Rai Ling
Anarchism and Cryptocurrency
10/20/2022

www.mutualismcoop.com

theanarchistlibrary.org

Anarchism and Cryptocurrency

Rai Ling

10/20/2022

Contents

rectly competes with the domestic currency and operates outside the purview of the government.

Because of the distributed nature of crypto, crackdowns have had little success. For example, despite being deplatformed by service providers and blacklisted by centralized exchanges, the Tornado Cash smart contract on Ethereum cannot be removed or changed, and can still be used via decentralized frontends. Additionally, some of the countries with the highest rates of adoption adjusted for purchasing power parity like Vietnam, Turkey and China are hostile towards cryptocurrency, demonstrating that they can do little to stop people from using it. Given this resilience, many Anarchist organizations use Bitcoin addresses as an option for fundraising, which is useful for contributors who want to maintain a degree of anonymity and don't have access to mainstream fundraising platforms. It also facilitates illegal praxis like squatting.

In light of these factors, the leftist narrative on cryptocurrency as an environmentally destructive "scam" is uninformed, reactionary and echoes concerns voiced by governments. While it can be used as a speculative asset, individuals also value cryptocurrency because it is permissionless, trustless, secure, distributed, and opens up spaces that are illegible to the state. More broadly, we ought to acknowledge that usefulness is subjective and how and whether people use a technology is up to them.

Introduction

Cryptocurrency, a digital currency in which transactions are verified and recorded by a decentralized system using cryptography, rather than by a centralized authority, is a controversial technology amongst anarchists, even though it is often used as a tool for undermining state power.

The left generally sees cryptocurrency as a negative due to its function as money (which some seek to abolish), volatility, ostensible harm to the environment, alleged lack of decentralization, scams, and association with right-libertarianism, which have resulted in many left-leaning anarchists irrationally lashing out against crypto. These conclusions lack nuance, ignore the real-world applications of crypto, stem from misinformation, and ultimately amount to technological conservatism. In this essay, I will explore crypto's potential as a liberatory tool, push back against many of the left's misconceptions about it, and explain why it's useful in both a capitalist and non-capitalist setting, while providing nuance on its shortcomings.

How Does Cryptocurrency Work?

Before directly addressing leftist arguments, it is first necessary to understand how cryptocurrencies work and why they are designed as they are. Cryptocurrencies typically use blockchain, an immutable distributed ledger that anyone can access but not unilaterally alter to record transactions. No single entity can seize assets, reverse transactions, or change the ruleset for a given blockchain. This ledger is stored on a decentralized network of computers which have to come to a consensus to validate transactions as there is only one valid state for the ledger at any given point in time.

Blockchains use consensus algorithms to disintermediate transactions that otherwise rely on trusting centralized payment processors. Abstractly speaking, in physical space, consensus is based on trust between individuals or violently imposed by the government. The cost of centralized consensus includes global police and military spending used to enforce government decisions. In a stateless context, the cost of consensus is the labor that goes into building relationships, deliberating, and compromising in order to come to agreements. In physical spaces, consensus becomes harder to scale without people being overruled because not everyone can agree on a singular course of action. However, in cyberspace, distributed consensus can be achieved at scale using algorithms.

Blockchains enable trustless, permissionless, open, and anonymous infrastructure for making transactions. These properties are achieved through a system of incentives to miners and validators, which requires the introduction of costs through artificial scarcity to prevent 51% attacks and the validation of malicious blocks. A 51% attack is when controlling at least 51% of the hashrate or stake in a blockchain allows one to censor transactions, undo blocks and change the order of transactions. The nature of these costs depends on the consensus algorithm used.

