur based on events. This claim neglects that we've had such systems for generations.

Just as society has had digital money for over two generations, our society has used programmable money for nearly as long. In 1975, what became the Vanguard 500 Index Fund was launched. Unlike previous mutual funds, where trades were directed by humans, the Vanguard 500 effectively implemented a small program to match the S&P 500 Index.

Since that time, Wall Street has launched thousands of systems based on programmable stock trading. An entire subindustry of high-frequency trading has sprung up, using computer programs for "picking up pennies from in front of a steamroller" to remarkable financial success. Our modern financial system runs on computer programs that use money as an input and do things on our behalf—there's nothing new about programmable money.

In theory, cryptocurrencies such as Ethereum, which enable "smart contracts," are intended to replicate the functionality that already exists within our financial system within the cryptocurrency space. A user can deploy a small program written in a domain-specific programming language that can interact with the underlying blockchain.

Backers of the cryptocurrencies claim that this can enable a whole host of new innovations, from "web3" to decentralized financial operations. In all this they promise both security and a lack of gatekeepers: no third party can interfere thanks to the widely distributed nature of the underlying cryptocurrency. They also promise to be more "democratic," as anyone can write such programs, rather than just the major participants in the financial markets.

VII. The Practice of "Smart Contracts"

In practice, these smart contracts have proven to be a disaster. Unlike the programmable money that runs our society, smart contracts have two massive defects: they run on an irreversible fabric and are open to the world for potential exploitation.

The first is subtle but critical. If a modern financial program experiences widespread failure, there is a strong possibility that transactions can be reversed if caught in time.[28] So although it is important for such code to be (mostly) free of bugs, at least some level of error can be tolerated as the reversible nature of modern financial systems enables bug remediation.

Such remediation is absent in smart contracts. If a smart contract has a bug that causes a loss of value, there is no remedy unless the underlying blockchain is updated to undo the effects. This has regularly resulted in multi-million-dollar losses, such as the case of the Parity multisignature wallet.

The Parity wallet, whose lead developer invented the smart-contract language used, was an attempt to secure the underlying Ethereum cryptocurrency by creating multiparty checks: an attacker would need to steal multiple keys to steal the cryptocurrency rather than one. Unfortunately there was a bug in the wallet where someone inadvertently

disabled the entire contract, locking some hundreds of millions of dollars' worth of ETH in a way that they can never be recovered short of Ethereum deploying a code update.

Not only is an irreversible fabric a natural target for theft, the "attack surface" of these smart contracts is vastly more open than other financial systems. Even with reversibility, a bank or stock exchange would not dream of opening up their infrastructure to allow anyone to attempt to hack the system. But the whole point of a smart contract is that it is public: anyone can see the compiled code, observe what it is supposed to do, and interact with it both through the official interface and any unprotected subfunctions.

The result is naturally that smart contracts are regularly exploited by attackers who take advantage of logical inconsistencies in the code. Million dollar thefts are almost a daily occurrence,[29] as any vulnerability will attract a host of anonymous attackers and there are many potential vulnerabilities in the code.

This raises the question: "If a smart contract is a contract, and the terms allow an attacker to take the cryptocurrency, is it actually theft?" Of course the question is rhetorical—the backers of various cryptocurrencies will exhort that code is law up until their cryptocurrency is stolen.

Finally, the "computer" these smart contracts actually execute on is remarkably poor. The entire Ethereum "global computer" has effectively 0.02% the computational power of a $45 Raspberry Pi 4, as there are a limited number of computations actually performed and, since all the miners are effectively running the same program, different miners aren't actually doing any more useful computation.

So what are smart contracts actually used for? The most common use is for creating "Decentralized Autonomous Organizations" (DAOs), non-fungible tokens (NFTs), "web3," and as the primary fabric for various "Decentralized Finance" (DeFi) systems.

DeFi systems mostly take three forms: decentralized exchanges, lending protocols, and yield farming. A decentralized exchange is simply an automated market maker, or a program that matches buyers and sellers using some level of reserve, for some token representing a DAO or other investment. This serves as an alternative to listings on conventional cryptocurrency exchanges. Normal cryptocurrency exchanges do at least

some vetting, but there is no vetting needed for adding an asset to one of these decentralized exchanges: an anonymous user just needs to provide some assets to create a liquidity pool.

Lending protocols are funded by participants to create an automated pool of cryptocurrencies. Someone else can then provide collateral and obtain a loan from the pool. Such lending protocols tend to be a mechanism to increase leverage in the cryptocurrency system. If prices go down, the pool will then automatically liquidate the collateral. Lending protocols are mostly used to increase leverage in the system, or for "flash loans": loans that only exist for a single transaction. Flash loans are used to exploit other DeFi projects that need a lot of funding for a single transaction but can return the funds when the exploitation is complete.

Finally, yield farming describes a large host of DeFi protocols where a user invests some amount of cryptocurrency in return for promised gains later on. At bottom, most of these yield-farming systems end up recapitulating a Ponzi scheme: there is no positive-sum activity for these yield farms to actually invest in, so they tend to create additional tokens to pay off previous investors.

The most famous such yield farming was the "Anchor Protocol" on the Luna blockchain. The Terra stablecoin was used to invest in this yield farm, obtaining some promised returns of 20% APY. These returns were, in the end, generated by creating more Terra, effectively creating a Ponzi scheme that destroyed some billions of dollars' worth of value.[30]

VIII. The Theory and Practice of DAOs and Join-Stock Companies

Most modern corporations are effectively autonomous organizations. There is a group of managers in charge of day-to-day operations who receive a salary or other compensation. The shareholders themselves can collectively vote on proposals on how the company should be governed and can even override management when it acts in an undesired way.

