June 2022 **No. 2022: 6**

Cryptocurrencies: Review of Economics and Policy

Working Paper 2022

Sonan Memon, Pakistan Institute of Development Economics, Islamabad

Cryptocurrencies: Review of Economics and Policy

Sonan Memon*

This version: June 2022

Abstract

In this review paper, I begin by discussing crypto's market penetration, legal status and economic opportunities for Pakistan. I mainly focus on the *economics of digital "currencies"*. Some key questions include how does crypto "currency" compare with traditional fiat currencies as a substitute? Which economic problems does it solve currently or has the potential to solve (e.g lowers verification costs and networking costs)? What are its economic limitations (e.g high energy costs, speculative bubbles, prohibitive costs of maintaining incentive compatibility and the blockchain trilemma)? How does widespread adoption of digital currencies change the monetary and fiscal policy paradigm? Which set of regulations are needed from policymakers to address crypto's adverse effects such as accommodating illicit activities and threatening consumer protection? In the appendix, I also provide a brief summary of design features of the technology which underlies cryptocurrencies.

Keywords: Cryptocurrencies: Bitcoin, Ethereum, Tether etc. Blockchain Technology. Economics of Cryptocurrencies. Implications for Fiscal and Monetary Policy. Regulation of Crypto Market.
JEL Classification: E00, E31, E40, E41, E42, E43, E44, E50-E58, E62, F33.

*Research Economist, PIDE, Islamabad. smemon@pide.org.pk

Contents

1. INTRODUCTION

Satoshi Nakamoto[1] invented *"Bitcoin"*, the first successful peer to peer system for decentralized exchange of currencies (see Nakamoto (2008)). Bitcoin is a particular cryptocurrency (crypto) and more than 18000 of these are in existence as of early 2022 Hayes (2022). A crypto, broadly defined is virtual or digital money that takes the form of tokens or *"coins"*. While crypto is the largest market in which blockchain technology is used, the *Web3* encompasses much more and can include broader "decentralized online ecosystems" Korpal and Scott (2022). However, the focus of this brief is on crypto only, not on *Web3* more broadly.

Cryptography in "cryptocurrencies" allows for communications in the presence of *adversaries*. It prevents adversaries[2] from accessing the information-privacy by allowing *secrecy* in transactions. It provides a substitute for *third party* involvement and a fully decentralized system for exchange of digital currencies, free from government control. In principle[3], it can make conventional banking largely irrelevant by replacing it with a technologically superior alternative. This solves the problems of fraud, privacy violation, high verification costs, misuse of market power by dominant banking players and security which exist with conventional banking.

However, the decentralized system also introduces some problems and the current technology is not sufficiently *scalable* to compete with conventional banking. For instance, while Visa can process up to 24,000 transactions per second, Bitcoin can only process 7 and Ethereum can handle only 20 crypto (2020). There are many other concerns regarding market volatility, speculation and limited use in pure economic transactions, which has led some economists to become highly skeptical of this "bubble" (see for instance Krugman (2018), Roubini (2018) and Cochrane (2017)). Nevertheless, in principle some solutions to these limitations may be found in the future.

Apart from Bitcoin, some major market players are Ethereum, Litecoin, Tether, Monero, Dogecoin etc (see Hayes (2022)). There are slight design variations across these in terms of the services they offer. The crypto market capitalization approximately amounts to $1.7 trillion; in every 24 hours, $91 billion worth of cryptos are traded, most of them Bitcoin or Ethereum White et al. (2022). Last year, the estimated crypto ownership rates were an average of 3.9% of global population, with over 300 million users worldwide.

[1] Who he/she/they were is still unknown since Nakamoto is a pseudonym.

[2] Fraudsters or agents who want to hack or interfere with the smoothness of free trade process.

[3] We are far from achieving this at the moment due to economic and technological constraints of current cryptocurrencies.

Over 18,000 businesses are already accepting crypto payments. Some top countries include India (100 million users), USA (27 million), Nigeria and Vietnam tripleA (2022). Next, I will briefly describe the services offered by three major market players, apart from Bitcoin.