In proof-of-work, miners solve hash functions, a computationally intensive process that consumes energy, for the right to build the next block. Therefore, it is infeasible for miners to carry out a 51% attack without massive capital and energy expenditure. The energy expenditure also disincentivizes miners from validating malicious blocks that would simply be rejected by other nodes that also have a copy of the ledger. Hence incentives are aligned around collecting the block reward and/ or transaction fees. In proof-of-stake, tokens are staked and nodes that validate malicious blocks have their tokens slashed. It has to be impossible for an attacker to control the majority of the tokens for 51% attacks so tokens must retain value. In all these examples artificial scarcity is used to create costs that in turn create incentives that help secure the underlying net-

consequence of its geographic decentralization. Some tend to favor further geographic decentralization of validators and embracing diverse validator preferences, while others support introducing additional incentives to the base layer such as slashing censoring blocks to disincentivize censorship. In the event that 51% of validators refuse to attest to blocks that include sanctioned transactions, the simplest solution to reestablish decentralization would be to start slashing staked tokens.

Conclusion

A good way for skeptical anarchists to approach cryptocurrency is to consider why the surveillance state is so threatened by it in the first place. Tornado Cash, a mixer deployed on many blockchains that allows users to make private transactions, was recently sanctioned by the US regime and a contributing dev was arrested in Belgium, setting further precedent for banning the use of technologies that threaten the state. ICE recently formed a contract with centralized exchange Coinbase for blockchain user analytics so they can track the movement of funds on-chain as best as it can[27]. Many nations have also passed anti-crypto legislation and voiced anti-crypto sentiment, sometimes to the point of all out bans[28].

In each of these cases, the state makes attempts to sanction crypto because it allows people to subvert regulations, evade financial surveillance, and undermine legal tender, all of which reinforce state power and the existing level and distribution of rent. Central banks, especially those of countries with high inflation such as Turkey, take steps to ban crypto as it can be used as a vehicle for capital flight, which further weakens the domestic currency. Others, such as Nigeria, have banned it for transactions because it di-

[27] theintercept.com/2022/06/29/crypto-coinbase-tracer-ice/

[28] en.wikipedia.org/wiki/Legality_of_cryptocurrency_by_country_or_territory

requirement nodes that can be embedded in desktop applications and deployed into wallets, allowing users to trustlessly verify information from infrastructure providers[25].

Another ongoing risk to the Ethereum network, which Bitcoin has never faced, is regulatory risk from the US Office of Foreign Assets Control (OFAC), which has sanctioned Tornado Cash. Validators are free to exclude and reorder transactions in blocks, which means it is possible for them to individually comply. Currently around 53% of blocks (as of writing this article) on Ethereum are OFAC compliant because they use Flashbots, a US based maximum extractable value (MEV) boost relay, which has built in censorship due to regulatory requirements[26]. MEV is the practice of including, excluding and reordering transactions from blocks in order to capture on-chain arbitrage opportunities. Flashbots is an intermediary software stack that allows a competitive market of searchers and builders to build and send blocks to proposers (validators), which prevents the market from becoming dominated by a small set of validators who are versed in MEV. Builders that use Flashbots cannot include sanctioned transactions. The remaining 49% of validators do not do this, so the network is as of yet censorship free. However if these validators refuse to attest to sanctioned blocks through the consensus client, it would constitute a 51% attack on the network.

The community is aware of these risks and generally agrees on a range of solutions, including a protocol level proposer-builder separation, better privacy features to mask whether transactions are OFAC compliant, and platforms like EigenLayer, which allows validators append MEV bundles to blocks, allowing them to still include censored transactions. That said, there is some division on whether incentives should be introduced to make the network inherently censorship resistant rather than censorship resistant as a

[25] openethereum.github.io/js-libs/light.js/concepts/light-client-development.html

[26] www.mevwatch.info

work. In PoW, the incentive to mine comes from the value of the token, which is important as a more decentralized network also increases security. Correspondingly, in PoS the value of the token prevents 51% attacks by making it costly to acquire most of the supply.