This basic concept—of a voting, collective ownership that directs management in company operations, with the voting owners receiving payments from the corporation's profits—is an idea that has existed for at least half a millennia. These corporations receive substantial

legal protections: it is the corporation itself, and neither the management nor the owners, that are usually liable for corporate activity. But, in return, corporations also have obligations. These obligations are heightened for any corporation that wishes to be publicly traded, which needs to perform substantial disclosures to comply with security regulations. Properly registered corporations also provide a liability shield: it is the corporation, not the individual investors, who are liable if the corporation misbehaves.

A DAO is an attempt to replicate this corporate structure but using an existing cryptocurrency as the fabric for voting. The DAO issues a set of "governance tokens." Possessing the governance token, at minimum, indicates a form of ownership that conveys voting rights in the DAO's activity.

The only major difference between a DAO and a modern joint-stock corporation is the paperwork. A DAO may or may not have a corporate parent created as a limited-liability corporation, but the DAO token itself is effectively never registered as a security.

DAOs operate their governance tokens in similar ways to the securities of a corporation. Importantly, governance tokens are offered in a way that is designed to create a secondary market where participants can actively trade the token beyond the initial set of people who received the token from the DAO.

The result is the commercialization of "securities fraud by proxy." A venture capital firm invests in a blockchain-related startup. This startup will then issue either a "governance" token (which represents an interest in the startup) or a "utility" token (which represents a promise of a future product from the startup), and the venture firm gets a large share of these new tokens.

The governance token represents an unregulated security, where the investors gain a vote and presumably a share of the profits. Utility tokens are instead a security in disguise: investors did not buy "dentacoin" to go to the dentist,[31] but instead in the hope that the Dentacoin service eventually launches and others will buy dentacoin to actually use.

Now the venture firm sells the tokens they obtained, either through a centralized exchange or on a DeFi exchange. This allows the venture firm to profit from their investment without needing to create a viable-enough company to withstand the mandatory disclosures

involved in a normal securities sale. And if the SEC ever enforces, it was the company they invested in, not the VC firm itself, that evaded a near century of securities law.

IX. The Theory and Practice of Stablecoins and Banknotes

During a large portion of the 1800s, the US did not possess a paper currency and did not have a central bank. During the "Free Bank Era," the US government only issued money in the form of coins. Physical coins, although always acceptable at face value, were inconveniently heavy. A $1 silver dollar weighed 26 grams, while a $20 gold piece weighed a similar 33 grams.

During this era, state-chartered banks would accept coinage and in return issue paper notes. The paper note represented a bearer asset—anyone with the note was assumed to have ownership over the noted amount of currency, and the bearer of the note was entitled to return to a branch of that particular bank to retrieve an appropriate amount of physical coins ("specie").

This system, however, had problems, notably "wildcat banks." A wildcat bank would issue banknotes that, through either mismanagement or deliberate action, were not actually backed by specie held in the bank. Stories abound of banks either showing state regulators barrels full of scrap covered with a layer of coins, or covertly moving barrels of coins between branches ahead of regulator inspections.

Backed stablecoins literally recapitulate the model of the free bank era. A stablecoin issuer such as Tether or Circle will accept a deposit from a "customer" and return them an equivalent amount of the stablecoin. This stablecoin is now a digital bearer asset, it can be arbitrarily transferred to others identified only by their public keys. Eventually, someone can then take that stablecoin and redeem it at the issuer for the underlying deposit value. Most centralized cryptocurrency exchanges are actually cut off from the global banking system, while the decentralized exchanges naturally have no banking ties. Thus the stablecoins became the unit of account in most cryptocurrency exchanges, with some exchanges effectively turning all real-money deposits into stablecoin deposits.

There are two major problems with these backed stablecoins. First, stablecoin issuers claim that their only customers are those who issue or redeem the stablecoins in the first instance, so they don't perform anti-money-laundering checks on the vast majority of stablecoin users. Second, the behavior of the major issuers, Tether and Circle, suggests that each is acting as a wildcat bank—and there is little to prevent additional wildcat banks from opening in the future.

The money laundering concerns with stablecoins are, so far, mostly theoretical. The on-ramps and off-ramps to the normal banking system for these stablecoins is limited, which acts as a cap on current potential criminal use. Similarly, stablecoins are not actually used in commerce but tend to only be used as a stable value on cryptocurrency exchanges, limiting their value for money-laundering purposes. But this could change if companies provide easier on-ramps to convert dollars into stablecoins.

The "wildcat bank" nature, however, is far less theoretical. Between Bitcoin's price peak on November 8, 2021, and September 1, 2022, the stablecoin Circle issued $17 billion in new circle. At roughly the same time, Coinbase saw that customer cash on deposit fell from $10 billion to $7 billion. The blockchain-nature of these stablecoins shows the amount issued, but offers no validation that the issued stablecoins are backed by actual funding.

For Circle's issued stablecoin to be fully backed directly implies that some $17 billion in new money was invested into the cryptocurrency space, during a massive bear market that saw Bitcoin drop from $67,000 to $20,000, and that this new money did not want to use a regulated exchange like Coinbase but instead wished to trade on unregulated exchanges.

Similarly, there is substantial evidence that the price bubbles seen in both 2017 and 2021 were largely driven by the issuance of new tether, as Tether printed billions of new coin.[32] The only alternative to Tether recklessly printing unbacked coin would be if tens of billions of new dollars flowed into the cryptocurrency space, sent by investors who wished to avoid the banked and regulated exchanges—exchanges that are regulated specifically to protect investors against deliberate manipulation.

There are two other classes of stablecoins: overcollateralized stablecoins and algorithmic stablecoins, although these two are less significant. In an overcollateralized stablecoin, such

as DAI, a participant will transfer a significant amount of cryptocurrency (say $15,000 at current price) and receive $10,000 worth of the stablecoin. These stablecoins then tend to be used to buy more cryptocurrency, creating a cycle of increased leverage, but have enough volatility to not be a true stablecoin because of the potential for a down-market unwinding collapsing the system.