For instance, *Ethereum* is a decentralized platform that enables smart contracts and decentralized applications without any downtime, fraud or interference from a third party. It creates decentralized financial products that anyone in the world can freely access, regardless of nationality, ethnicity, or faith. In some countries where state infrastructure is weak, it has the potential to provide bank accounts, loans and a variety of other financial products. Meanwhile, *Stellar* is an open blockchain network designed to provide enterprise solutions by connecting financial institutions for the purpose of large transactions. Huge transactions between banks and investment firms typically take several days, involving a number of intermediaries, and high costs can now be made nearly instantaneously Hayes (2022). On the other hand, *Tether* and other "stablecoins" attempt to smooth out price fluctuations to attract risk-averse users. Tether's price is tied directly to the price of U.S. dollar and allows convenient transfers from other cryptocurrencies back to U.S dollars in a more timely manner than actual conversion to normal currency Hayes (2022).

2. Crypto in Pakistan: Market Size, Policy and Opportunities

It is estimated that more than 9 million people own cryptocurrencies in Pakistan and interest in crypto is dramatically increasing tripleA (2022).

The State Bank of Pakistan (henceforth SBP) stated that "Digital currencies are neither recognized as a Legal Tender nor has it authorized for the issuance, sale, purchase, exchange or investment in Virtual Currencies" Khurshid (2020). The SBP has cautioned against the use of crypto and advised both the public and institutions against dealing in the coins but it is not an *outright* ban. SBP submitted to the Sindh High Court that virtual currencies have become a source of major fraud, targeting vulnerable subsets of population to exploit their urge for earning quick profits, including offer of Ponzi schemes. There are also concerns regarding use for money laundering and terrorism financing. The anonymous nature of these coins makes legal recourse in the case of fraud almost impossible Khurshid (2020).

Meanwhile, Younus (2022) has argued that Pakistan's young talent base has the capability for innovating at home for the global *Web3*[4] ecosystem including crypto. If empowered, this talent can bring in significant foreign exchange earnings, slow the brain drain of top talent, and add billions of dollars to the local economy through additional direct and indirect tax revenues, investment in new businesses, and excess savings in Pakistan. Based on calculations in Younus (2022), this emerging ecosystem can generate almost $100 billion in total income for technology talent over the next 25 years in Pakistan.

3. Economics of Cryptocurrencies

I will discuss some key economic implications of widespread adoption of crypto such as impact on electricity costs, substitution for Fiat currencies and effect on inflation, potential reduction in verification and networking costs of transactions, implication of rent seeking and incentive compatibility, speculation and volatility, as well as the Blockchain Trilemma.

3.1. Energy Consumption

Electricity consumption of Bitcoin has become as high as electricity costs of countries like Denmark and Ireland Sarkodie and Owusu (2022) world wide. For instance, Benetton et al. (2019) found empirical evidence that crypto-mining crowds out other economic activities and may result in net welfare loss. Using data from various cities in China and New York State, Benetton et al. (2019) found large negative externalities of crypto-mining on the local economy, such as distortion to local wages and electricity prices. Given the already existent energy crisis in Pakistan, excessive use of crypto can exacerbate the energy supply shortfall.

The following figure uses data from Cambridge Center For Alternative Finance at *Cambridge University*, depicting monthly electricity consumption data from 2017-2022 for Bitcoin, indicating a dramatic explosion in terawatts of electricity consumed by Bitcoin.

[4] *Web3* includes crypto and other blockchain innovations.