Hence, there is a degree of path dependency as early adopters accumulate tokens and power in their respective networks leading to a variable amount of economic rent, where revenues are in excess of costs (including labor costs)[1]. This can still be mitigated by experimenting with tokenomics like making issuance relatively high, or consensus protocols like delegated proof-of-stake, which is used by blockchains like Cosmos, where all users can stake their tokens to a validator as part of the blockchain without running any hardware. Technically, one can also do this on Ethereum by staking with staking aggregators like Lido, but this isn't part of the consensus protocol itself. There are also coins like Nano where there are zero transaction fees, although this comes with trade-offs like huge amounts of spam on the network. In the cryptocurrency ecosystem as a whole, transaction fees are being constantly eroded through layer 2 scaling solutions and a competitive multi-chain ecosystem.

The cost of trust in our current economy is often far more than scarcity rents paid to miners and transaction fees, which is why many people use blockchain technology to make transactions. When using a centralized payment processor, transactions are validated through services like ACH, Fedwire, and SWIFT, which are monitored by the state for "illicit" activity and require us to place our trust in banking corporations and the state, which is not an option for many people. The reason ACH and wire transfers usually take several business days is that transactions are "processed" or audited by the state, in the US the federal reserve fulfills this role. By using regulated services, one is implicitly trusting corporations and the government. These services limit services

[1] en.wikipedia.org/wiki/Economic_rent

to people based in certain location, profession, legal status, and so on, whereas blockchain is permissionless, the only thing one must trust are the incentives created by the consensus protocol, or "math," as some say.

Cryptocurrency as a Tool for Liberation

For most leftists, cryptocurrency is primarily seen as a tool for financial speculation that is rife with scams. Indeed, many early adopters made millions as artificial scarcity combined with an influx of speculative capital caused crypto prices to rise exponentially. The space is also utterly rife with scams, some obvious and others not. However, these facts do not take away from its benefits and only cover a small fraction of the overall picture. In the same vein, the internet is also rife with scams and has created many billionaires. Neither of these facts mean that we should do away with the internet, but rather think about how it is designed and organized.

Cryptocurrency allows people to make unauthorized transactions, protect their assets from government seizure and escape financial surveillance, which challenges several major vectors of state oppression. Its permissionless property means people can buy drugs, remit money, fund unauthorized activities like protests and avoid taxation, all without having to go through state controlled channels. For example, undocumented people use crypto to remit funds without having to use banks, which they may not have access to and could expose them to the state[2]. Unlike the banking sector, sufficiently decentralized crypto networks cannot be subject to international sanctions and do not require identification to use. Sex workers use it for payments after getting barred from banks and platforms such as Patreon, Cashapp and

[2] decrypt.co/46019/bitcoin-helping-undocumented-immigrants-send-money

The decentralization of PoS networks like Ethereum depends on the number of validators, nodes, and how tokens are distributed across them. The number of Ethereum validators is roughly calculated as the amount of staked Ethereum divided by 32, the minimum amount of Ethereum one must stake in order to become a validator. At present, there are 441,747 validators securing the Ethereum network[23]. However, not all of these validators operate their own nodes, rather, 60% of staked is custodied by staking pools like Lido that stake deposited Ethereum with a validator from a set of node operators. Because hardware requirements for running a validator are very low, individual nodes can run many validators and nodes do not necessarily have to function validators. The distribution of staked tokens across nodes or staking pools gives us more insight into how decentralized the network is. At present, the largest staking pool, Lido, holds 30% of staked Ethereum, which is less than 51%[24]. Moreover, just like mining pools, users can exit staking pools and go elsewhere. Also staking pools distribute Ethereum to many independent nodes, which mitigates the threat they pose to decentralization.

While cryptocurrencies like Ethereum have trustless and distributed consensus mechanisms, centralization has crept in through other avenues. Most of the space trusts centralized infrastructure providers such as Infura and Alchemy, which allow decentralized applications to remotely query the underlying blockchain through APIs, as it may be infeasible for them to run their own full nodes (which involves storing the entire blockchain). The problem with this is that infrastructure providers can censor and misrepresent information from the blockchain. This is a vulnerability in the Ethereum software stack, but does not compromise the underlying blockchain. There are also solutions to this problem such as light clients, which are low resource

[23] ethereum.org/en/staking/#gatsby-focus-wrapper

[24] decrypt.co/108906/ethereum-staking-pools-who-runs-the-largest-ones

ticle[17][18]. However, blockchain decentralization is a spectrum and we can ask *how decentralized* a given blockchain is and how this is measured. For this purpose we can look at decentralization metrics of Bitcoin, which uses PoW, and Ethereum, which uses PoS.