Finally, algorithmic stablecoins couple a stablecoin with a volatile cryptocurrency. If the value of the stablecoin drops below a dollar, one can turn the stablecoin into the volatile cryptocurrency and make a "profit"; similarly if the stablecoin is above a dollar, one can turn the volatile cryptocurrency back into the stablecoin.

These stablecoins inevitably fail. The most recent major example, Terra/Luna, claimed to offer 20% rates of return on the Terra stablecoin within the Anchor lending pool before collapsing in a matter of days. The result was a classic Ponzi scheme: there were no actual borrowers willing to pay 20% interest so the gains were paid from other investors. When it collapsed, destroying a notional billion dollars of investor value, it caused many follow-on collapses as many cryptocurrency "investment" firms that were simply running Ponzi-pass-through funds were subject to additional investor scrutiny.[33]

X. Regulatory Principles

By now, it should be clear that the cryptocurrency space is not novel and cannot improve our existing financial system in a meaningful way. Instead, most innovations in the cryptocurrency space involve recapitulating the real financial system, overlaying it with a surfeit of historical frauds and failures, and disguising this by means of technobabble.

Our existing system is not free of problems, but these problems are not due to a lack of regulation. People complain about their bank or brokerage firm, but they don't complain that the regulations creating the FDIC and SIPC protect them from loss should their bank fail. Regulated stock exchanges don't wash trade against their customers, and insider traders and Ponzi scammers face meaningful risk of prosecution.

Fortunately most of the regulations constructed to deal with the cryptocurrency-related failures are also old, and most implement a "duck test": if it looks like a duck, quacks like

a duck, and swims like a duck, it's probably a duck. Thus, in regulating cryptocurrency activity, it is best to look past the technology and instead understand the systemic behavior that needs regulation. We already have the legal tools we need to create meaningful regulation of the cryptocurrency space.

XI. Regulating Tokens

As previously discussed, cryptocurrencies don't work for legal, above-the-board payments. Instead the legal use is restricted almost exclusively to a speculative casino where participants bet on whether the value of things like the Shiba Inu token goes up or down. Almost all of these speculative "assets" are zero-sum: every dollar "earned" is at the expense of some other participant. This nature is why I describe the system as a "self-assembled Ponzi scheme."

Newly released cryptocurrencies and related items generally fall into at least one of four categories: new "L1 cryptocurrencies," "utility tokens," "governance tokens," and "non-fungible tokens." But all except NFTs are securities under existing US law, correctly understood according to some principles I discuss here; indeed, arguably many NFT releases are also securities.

A new L1 cryptocurrency is simply a new blockchain with a new associated cryptocurrency. The promoter of the cryptocurrency creates a new network, arranges for at least some computers to validate, and then attempts to sell the tokens to others promising that the cryptocurrency somehow has an innate value. We previously discussed how "utility tokens" and "governance tokens" work in the context of various DAOs: they represent either a future service or a voting share in the corporate structure.

Finally there are "non-fungible tokens" (NFTs), which represent a nebulous ownership interest in a "unique" item, such as a URL pointing to an image. These are usually sold as collectables, akin to digital baseball cards, with some offering additional rights such as a license to produce derivative works or access to membership-only events.

All but the NFTs clearly fall under the SEC's ambit as they pass the Howey Test, which emerges from the Supreme Court's holding in *SEC v. W.J. Howey Co*.[34] This test defined

"investment contract" for the purpose of regulation under the Securities Act of 1933 and is a prototypical duck test: "In other words, an investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise."[35]

Whether a newly issued token purports to provide a new blockchain, some direct utility, or governance interest in a shared enterprise, they inevitably act as an "investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others."[36] This logic is no different than the ownership of the collectively managed orange trees in Florida which were the subject of *SEC v. W.J. Howey Co.*, the case from which the test derives.

Even many NFT projects should trigger the Howey Test, as the "art" is not being collected for the sake of the art, but on the belief that someone else will pay more for the NFT as a result of activity done by the group promoting the NFT. The group behind the NFT usually promises to produce some sort of "metaverse" project where the NFTs will provide access. So the future value of the NFT specifically depends on future action of others while those buying the NFT are seeking an investment.

A significant problem, however, is that the SEC has previously taken a hands-off approach when regulating these obvious securities. The SEC mostly seems to intervene only in the case when the security fails, with the notable exception of Telegram and their "TON" token.[37] The SEC must take a more proactive approach to regulation of these clear securities.

The SEC should start by reminding the cryptocurrency community that newly issued tokens, unless formally specified otherwise, fall under the Howey Test. The SEC did this in general with the original "DAO" report,[38] concerning the collapsed Ethereum investment fund, but has not been subsequently proactive. The report makes clear that most of these schemes satisfy the requirements set forth by the Howey Test and thus should be registered as securities. But amidst a flurry of various token releases, often backed by major venture capital companies, the SEC generally takes no action unless the release fails.

The lack of widespread proactive prosecution means that promoters can simply play the odds. If the SEC does not reliably enforce the rules, promoters can simply issue tokens and hope to get away with it. This problem is magnified by the presence of venture capitalists (VCs). VCs invest in companies that issue tokens and then sell the tokens as unlicensed securities. Even if the SEC eventually prosecutes the token issuer, the VCs that support and incentivize the continuation of this system are protected from SEC regulation. After all, the VC did not issue the unregulated security.

Instead of waiting for the collapse of a particular token, the SEC should send out what amounts to a "Wells-Notice-Lite," a formal reminder that the proposed issuance is an unregistered security and that if the issuer doesn't recall the issue, the SEC will proactively prosecute.