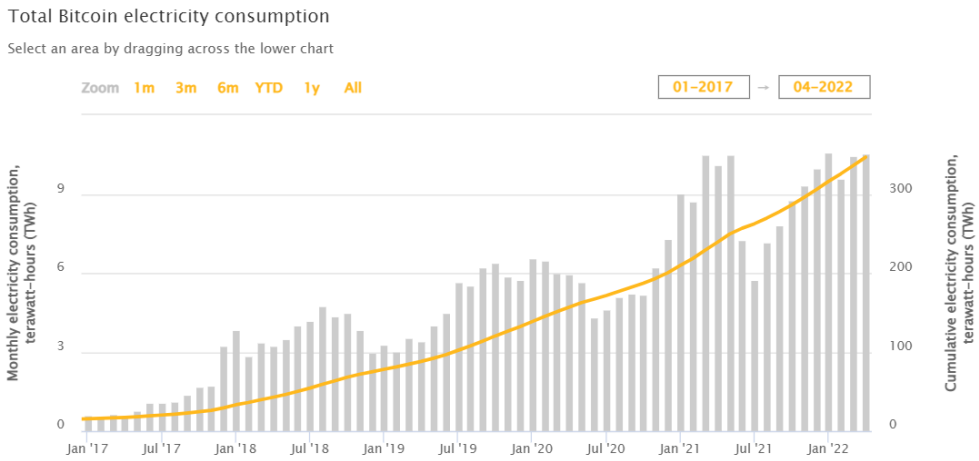

Figure 1: Source is *Cambridge Center for Alternative Finance*

3.2. Bitcoins as Substitutes for Fiat Currencies

Bitcoin is fundamentally a *deflationary* asset, which is why citizens of countries with unstable fiat currencies are increasingly using it as store of value to protect against hyperinflation and rising costs of living. Some major examples of such countries are Venezeula, Iran and El-Salvador Reiff (2021). There is evidence that investors move from fiat currencies to Bitcoin cryptocurrency in environments with low trust and high uncertainty Jin et al. (2021).

Unlike dollars or any other traditional fiat currencies, Bitcoin is designed to have a limited supply which will never exceed 21 million by design Nakamoto (2008), making it an attractive store of value that is resistant to inflation and devaluation by a government or central banks. Figure 2 below shows data from Bloomberg, indicating that since 2011, Bitcoin has deflated by more than 99%. However, there are concerns that Bitcoin is more volatile than traditional *inflation hedging* tools such as gold and currently, there does not exist a sufficiently large sample of data to claim that Bitcoin is deflationary.

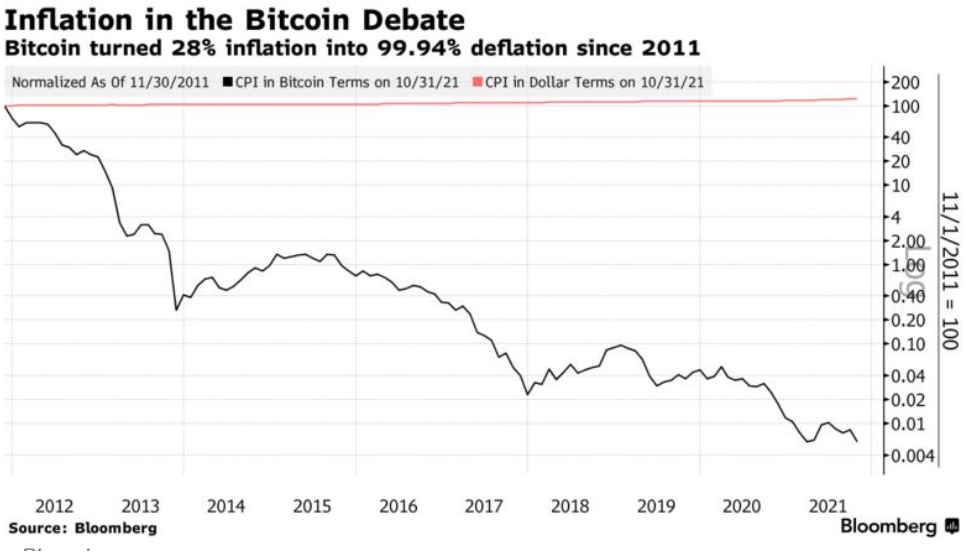

Figure 2: Source is Bloomberg

There is also empirical evidence from time series VAR models[5] that Bitcoin appreciates in response to inflation or inflation expectation shocks, confirming its inflation-hedging property (see Choi and Shin (2022) and Blau et al. (2021)) in line with claims by investors. Meanwhile, Bitcoin prices do not decrease after policy uncertainty shocks, partly consistent with the notion of Bitcoin's independence from government authorities Choi and Shin (2022).