The decentralization of PoW networks like Bitcoin can be measured in terms of the hashrate and distribution of hashrate. Hashrate increases as more nodes enter the network, making it more decentralized, but who controls these nodes also matters in terms of decentralization and security. The distribution of computational power or hashrate across miners is a way to understand this. As of writing this article, the largest Bitcoin mining pool, Foundry USA, controls approximately 28% of the hashrate, which is lower than the 51% it would take to carry out an attack[19]. Mining pools also represent many different individuals and groups who own their own hardware and can pull out if they believe the operator is a threat to the network. The incentives of PoW mean that pools are unlikely to collude, but to carry out such an attack today it would take the top 5 pools who collectively control 52% of the hashrate[20]. Another potential vector of attack is state coercion, which is why the geographic distribution of hashrate matters — currently no single country controls more than 37.84% of the hashrate[21]. Bitcoin's supply dispersion doesn't determine the decentralization or security of the network, but does reflect external speculation and internal accumulatory dynamics. One point to note here is that supply appears more concentrated than it is due to exchange wallets that represent millions of users and asset custodians[22].

[17] bitnodes.io

[18] ethernodes.org

[19] btc.com/stats/pool

[20] blockworks.co/news/measuring-decentralization-is-your-crypto-decentralized

[21] ccaf.io/cbeci/mining_map

[22] insights.glassnode.com/bitcoin-supply-distribution/

Ko-fi, which also have arbitrary KYC (know your customer) requirements[3]. Crypto was used in Nigeria to fund an anti-police brutality movement that was barred from the banking sector[4]. It is also used to buy both recreational and life-saving drugs like HRT on black and gray marketplaces such as Hydra.

A recent study by Chainalysis shows that "grassroots crypto adoption" is high in emerging markets and countries with unstable financial conditions and relatively high levels of monetary repression such as Vietnam, Nigeria and Ukraine[5]. Crypto also allows people to bypass foreign sanctions. For example, in Afghanistan an NGO used BUSD, a dollar stablecoin, to sidestep US sanctions, the Taliban and failing banks, which were cut off from systems like SWIFT, to provide emergency funds for food in the unstable period following the American withdrawal[6]. As crypto adoption increased, the Taliban eventually banned crypto to force people into the banking system where their activities are more legible and funds cannot be easily transferred overseas, but given its properties, such bans are difficult to enforce.

Crypto has seen heavy adoption as a way to hedge against inflation. In Turkey, where the government continues to debase the Lira, Bitcoin currency exchanges have been appearing on the streets. Similarly, many Lebanese people have turned to crypto after banks suspended withdrawals and the Lebanese pound collapsed. The same trend has appeared in Venezuela during its period of hyperinflation[7]. Although many cryptocurrencies are volatile, they have still retained their value better than many global currencies. Moreover, cryptocurrency has globalized access

[3] www.cnbc.com//2022/02/05/bitcoin-a-lifeline-for-sex-workers-like-ex-nurse-making-1point3-million.html

[4] qz.com/africa/1922466/how-bitcoin-powered-nigerias-endsars-protests

[5] blog.chainalysis.com/reports/2022-global-crypto-adoption-index/

[6] theintercept.com/2022/01/19/crypto-afghanistan-sanctions-taliban/

[7] www.dw.com/en/venezuelans-try-to-beat-hyperinflation-with-cryptocurrency-revolution/a-57219083

to the US dollar through stablecoins. As an aside, although many people claim that Bitcoin is not an inflation hedge due its recent performance in the face of extremely high inflation, a closer look shows that global markets haven't been reacting to inflation but an increasingly Hawkish Fed Reserve for the past year, specifically from when Fed chairman Jerome Powell acknowledged that inflation was no longer transitory in November 2021, a signal that they would stop debasing the dollar. In the subsequent period, historical inflation hedges like gold and growth stocks depreciated in value, while real yields on bonds went up alongside the dollar. *Unchecked* inflation decreases real bond yields and reduces the purchasing power of fiat currency.