Additionally, when the issuer is an informal DAO rather than a formal corporation, the SEC should remind the participants that in the absence of a formal corporate structure, a DAO acts as a partnership, a legal structure where the participants face joint and several liability.[39] This is a particularly impactful reminder when DAOs are formed to operate unregulated stock exchanges, money laundering systems, or other activity that would be illegal in a conventional manner.

Finally, for the few who are not dissuaded, the SEC should file suit immediately to make it clear that this is not a bluff but a change in enforcement priority. Taken together, these methods of SEC enforcement should generally reduce the problem of newly issued tokens detrimentally affecting retail investors.

Existing tokens, however, still remain a significant problem. There are simply too many that have been issued over the years for the SEC to meaningfully protect investors from these existing unregistered securities. Current enforcement priority needs to stop the further issuance of unregistered securities. But they do serve an important lever for regulating the cryptocurrency exchanges to protect consumer interests even in the absence of direct action against the issuers.

XII. Regulating Cryptocurrency Exchanges

Cryptocurrency exchanges take three forms: lightly regulated exchanges with banking ties, unregulated offshore exchanges without significant bank connections, and decentralized exchanges that operate directly as a combination of a smart contract and a web page.

The lightly regulated exchanges must be more heavily regulated. There are only a few in the US (notably Coinbase, Kraken, Gemini, and, until recently, FTX-US), and they have devolved over the years.

To begin with, these exchanges are acting as broker/dealers—after all, their pitch is that individuals are "investing" in cryptocurrencies. Thus they should be regulated like broker/dealers. They need to be clearly under the SEC and FINRA (the Financial Industry Regulatory Authority) and mandated to carry SIPC insurance.

Coinbase is one of the oldest, largest, and most reputable exchanges operating in the US. Coinbase has shifted from an exchange that only listed a few cryptocurrencies that one could argue should be treated as commodities to an exchange that lists over 200+ cryptocurrencies, most of which explicitly trigger the Howey Test in their marketing materials. After all, if "staking" a token is supposed to earn an interest rate of 20%, it is clearly acting as a security contract.

In a recent lawsuit against a Coinbase insider who was performing insider trading, the SEC in its complaint explicitly listed over half a dozen cryptocurrencies that clearly acted as investment contracts, pointing explicitly to statements from the particular cryptocurrencies' promoters.[40] Coinbase's response was a blanket denial, claiming they categorically do not actually list any securities on their exchange.

The SEC should continue the process. The SEC should go through every listing for all exchanges that support US customers, document how each particular token satisfies the Howey Test, and then actively challenge the exchanges in court for acting as broker/dealers that facilitate the sale of unregistered securities. This would have multiple benefits, including both consumer protection and disrupting the modern business of securities fraud by proxy.

Increased consumer protection would follow from the requirements that a stock broker and exchange need to follow. Currently, a Coinbase or other cryptocurrency exchange customer in case of bankruptcy is simply an unsecured creditor.[41] If their account gets compromised, they lack any form of consumer protection.

If cryptocurrency exchanges wish to behave as investment vehicles for the general public, they should abide by the requirements we apply to banks, brokers, and exchanges to protect consumers in the case of insolvency or computer security compromises.

The offshore exchanges represent two additional problems which need further regulatory action: money-laundering risks and blatant market manipulation.

The money-laundering risk arises from accounts with weak or nonexistent "Know Your Customer" (KYC) and "Anti-Money Laundering" (AML) controls that are actively used to perform "chain swaps" to hide criminal activity. In a chain swap, a weak KYC account is funded with one cryptocurrency. The bad agent then uses that to buy a different cryptocurrency, and then withdraws the second cryptocurrency. This is commonly used to break the traceability of stolen cryptocurrency.

These offshore exchanges are also notorious for active market manipulation, including both wash trading and front running. The presence of these markets and the indirect coupling with the regulated exchanges represents a substantial threat to market regularity.

Some of the exchanges, notably FTX[42] and Crypto.com, have "independent" US subsidiaries. These subsidiaries should not be allowed to operate in the US while their corporate parents continue to operate unregulated offshore exchanges. Not only should these exchanges be brought under the same regulatory-type structure of a domestic stock exchange, they should also be required to ensure that their offshore parents meet both KYC/AML requirements and block blatant market manipulation.

As for the exchanges without ties to the US, a key lever will be enforcing the "Travel rule"[43]—regulations requiring that the sender and receiver are documented. The foreign exchanges which do not enforce the travel rule should effectively be cut off from transferring cryptocurrency to and from US exchanges, effectively segregating the market.

The final question is how to regulate the "autonomous, decentralized exchanges" that exist on Ethereum and other platforms. It starts with the observation that absent a corporate structure, a DAO is simply a partnership and all partners have joint and several liability. This means that those "investing" in Uniswap, the biggest of these decentralized exchanges, are themselves liable for the securities-law violations that occur every day on that platform. And if there is a corporate parent, then the corporate parent bears direct responsibility for enforcing securities laws on the "decentralized" platform.

But these decentralized exchanges have another hazard: automatic front running by the cryptocurrency miners themselves. Front running is illegal behavior on the part of an exchange, where the exchange observes a user's intended trade and conducts its own first, designed to benefit the exchange at the cost of the user.

In decentralized exchanges, a user's transaction is the atomic unit. But from the miner's viewpoint, it is a group of transactions. Miners will automatically construct the group of transactions to automatically front run the normal trader, a process known as "Miner Extractible Value."

This would clearly be illegal in a normal exchange, but this appears to be accepted in the cryptocurrency space. Fortunately most of the miners for Ethereum have a US nexus, and the Ethereum switch to proof-of-stake also has a significant US nexus. Any block producer who extracts MEV by actively trading against market participants is failing to properly operate the decentralized exchange as an actual exchange.