3.3. Verification Costs

For a market exchange, key attributes of a transaction need to be *verified* by the parties involved. When an exchange takes place in person, the buyer can usually directly assess the quality of goods and the seller can verify cash. The only intermediary involved is the central bank, issuing and backing currency. When a transaction is performed online, financial intermediaries broker it by their verification services. These intermediaries add value to marketplaces by reducing *information asymmetry* and the risk of *moral hazard*. In the extreme case where verification costs are prohibitively high, markets unravel and beneficial trades do not take place Catalini and Gans (2020).

In exchange for their services, intermediaries typically charge a fee. This is one of the costs buyers and sellers incur when they cannot verify transaction attributes themselves.

[5]Vector Autoregression Models.

Additional costs may stem from the intermediary having access to transaction data (*privacy risk*), and being able to select which transactions to execute (*censorship risk*). These costs are exacerbated when intermediaries gain market power, often as a result of the informational advantage they develop over transacting parties Stiglitz (2002). Blockchain technology can prevent information leakage by allowing market participants to verify transaction attributes and enforce contracts without exposing the underlying information to a third-party. This allows an agent to verify that the information is true without full access to all background information Catalini and Gans (2020).

3.4. Networking Costs

The cost of networking relates to the ability of operating a marketplace without assigning control to a centralized intermediary. Low networking costs are achieved by combining the ability to cheaply verify state with economic incentives targeted at rewarding those state transitions which are particularly valuable from a network perspective. Blockchains that utilize network effects have the following economic returns.

Firstly, blockchains that utilize network effects are less likely to leave market power in the hands of first movers or early players. This limits the ability of any party to unilaterally censor transactions or exclude participants from the network and removes single points of failure Catalini and Gans (2020). A single point of failure is essentially a flaw in the design that poses a potential risk because it could lead to a situation in which just one malfunction or fault causes the whole system to stop working due to over-reliance on small subsets Noveck (2011).

Secondly, capitalizing on network effects leads to lower *privacy risks* as no single entity (or group) has superior control over the information Catalini and Gans (2020). In traditional platforms, the privacy risk is particularly troublesome in markets which allow intermediaries to access data. This concern is increasingly relevant because of the role that such data plays in the training of modern AI[6] algorithms.

Moreover, blockchain implementations such as permission-less[7] systems which take advantage of the lower cost of networking induce architectural changes, encouraging open opportunities for entrants to experiment with new business models Catalini and Gans (2020). By allowing for the separation of network benefits from the costs of market

[6] Artificial Intelligence.

[7] Bitcoin is an example of a permission-less blockchain which means that the known set of participants are unknown.

power, we can build creative and high quality applications on top of shared data while preserving the privacy of information.

3.5. Implication of Rent Seeking and Incentive Compatibility

The amount of computational power devoted to blockchains such as Bitcoin must simultaneously satisfy two conditions in an economic equilibrium Budish (2018): first, a *zero-profit condition* among miners who engage in rent-seeking while adding the next block to the chain and secondly an *incentive compatibility* condition on the system's vulnerability to a "majority attack". The latter is secured when the computational costs of a majority attack exceed benefits. Together, these two equations (1 and 2) imply that equation 3 holds: the recurring "flow" payments to miners for running the blockchain must be large relative to the one-off "stock" benefits of attacking it. These flow payments are prohibitively high in the current crypto system, as argued by Budish (2018).

Let P_{block} denote the economic reward to the miner who wins the computational tournament. Let c denote the per-block cost of 1 unit of computational power such as electricity and a rental cost for capital equipment. If there are N units of computational power in the network, then each unit has a $\frac{1}{N}$ probability of winning the prize: P_{block}. The equilibrium amount of computational power devoted to blockchain mining N^* is thus characterized by equation 1 below. Equation (1) is the standard characterization of a *rent-seeking tournament*: prize in the tournament P_{block} is dissipated by expenditures aimed at winning the prize N^*c.

$$N^*c = P_{block} \tag{1}$$

Suppose that there exists a majority attack that yields an expected payoff to the attacker of V_{attack} and that has an expected cost to the attacker, net of block rewards of $\alpha \times N^*c$.