Crypto is also useful as a tool for digital transactional privacy, which is impossible through the banking sector. Crypto networks provide varying degrees of privacy; to begin with, wallet addresses are randomly generated strings that do not require KYC. Transactions on conventional blockchains are public but external observers cannot know who they involve unless they are associated with bank accounts through fiat-onramps like centralized exchanges. Tools like LocalCryptos allow users to bypass centralized exchanges for transferring funds on and off chain. However, most cryptocurrencies do not hide transaction amounts and wallet addresses by default, this can be achieved by using mixers such as Tornado Cash and Blender, which pool deposits from many addresses and allow users to withdraw to unlinked addresses later, providing probabilistic privacy. There are also "privacy coins" like Monero and Zcash that have base layer privacy, the former uses ring signatures that group transactions for probabilistic privacy, while the latter uses zero knowledge proofs to hide transactions, where only the proof is published on-chain. There are also many newer privacy protocols with smart contract capabilities such as Penumbra, Secret Network, DarkFi and Aztec. Some have argued that cash can achieve the same things, but this doesn't take into account that we live in an

for them to charge for services or for people to donate what they want[16].

In this framework, it is inconsistent for NFTs to be singled out but not Netflix, Spotify, games that sell in-game items and all other services that paywall users to access digital content. The silver lining of NFTs in gaming is that they redistribute scarcity rents to users instead of concentrating them in the hands of gaming corporations by creating an economy for in-game items; one could think of it as a decentralized marketplace for Counter Strike skins.

When all is said and done, people nevertheless treat NFTs as a form of ownership in a speculative or in-game context. If people want to play speculative zero-sum games or pay rent to each other, it's their prerogative. A similar phenomenon is people paying for Netflix even though there are practically no legal consequences to piracy and pirated content is available on a similar interface through services like the utorrent web player, streaming sites and apps like Popcorn Time. In such cases, persistent informational asymmetries on how to pirate media, moral values that support copyright, relatively seamless interoperability, misplaced fear of legal action, amongst other things, seem to create long term market failure. Some economic rent is unavoidable and is ultimately compatible with anarchy if people aren't forced to pay it by authorities.

Is Cryptocurrency Centralized?

The question of whether crypto is truly decentralized is important for people who value it for its properties. With many dishonestly arguing that it is centralized and thus not secure, this is an important issue to discuss. On the surface, most major cryptocurrencies are clearly decentralized because they consist of many nodes coordinating to maintain a distributed ledger. Bitcoin has 15,161 nodes and ethereum has 8,068 nodes at the time of writing this ar-

[16] extortionindustry.org/extortion.html

incentivize attendance for future rewards. Insofar as they are used to reference artwork, NFTs can be used for commissions and to support artists, much of the art sold on platforms like Foundation has no speculative resale value and "buying" this art can be considered a donation that incentivizes the creation of art. Finally they can be used to represent or signal group membership in a trustless manner, where linked content provides relevant context.

However, beyond the generalizations, there are coherent critiques of the use cases of NFTs, like them being used to denote ownership of the information they reference. Ownership allows one to exclude others from access by definition, which NFTs do not do. People are essentially paying for a token with a pointer to something they do not actually own and can be freely copied by anyone. Therefore, one could argue that these tokens are worthless *outside of a speculative context.* The most common manifestation of this is speculators buying tokens that reference artwork. Many freely acknowledge this in the crypto industry, referring to NFTs as "shitcoins" (coins with no use-case besides speculation) with pictures attached to them. Recent innovations in the space like Sudoswap further cement this perception, which has implemented NFT liquidity pools that allow users to instantly buy and sell NFTs on-chain.