XIII. Regulating Stablecoins

The final area that needs substantial regulation is the backed stablecoins.[44] In the end, the backed stablecoins like Tether and Circle are the foundation upon which the entire edifice of unregulated exchanges are built. Eliminate the problematic nature of these stablecoins and you eliminate much of the entire space's problems.

The philosophy for regulating stablecoins should be straightforward: *all* users of a stablecoin are considered customers of the stablecoin issuer for all relevant money transmission regulations. All transfers of stablecoin balances between customers are

facilitated in part by the stablecoin issuer acting as a money transmitter. This may already be the case legally but it needs to be formally clarified, either directly by the regulators or by a legal change from Congress.

This would require just a minor technical change for the stablecoin's underlying smart contract. Instead of allowing the stablecoin to be transmitted between arbitrary individuals, the code should be modified to only allow transfers between individual public keys vetted by the stablecoin issuer. Registering the vetting is simply a cryptographic signature, a proof that a certain key is authorized to use the stablecoin created by the stablecoin issuer.

It would however require that the issuer conduct due diligence on its users, which will substantially increase operational cost. But why should a stablecoin issuer be exempt from the basic due diligence that any other payment processor is legally obligated to conduct?

In a single stroke this change would have multiple substantial benefits, including making it clear that Tether is subject to US jurisdiction, eliminating a potential money laundering threat, and disrupting the entire ecology of unbanked exchanges.

Currently, Tether maintains an assertion that they are exempt from US regulation because their only "customers" are the few corporations allowed to purchase new tether or redeem tether. Tether has even advertised this as a feature, suggesting that Iran should use tether to evade US sanctions.

This lack of ties to the US is clearly a fiction. Tether can be purchased on both the Coinbase and Kraken cryptocurrency exchanges and then transferred off for US speculators using DeFi or unregulated exchanges.[45] But making it clear that Tether's "customers" are the users, not just the purchasers, makes the ties explicit.

It would also prevent both Tether and Circle from becoming significant vehicles for money laundering. As a business, both Tether and Circle recapitulate many features of Liberty Reserve, a prior digital currency shut down by criminal prosecution by the Department of Justice.[46] Currently the stablecoins are not used for purchasing significant amounts of goods or services, but if they were to be used outside of cryptocurrency then they would probably find themselves like Liberty Reserve: the de-facto currency for online criminality.

The US Department of Justice disagreed with Liberty Reserve's similar assertions of exemption from US jurisdiction and successfully prosecuted those behind Liberty Reserve. Liberty Reserve deliberately did not vet the users of the currency and as a consequence became a center for online criminal-to-criminal payments. The notion should be rejected that using a pseudonymous public ledger,[47] as Tether does, rather than a confidential private database, as Liberty Reserve did, absolves the stablecoin issuer of the liability Liberty Reserve faced. After all, the only major difference between the two is how the records are maintained.

Vetting stablecoin users should also substantially disrupt the unbanked exchanges. Since the unbanked exchanges are clearly acting outside of existing regulatory frameworks but rely on the stablecoins as a unit of account, the stablecoin issuers should clearly not allow the unbanked exchanges to act as customers of the stablecoin.

Given these unbanked exchanges' weak KYC/AML controls, they would likely not pass muster with even the most cursory due diligence. After all, if these unbanked exchanges could pass such diligence, they wouldn't be unbanked; instead they would have ties to the normal financial system that eliminate the need for using stablecoins.

These unbanked exchanges really are, in reality, more akin to acting as a casino for cryptocurrency, where participants can bet on whether a number goes up. But as casinos they need chips, units of account that are stable for participants. The stablecoins are what provide this facility for exchanges otherwise cut off from conventional banking. If an exchange is not served by conventional banking, why should a stablecoin serve as the money transmitter?

XIV. Conclusions

Regulators, especially regulators in the United States, often fear accusations of stifling innovation. As such, the cryptocurrency space has grown over the past decade with very little regulatory oversight.

But fortunately for regulators, there is no actual innovation to stifle. Cryptocurrencies cannot revolutionize payments or finance, as the basic nature of all cryptocurrencies render

them fundamentally unsuitable to revolutionize our financial system—which, by the way, already has decades of successful experience with digital payments and electronic money. The supposedly "decentralized" and "trustless" cryptocurrency systems, both technically and socially, fail to provide meaningful benefits to society—and indeed, necessarily also fail in their foundational claims of decentralization and trustlessness.

When regulating cryptocurrencies, the best starting point is history. Regulating various tokens is best done through the existing securities law framework, an area where the US has a near century of well-established law. It starts with regulating the issuance of new cryptocurrency tokens and related securities. This should substantially reduce the number of fraudulent offerings.

Similarly, active regulation of the cryptocurrency exchanges should offer substantial benefits, including eliminating significant consumer risk, blocking key money-laundering channels, and overall producing a far more regulated and far less manipulated market.

Finally, the stablecoins need basic regulation as money transmitters. Unless action is taken they risk becoming substantial conduits for money laundering, but requiring them to treat all users as customers should prevent this risk from developing further.

References

[1] The cost to merchants for credit cards may be higher, but many credit cards effectively transfer 1% of the purchase to the cardholder as miles, cash-back, or other explicit benefits. Additionally, "card-not-present" transactions often charge an additional 1% compared with "swipe" or "dip" card-present transactions due to the greater fraud risk present in card-not-present transactions. My own small-business checking account, should I wish to accept credit cards, charges 2.6% + $0.10 for card-present transactions and 3.5% + $0.10 for card-not-present transactions.