Equation (2) below simply says that the costs of manipulating the blockchain $\alpha \times N^*c$ must be greater than the benefits of doing so, V_{attack}. The equation captures what enables the "decentralized trust" of the blockchain system is the computing power devoted to maintaining it. Economically, the key thing to note about equation (2) is that the cost of manipulation V_{attack} is related to the *flow cost* of maintaining the blockchain, i.e., to N^*c.

$$\alpha \times N^*c > V_{attack} \tag{2}$$

In the ideal equilibrium in which participants are honest, the amount of computational power devoted to maintaining the blockchain is characterized by the rent-seeking competition among miners, equation (1). Combining (1) with the incentive compatibility condition (2), we have the following equilibrium constraint (equation 3):

$$P_{block} > \frac{V_{attack}}{\alpha} \tag{3}$$

In sum, the equilibrium per-block payment to miners for running the blockchain must be large relative to the one-off benefits of attacking it. This places potentially serious economic constraints on the applicability of blockchain innovation. By analogy, imagine if users of the Visa network had to pay fees to Visa, every ten minutes that were large relative to the value of a successful one-off attack on the Visa network Budish (2018).

3.6. Speculation, Volatility and Transaction Costs

Some leading economists are very critical of the crypto "bubble" and argue that there is no *fundamental* economic value of this technology. For instance, NYU based economist Nouriel Rubbini argued that "Since the fundamental value of bitcoin is zero and would be negative if a proper carbon tax was applied to its massive pollution, the current bubble will eventually end in another bust" Roubini (2018). Crypto is also not a stable store of value due to its massive volatility and has limited use as a medium of exchange which raises questions over whether it can even be referred to as "currency" in the classical sense.

The first concept of asset pricing is that price equals the expected present value of dividends Cochrane (2009). Bitcoin has no cash dividend, so how does it have value above and beyond cash dividends? If the price is greater than zero, either people see something that acts like a dividend, some value in holding the asset beyond its cash payments or they are willing to hold the asset despite a lower expected return or they think the price will keep going up forever, so that price appreciation alone provides a competitive return. The first explanation represents a "convenience yields" and the latter is a "rational bubble" such as the famous tulip bubble in 17th century Goldgar (2008).

Some of the *convenience yield* of Bitcoin is that it facilitates tax evasion, and allows for illegal voluntary transactions such as drugs, bribes and hiring undocumented workers. Bitcoin is great for avoiding capital controls i.e getting money out of China for instance Cochrane (2017). On top of this fundamental demand, it also has *speculative demand*. Sup-

pose that you know that Bitcoin will go up some more before its inevitable crash. Someone speculating on Bitcoin over a week cares little about its fundamental value since they can make a lot of money in a volatile market over the course of a week if they get on the right side of the volatility Cochrane (2017).

Krugman (2018) argued that in crypto, instead of money created by the click of a mouse, we have money that must be mined through resource-intensive computation, which has high transaction costs. Moreover, crypto, unlike *fiat* money has no backstop to reality Krugman (2018). Their value depends entirely on *self-fulfilling expectations*, which means a total collapse is a real possibility. If speculators were to have a collective moment of doubt, suddenly fearing that Bitcoins were worthless, Bitcoins would become actually worthless.

3.7. BLOCKHAIN TRILEMMA

While the ideal qualities of any record-keeping system are *correctness* of information during exchange, *decentralization* and *cost efficiency*, there exists a *Blockchain Trilemma*, as argued by Abadi and Brunnermeier (2018) (see Figure 3 below) i.e no ledger can satisfy all three properties simultaneously. In particular, decentralization has three main costs: waste of resources, scalability problems and network externality inefficiencies.

In order to understand the blockchain trilemma, one needs to understand why blockchains require a waste of computational resources since this is the most significant of the three costs. Given that virtually anyone can add a public blockchain, a consensus algorithm[8] determines the true history out of possibly different fraudulent reports. The solution proposed by Nakamoto (2008) was to force blockchain writers[9] to perform a computationally intensive *proof of work* [10].