In NFT gaming, NFTs are used to reference in-game items. What makes them different from art NFTs is that a game creates a stable context for them to retain value that isn't strictly speculative. People who play games may buy in-game items to improve their gameplay experience and expend effort to acquire items, which has a cost. An economic rent minimizing critique of this paradigm applies to pretty much all video games today, which is that developers and gaming corporations accumulate artificial scarcity rents by selling information, which is not scarce despite the value people happen to assign to it. Therefore, the only way to compensate content creators without them benefitting from scarcity rents is

increasingly digitized world. Unlike cash, cryptocurrency doesn't have to be physically carried around and stored, allows people to transact from afar, and is not subject to government monetary policy. Given the use cases we have already covered, it should be clear why privacy makes crypto networks more resilient to government intervention while allowing marginalized users to meet their goals.

A good rule of thumb for how to evaluate the usefulness of a cryptocurrency is to consider whether it steps in to solve an existing problem or comes up with a contrived use case. For example, crypto is being used as an incentive layer on top of p2p protocols like decentralized wireless networks, torrenting, and decentralized file storage. Helium, introduced the Helium token as an incentive for users to run hotspots for a low bandwidth peer-to-peer wireless network catered to IoT (internet of things)[8]. The project has had little success so far due to low demand in a niche market and having to compete with large state subsidized internet providers[9]. Similarly, decentralized file storage protocols like IPFS and Arweave have adopted Filecoin and the Arweave token, respectively, to account for storage costs. Another example is Bittorrent, a communication protocol for peer-to-peer file sharing, introducing a token for leechers to pay seeders, which is useful for users who want to incentivize others to seed neglected files or provide extremely fast download speeds.

Decentralized finance, disintermediated financial services such as loans, insurance and stablecoins provided on-chain through smart contracts, is another important use case for cryptocurrency. It competes with traditional banking services, sometimes with more competitive product offerings. For example, Liquity protocol allows users to take out zero-interest loans against Ethereum

[8] www.nytimes.com/2022/02/06/technology/helium-cryptocurrency-uses.html

[9] blockworks.co/news/where-is-the-revenue-helium-investors-inquire

collateral with a ratio of 110% (you can borrow up to 90% of the dollar value of your provided collateral) with a one time fee as low as 0.5%. The protocol issues its own native stablecoin against the underlying collateral, which means it doesn't have any associated capital costs, allowing borrowing costs to be far lower than anything found in traditional finance[10]. The main drawback of Liquidity compared to offline lending is the necessary collateral requirements, which can be much lower or non-existent depending on how much counterparties trust each other.

To summarize, many people who benefit from cryptocurrency don't have unstable currencies, are seen as criminals for existing, live under totalitarian governments that ban all forms of protest, and are illegal immigrants barred from the banking system, etc. Cryptocurrency also creates incentives on decentralized networks that undermine the state such as torrenting and mesh networks. From an anarchist perspective, crypto can be used today as a tool for undermining and evading the state. Absolutely opposing cryptocurrency in this context ignores the lived experiences of those who benefit from it and further marginalizes them.

Cryptocurrency in an Anarchist Context

Despite the difficulty of reaching consensus at scale, transaction fees, and accrual of economic rent, cryptocurrency is useful and sometimes even lifesaving for certain individuals in capitalist context. Can the same be said in an anarchic context?

In the absence of a state monitoring transactions and top-down rules and regulation, people would probably be more inclined to trust centralized services for cheap and instant transactions, everyone would have access to them, and market competition would encourage trustworthiness and good risk management. However, there are no guarantees, and centralized platforms are inherently

[10] www.liquity.org/blog/on-price-stability-of-liquity

typically used discretionarily, consume 1.6 times the energy of Bitcoin mining.