[2] *See, e.g.*, Chase Bank's schedule of fees for business accounts, in *Additional Banking Services and Fees for Business Accounts: Deposit Account Agreement*, CHASE BANK 11 (Oct. 16, 2022), https://www.chase.com/content/dam/chasecom/en/checking/documents/biz-how-your-transaction-will-work.pdf. Cash deposits over a threshold are subject to a $2.50 per $1,000 fee for counting and verification, although it does not apply to ATM deposits.

[3] FinCEN, the Financial Crimes Enforcement Network of the US Treasury, provides a convenient guide for consumers. *See Notice to Customers: A CTR Reference Guide*, U.S. DEP'T TREASURY FIN. CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/sites/default/files/shared/CTRPamphlet.pdf.

[4] The size of the key is actually measured in "Bits," or "Binary Digits." So instead of 0-9, it is either 0 or 1. Bitcoin uses 256 bit public keys, which when written in decimal would be roughly 76-digits long.

[5] "Alice," "Bob," "Carol," and "Dave" are commonly used names of the participants in cryptographic protocols, with "Eve" acting as a passive eavesdropper and "Mallory" acting as a manipulating adversary.

[6] Traditionally, the rules only ask if the check is well-formed and actually sound, with sufficient fees paid to the miner to make it worth including, but miners can impose additional restrictions should they desire, such as only validating a check if it comes from an OFAC sanctioned entity.

[7] A good example of this is the State of Colorado's "acceptance" of cryptocurrency for tax payments. They don't actually accept Bitcoin. Instead, the Bitcoin is transferred through PayPal, which converts it into dollars and charges an additional $1 and 1.83% of the amount transferred. *See Cryptocurrency*, COLO. DEP'T REVENUE: TAXATION DIV. (2022), https://tax.colorado.gov/cryptocurrency.

[8] The attack attempted to steal $1 billion, but damage limitation limited the North Korean attackers to only succeeding in transferring $100 million. Of that, $20 was subsequently recovered. *See The Lazarus Heist: How North Korea Almost Pulled Off a Billion-Dollar Hack*, BBC NEWS (June 21, 2021), https://www.bbc.com/news/stories-57520169.

[9] This attack was also attributed to North Korea. Aaron Schaffer, *North Korean Hackers Linked to $620 Million Axie Infinity Crypto Heist*, WASH. POST (Apr. 14, 2022), https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/. A good resource tracking various thefts and scams is *Web 3 Is Going Just Great*, available at https://web3isgoinggreat.com.

[10] The only major exception to this was the "DAO hack," where the original Ethereum Decentralized Autonomous Organization suffered a massive theft. Normally the theft would be irreversible, but the programmers in charge of Ethereum released a new version of the code that undid the theft. The reversal happened not because normal users suffered a loss, but because a significant number of those responsible for coding and running Ethereum suffered losses. As such, these reversals are not commonplace, and irreversibility continues to be a fundamental part of cryptocurrency systems.

[11] Anyone who doesn't follow these rules will find their money quickly lost. One of the earliest Bitcoin exchanges, Tradehill, went out of business when faced with chargebacks from their payment processor. Sienrak, *Bankrupt Bitcoin*

Exchange Tradehill Suing Red Hot Payment Startup Dwolla For $2M, VENTUREBEAT (Mar. 7, 2012), https://venturebeat.com/security/tradehill-sues-suing-dwolla-Bitcoin/. Similarly, Steve Wozniak attempted to sell $70,000 worth of Bitcoin to someone who paid through PayPal. The transaction turned out to be fraudulent. James Cook, *Apple Cofounder Steve Wozniak Said He Was Scammed Out Of $70,000 In Bitcoin*, BUS. INSIDER (Feb. 27, 2018), https://www.businessinsider.com/steve-wozniak-stolen-70000-Bitcoin-2018-2.

[12] This is why most cryptocurrency "purchases" on cryptocurrency exchanges don't actually involve a cryptocurrency transaction. Instead, the exchange just updates its own internal database of "who owns what cryptocurrencies." The only cryptocurrency transactions actually occur when the user moves the cryptocurrency to or from their account on an exchange.

[13] The Lightning network was intended as a peer-to-peer system, but the basic nature and usage require that most transactions pass through just one or a few highly connected central relays.

[14] For a good retrospective of the Salvadorian Bitcoin environment a year after the experiment began, *see* Jacob Silverman & Ben McKenzie, *Nayib Bukele's Broken Bitcoin Promise*, INTERCEPT (July 22, 2022), https://theintercept.com/2022/07/22/Bitcoin-crypto-el-salvador-nayib-bukele/.

[15] David Gerard, *El Salvador's Bitcoin Law—One Year On, With The World's Coolest Dictator*, ATTACK OF THE 50 FOOT BLOCKCHAIN (Sept. 7, 2021), https://davidgerard.co.uk/blockchain/2022/09/24/el-salvadors-Bitcoin-law-one-year-on-with-the-worlds-coolest-dictator/.

[16] Samuel Haig, *El Salvador Introduces Fuel Subsidy of $0.20 Per Gallon to Locals Who Pay in BTC*, COINTELEGRAPH (Oct. 4, 2021), https://cointelegraph.com/news/el-salvador-introduces-fuel-subsidy-of-0-20-per-liter-to-locals-who-pay-in-btc.

[17] *See* Kyle Soska & Nicolas Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, USENIX (Aug. 12, 2015), https://www.usenix.org/system/files/sec15-paper-soska-updated_v2.pdf, for a detailed analysis of these marketplaces. Since then the markets have actually shrunk, as the indictment of the administrators of Deep Dot Web have made it significantly less convenient for new users to find these markets. *See* Press Release, *Administrators of DeepDotWeb Indicted for Money Laundering Conspiracy, Relating to Kickbacks for Sales of Fentanyl, Heroin and Other Illegal Goods on the Darknet*, DOJ OFF. PUB. AFF. (May 8, 2019), https://www.justice.gov/opa/pr/administrators-deepdotweb-indicted-money-laundering-conspiracy-relating-kickbacks-sales.