The purpose of these comparisons is to reveal that much of the criticism of Bitcoin's energy use stems from the idea that it is wasteful, which is ultimately a function of one's subjective view of the utility of Bitcoin's security model, which many people nevertheless find useful. From a practical standpoint, it makes little sense for us to complain about how individuals utilize the grid as long as they internalize the costs of doing so. Rather we can look at decarbonizing the grid and making proof-of-work more sustainable.

A Breakdown of NFTs

An examination of cryptocurrency would be incomplete without deconstructing the phenomenon of NFTs seeing as they get a lot of ire from left-leaning anarchists and the left in general. An NFT is a unique token stored in a blockchain with an optional metadata extension that can contain a URI (Uniform Resource Identifier). There are various use cases for NFTs, from a tool to compensate artists to just another speculative asset for people to trade.

The first mistake people make is conflating NFTs with tokenized artwork when they can actually be used for many different purposes (none of which necessarily require blockchain). NFTs can be used to represent any physical object for sale in a marketplace. This can technically take place on a variety of platforms but the properties of blockchains mean people can display goods for sale without permission, even though the physical transfer of property ultimately requires trust. They can also be used as a public, trustless *interface* for provenance as third party platforms can connect to a blockchain and reveal authorship for a given piece of media, one example being NFT profile pictures on Twitter. Today NFTs are commonly used for proof of attendance in the crypto space, where event attendees receive POAPs (Proof of Attendance Protocol) to

try. Mining incentivizes the buildout of baseload for the grid by providing a demand for electricity in underserved areas where it may not be profitable for energy companies to invest. For example, Gridless Compute uses Bitcoin mining to monetize micro-hydro plants in Kenya as a buyer of last resort. Bitcoin miners can also dynamically shut off during surge demand and turn on when there is excess capacity, which subsidizes intermittent renewable energy[14]. An example of miner mobility is Chinese miners moving from the Northern Province of Xinjiang where they use coal power to the South-Western Province of Sichuan where they use cheap surplus hydro power during the monsoon season. In general, non-rival or stranded energy tends to be cheap and Bitcoin miners are likely to seek it out. However, this can also backfire as the cheapest option, in one case, turned out to be a decommissioned coal plant. Finally, Bitcoin mining can capture and utilize waste methane that would have otherwise been flared or vented, which is net-zero in terms of emissions, but also subsidizes the underlying industrial processes.

Another way of contextualizing Bitcoin's energy use is by looking at how it compares to other activities that also draw energy from the grid. Technically, in the traditional global banking system, settlement in dollars is ultimately enforced by the US military and police, the former is one of the largest polluters in the world and consumes 7 times more energy than Bitcoin. Moreover, the dollar is legitimized through the US government taxing and fining individuals and businesses. Both in ethical and energy terms, Bitcoin seems like a better alternative. We can reasonably estimate that gaming uses 46% more energy than Bitcoin mining, with a less sustainable energy mix[15]. Despite this, nobody complains about the collective energy use of professional Twitch streamers with their electricity guzzling gaming rigs. Similarly, domestic tumble dryers, which are

[14] gridlesscompute.com

[15] braiins.com/blog/bitcoin-mining-vs-gaming

able to do anything they want with the funds they custody including blocking transactions, freezing funds and leaking information. Centralized platforms also have a single point of failure, making them more susceptible to attacks.

Cryptocurrency provides an alternative to trust itself, which was the sole basis for reciprocal social relationships prior to the invention of blockchain. Even attempts to hedge against trust, such as the use of systems like escrow, require the use of a trusted intermediary. Trust is scarce and therefore costly because it requires a certain amount of labor to maintain and labor always has a cost, although it can be negligible in many cases. In other words, the social dimension is not free of friction and our everyday interactions carry transaction costs.