[18] It is unfortunately very hard to estimate total damage, but the scale of payments is in the billions: FinCEN reports seeing $1.2 billion in ransomware payments in 2021. *See FinCEN Analysis Reveals Ransomware Reporting in BSA Filing Increased Significantly During the Second Half of 2021*, FIN. CRIMES ENFORCEMENT NETWORK (Nov. 1, 2022), https://www.fincen.gov/news/news-releases/fincen-analysis-reveals-ransomware-reporting-bsa-filings-increased-significantly.

[19] *See* Nicholas Weaver, *The Ransomware Problem Is a Bitcoin Problem*, LAWFARE (May 27, 2021), https://www.lawfareblog.com/ransomware-problem-Bitcoin-problem.

[20] An example of the claimed benefits are those stated by Amazon in a blog entry promoting their AWS blockchain product. *See, e.g.*, *What is Decentralization in Blockchain?*, AMAZON WEB SERVS., https://aws.amazon.com/blockchain/decentralization-in-blockchain/.

[21] For example, the ACH system in the US has processed 185 million same-day transactions, moving some $486 billion per quarter through this distributed system. *Same Day ACH Growth Leads ACH Network to Second Quarter Gains*, NACHA NEWS (Aug. 2, 2022), https://www.nacha.org/news/same-day-ach-growth-leads-ach-network-second-quarter-gains.

[22] *Hashrate Distribution*, BLOCKCHAIN.COM, https://www.blockchain.com/explorer/charts/pools (estimating the hashrate distribution amongst the largest mining pools).

[23] *Coinbase and Lido Dominate Ethereum Staking*, TRUSTNODES (Sept. 15, 2022), https://www.trustnodes.com/2022/09/15/coinbase-and-lido-dominate-ethereum-staking.

[24] One recent such event lost $160 million when a wallet was generated using a tool that lacked sufficient entropy when generating private keys. *See* Vishal Chawla, *Experts Blame a "Vanity Address" Bug for Wintermute's $160 Million Hack*, BLOCK (Sept. 20, 2022), https://www.theblock.co/post/171192/experts-blame-a-vanity-address-bug-for-wintermutes-160-million-hack.

[25] A classic example of this is the original major Bitcoin exchange Mt. Gox, which had an exchange-controlled program (the "Willy Bot") that manipulated prices, before the exchange failed leaving the users without their cryptocurrencies. For the original reporting of the bot, *see* Willyreport, *The Willy Report: Proof of Massive Fraudulent Trading Activity at Mt. Gox, and How it Has Affected the Price of Bitcoin*, WILLY REPORT (May 25, 2014), https://willyreport.wordpress.com/2014/05/25/the-willy-report-proof-of-massive-fraudulent-trading-activity-at-mt-gox-and-how-it-has-affected-the-price-of-Bitcoin/. Later the operator of Mt. Gox, Marc Karpeles, admitted to running this bot in court. William Suberg, *Mt. Gox Trial Update: Karpeles Admits 'Willy Bot' Existence*, COINTELEGRAPH (July 11, 2017), https://cointelegraph.com/news/mt-gox-trial-update-karpeles-admits-willy-bot-existence.

[26] This is a process the Ethereum community calls "Miner Extractable Value" or MEV. In reality, most MEV is the miners explicitly front running trades on decentralized exchanges. For a detailed analysis of the profit involved, *see* Julian Piet, Jaiden Fairoze & Nicholas Weaver, *Extracting Godl [sic] from the Salt Mines: Ethereum Miners Extracting Value*, ARXIV:2203.15930 (Mar. 29, 2022), https://arxiv.org/abs/2203.15930.

[27] In the early days of Ethereum, 10% of all ETH was "invested" in a system called "The DAO," the first major Decentralized Autonomous Organization (at the time, around $150 million worth of ETH was invested, Klint Finley, *A $50 Million Hack Just Showed That the DAO Was All Too Human*, WIRED (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/, while Ethereum's total market capitalization at the time was ~$1 billion, *Market Capitalization of Ethereum (ETH) from August 2013 to November 9, 2022*, STATISTA, https://www.statista.com/statistics/807195/ethereum-market-capitalization-quarterly/). Someone discovered an oversight in the DAO's underlying code and used it to extract a substantial amount of the ETH. As many Ethereum developers' assets were amongst the amount stolen, the developers changed the code running Ethereum (a "hard fork") to undo the theft. Of course, by the "code is law" and "smart contract" logic behind Ethereum, the thief had a legitimate right to the ETH (the thief followed the code to the letter), which means that the developers, by doing a post hoc changing of the Ethereum code, were by Ethereum's logic stealing from the honest theft to benefit the developers.

[28] Earlier this year, the London Metal Exchange reversed and canceled a large number of transactions during unprecedented market conditions, demonstrating that the principle of reversibility is fundamental to how these markets work. Reuters, *LME Had Regulatory Obligation to Be Able to Cancel Nickel Trades in March, Filings Say*, CNBC (Nov. 29, 2022), https://www.cnbc.com/2022/11/29/lme-had-regulatory-obligation-to-be-able-to-cancel-nickel-trades-in-march-filings-say.html.

[29] A good reference is the site *Web 3 Is Going Just Great*, available at https://web3isgoinggreat.com/. At the time of writing, the first article was on a $20 million theft from the "Transit Swap" due to a vulnerability in the smart contract.

[30] *See* Elizabeth Lopatto, *How the Anchor Protocol Helped Sink Terra*, VERGE (May 20, 2022), https://www.theverge.com/2022/5/20/23131647/terra-luna-do-kwon-stablecoin-anchor.

[31] Dentacoin, released in 2017, promised to be the blockchain solution for the global dental industry. The notional value of all dentacoin peaked at $1.9 billion before quickly crashing. Currently the value of all dentacoin is just over one million dollars, representing a fall of 99.95%. *Dentacoin to USD Chart,* COINMARKETCAP, https://coinmarketcap.com/currencies/dentacoin/.

[32] For more information on the 2017 boom, *see generally* John Griffin & Amin Shams, *Is Bitcoin Really Untethered?*, 75 J. FIN. 1913 (2020), https://onlinelibrary.wiley.com/doi/full/10.1111/jofi.12903.The 2021 boom was accompanied by an even larger issuance of new tether, both in absolute terms and relative to the increase in market capitalization.

[33] The Terra/Luna system is still crumbling. First, Three Arrows Capital (3AC), a crypto hedge fund which was invested very heavily into this scheme, collapsed in July of this year. This was quickly followed by the crypto lenders Celsius,

Voyager, and Blockfi, all three of which lent customer funds to 3AC, which 3AC invested in the Terra/Luna anchor protocol. Lachlan Keller, *Three Arrows, Voyager Failures Raise Questions of Who Is Next in Crypto Fall From Grace*, FORKAST (July 6, 2022), https://forkast.news/three-arrows-voyager-failure-crypto-fall-from-grace/.

[34] 328 U.S. 293 (1946).

[35] *Id.* at 298-99.

[36] *Id.* at 301.

[37] For further information on this event, *see* Press Release, *Telegram to Return $1.2 Billion to Investors and Pay $18.5 Million Penalty to Settle SEC Charges*, SEC (June 26, 2020), https://www.sec.gov/news/press-release/2020-146.

[38] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, SEC (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf.

[39] The CFTC just sued one such DAO, the "Ooki DAO," specifically under the theory that the DAO, by not formally incorporating, leaves all the individual participants liable for the actions of the DAO. A copy of the docket is available at https://www.courtlistener.com/docket/65369411/commodity-futures-trading-commission-v-ooki-dao/.

[40] *See* Complaint, SEC v. Wahi, 2:22-CV-01009 (W.D. Wash. July 21, 2022), https://www.sec.gov/litigation/complaints/2022/comp-pr2022-127.pdf.

[41] *Form 10-Q*, COINBASE at 83 (May 10, 2022), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001679788/89c60d81-41a2-4a3c-86fb-b4067ab1016c.pdf.

[42] Subsequent to the writing of this report, the FTX enterprise collapsed, with the offshore exchange's collapse also drawing in FTX US. Now all FTX US customers are unsecured creditors in a corporate bankruptcy where the new restructuring CEO, John Ray III, described the situation as worse than Enron.

[43] *See Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies,* FINCEN (May 9, 2019), https://www.fincen.gov/sites/default/files/201905/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[44] There are arguments made for "Central Bank Digital Currencies" (CBDCs), stablecoins issued directly by the central bank. Such CBDCs really can take three separate forms. The first is an improvement of the central bank's operating infrastructure. This represents a case where "blockchain" or "CBDC" is simply a distraction, designed to enable the central bank to pay to improve its internal infrastructure. The second form has the CBDC available only to participants who pass KYC/AML checks. In that case the CBDC is really the central bank acting as a retail bank, no different than some countries use their post offices to perform. The final form, a bearer asset without KYC/AML controls, would have the same money-laundering concerns as the backed stablecoins. It is doubtful a major central bank would wish to create such a criminal-friendly structure.

[45] *See Tether*, COINBASE, https://www.coinbase.com/price/tether; *Tether*, KRAKEN https://www.kraken.com/prices/tether.

[46] The founder of Liberty Reserve pled guilty and received a 20 year prison sentence. *See* Press Release, *Liberty Reserve Founder Sentenced to 20 Years for Laundering Hundreds of Millions of Dollars*, DOJ OFF. PUB. AFF'S (May 6, 2016), https://www.justice.gov/opa/pr/liberty-reserve-founder-sentenced-20-years-laundering-hundreds-millions-dollars.

[47] This is equivalent to a system where everyone has an arbitrary number of Swiss-style numbered accounts, where transactions between accounts are publicly viewable but there is no notion tying accounts to individuals.

Published by the Information Society Project at Yale Law School, Baker Hall, 100 Tower Parkway Room 412, New Haven, CT 06520 United States of America.

The Digital Future Whitepaper Series is made possible thanks to the support of Immuta.

About the Author

Nicholas Weaver received his Ph.D. in computer science in 2003 and since then has worked at the International Computer Science Institute with a focus on security, including criminal activity. He has followed the cryptocurrency space professionally for a decade. He holds no cryptocurrencies, and the only Bitcoin he ever possessed he gave away in 2015.

Digital Future Whitepaper Series

The Digital Future Whitepaper Series, launched in 2020, is a venue for leading global thinkers to question the impact of digital technologies on law and society. The series aims to provide academics, researchers, and practitioners a forum to describe new challenges of data and regulation, to confront core assumptions about law and technology, and to propose new ways to align legal and ethical frameworks to the problems of the digital world.

The Digital Future Whitepaper Series is led by ISP visiting fellow Andrew Burt and co-edited by ISP Wikimedia fellow Artur Pericles Lima Monteiro and ISP affiliate fellow Nikolas Guggenberger. Sachin Holdheim (Yale Law School '24) served as the research assistant for this whitepaper.

Information Society Project

The Information Society Project (ISP) is an intellectual center at Yale Law School, founded in 1997 by Professor Jack Balkin. Over the past twenty years, the ISP has grown from a handful of people gathering to discuss internet governance into an international community working to illuminate the complex relationships between law, technology, and society.

Information Society Project
Yale Law School

127 Wall Street
New Haven, CT 06511

203.432.4992
www.law.yale.edu/isp