Trust is also intertwined with social capital and the path dependency of social capital accumulation is somewhat analogous to the artificial scarcity on a blockchain, both of which result in the accrual of scarcity rents. Despite relatively competitive markets, institutions that people trust may become fixed, and trustless modes of interaction provide an exit and a check on social capital as a whole. For any given individual, the choice between using trust based vs. trustless systems depends on which carries higher transactions for them. This could vary significantly from transaction to transaction and it's unlikely that one would be entirely dependent on one or the other. It is important to note that anything that cannot be mediated entirely by smart contracts cannot be trustless, which means it has a limited scope given current levels of technology and is likely to be limited to scarce digital goods like p2p storage and processing power. However, as things are increasingly digitized and automated, the applicability of blockchain for everyday transactions increases.

Trustless infrastructure competes with and lowers the cost of trust offline by allowing people to escape local context, essentially making trust more inexpensive by providing an alternative. When transacting from afar, one would have to trust all correspondents

involved in a transaction and trustless infrastructure is an alternative to the due diligence one might have to undertake. Blockchain is therefore an extremely useful tool for transactions even in a stateless context. It is also useful for a lot more than transacting, as it can be used to publicly and transparently track goods in supply chains, set up tokenized governance structures for organizations (DAOs) particularly if members can't coordinate in person, and so on.

Is Crypto Destroying the Environment?

Before we go down this rabbit hole, it's important to note that most blockchains use proof-of-stake, which doesn't consume more energy than any other decentralized computing process and only requires a network of computers to run. Ethereum, the most active blockchain in existence, recently switched over the proof-of-stake, reducing its energy use by more than 99% so we need not say more in this area.

It is only proof-of-work, used by Bitcoin, the largest cryptocurrency by market capitalization, that requires miners to consume energy for the right to build the next block. That said, Bitcoin's environmental impact is generally exaggerated and misinterpreted by its critics, and proof-of-work can incentivize grid stabilization, investment into renewable energy and methane mitigation. Seeing as Bitcoin has and continues to provide value to its users by storing around $600 billion dollars and processing $10-$20 billion dollars in settlements per day, it makes sense to contextualize its energy use rather than disregarding the technology altogether for simply using energy.

To recap on why energy consumption is necessary in PoW, computational work incurs a cost to miners, ensuring that they cannot capture over 51% of hashrate (which allows them to change the history of network and double spend) and disincentivizing them

from validating malicious blocks, which would be rejected by other nodes. Bitcoin's energy consumption is linked to block production and scales with the price of Bitcoin because mining becomes more profitable as prices rise. Therefore, even if a block is empty, it would still be mined. Moreover, off-chain scaling solutions like Lightning mean that a single on-chain transaction can represent thousands of smaller transactions. This means commonly cited metrics like energy cost per transaction is an impractical way of gauging the efficiency of the Bitcoin network as adding or removing transactions would not change energy usage.

Overall, Bitcoin only consumes about 0.4% of the world's energy (this is an annualized figure based on October 2022 data and the estimate varies considerably with hashrate)[11]. However, to get a better sense of Bitcon's environmental impact it makes sense to look at its energy mix (sustainable vs non-sustainable) because energy consumption does not necessarily translate into emissions. Estimates for this vary widely, the Cambridge Center for Alternative Finance (CCAF) estimates that 37.6% or Bitcoin mining is sustainable, while industry estimates from the Bitcoin Mining Council, which disproportionately represents American miners, put it at around 59.5%, which is better than the American average grid of 40% sustainable[12][13]. Bitcoin's energy mix is difficult to determine because miners are highly mobile and often operate in remote regions with cheaper energy. Given that mining is increasingly moving out of China due to a government crackdown, Bitcoin's energy mix is constantly improving and is already far better than the vast majority of other industries.

Another important nuance to Bitcoin's environmental impact are the incentives proof-of-work introduces to the energy indus-

[11] ccaf.io/cbeci/index

[12] www.jbs.cam.ac.uk/insight/2022/what-is-the-environmental-footprint-of-bitcoin/

[13] bitcoinminingcouncil.com/bitcoin-mining-electricity-mix-increased-to-59-5-sustainable-in-q2-2022/