The *free entry* in blockcchains has crucial consequences for how the agents are incentivized. Traditional centralized intermediaries are incentivized against fraud because they lose their franchise value when fraud is detected i.e they are incentivized *dynamically* by their expected future profits. However, blockchain users have no franchise value because free entry implies that their rents are competed away by entrants. Meanwhile, the incentives provided by the *proof of work* are *static* since a block writer weighs the benefits of one-time attack against the cost of adding the block i.e the *flow* of fees paid to honest[11]

[8] See appendix section 6.4.
[9] By writer, we mean agents who add blocks.
[10] See appendix section 6.5.
[11] Agents who are not part of the attack but following honest chain of original blocks.

participants. Therefore, decentralization via free entry leads to a large waste of computational resources[12].

Free entry is also related to the second cost of blockchains: scalability problem. If a blockchain user does not trust any entity to truthfully report the information, that user must store the blockchain in its entirety. For example, Bitcoin, which processes only 7 transactions per second, exceeds 250GB in size due to these scalability problems Abadi and Brunnermeier (2018). In short, the more a blockchain is used, the more costly it is to maintain truly decentralized record-keeping.

Blockchains also allow for a second type of competition which is "forking" i.e a subset of the community wishes to change the rules and add new blocks. Accordingly, the blockchain will split in two: those who adopt the new rules will extend one chain, whereas those who stick to the old rules will ignore that chain and build another[13] one. This type of "fork competition" has a remarkable property that all the information on established ledger is conveniently transferable towards the new growth. Abadi and Brunnermeier (2018) argues that with this type of portability, there is essentially perfect competition among ledgers.

While this fork competition enhances competition, it is the direct cause of the third cost of blockchains, namely, network externality inefficiencies Abadi and Brunnermeier (2018). The ease of switching between branches of a blockchain fork can engender instability and miscoordination. Blockchains may fail to fully exploit network externalities by splitting into several different forks over time. In fact, the two largest crypto blockchains i.e Bitcoin and Ethereum have experienced forks in which substantial portions of the community have abandoned the established chain.

[12] Also see section 3.5 above.
[13] See Appendix 6.4.

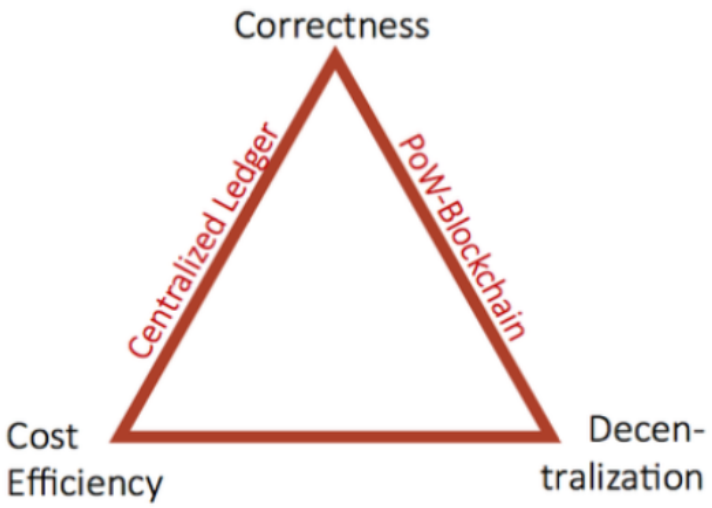

Figure 3: The Blockchain Trilemma (PoW is proof of work)

4. Economic Policy and Cryptocurrencies

How does widespread adoption of cryptos effect economic policies? For instance, how does it change the paradigm of monetary and fiscal policy? Moreover, which regulation interventions should be utilized to address downsides of crypto such as facilitation of illicit activities and threatening consumer protection?

At one extreme, some countries have chosen to completely ban crypto. For instance, China enacted regulation that prohibits crypto trading. On the other end of the spectrum, Australia and Japan have both recognized crypto as a formal means of payment and financial asset Comply (2022). Figure 4 below summarizes legal treatment of crypto around the world.

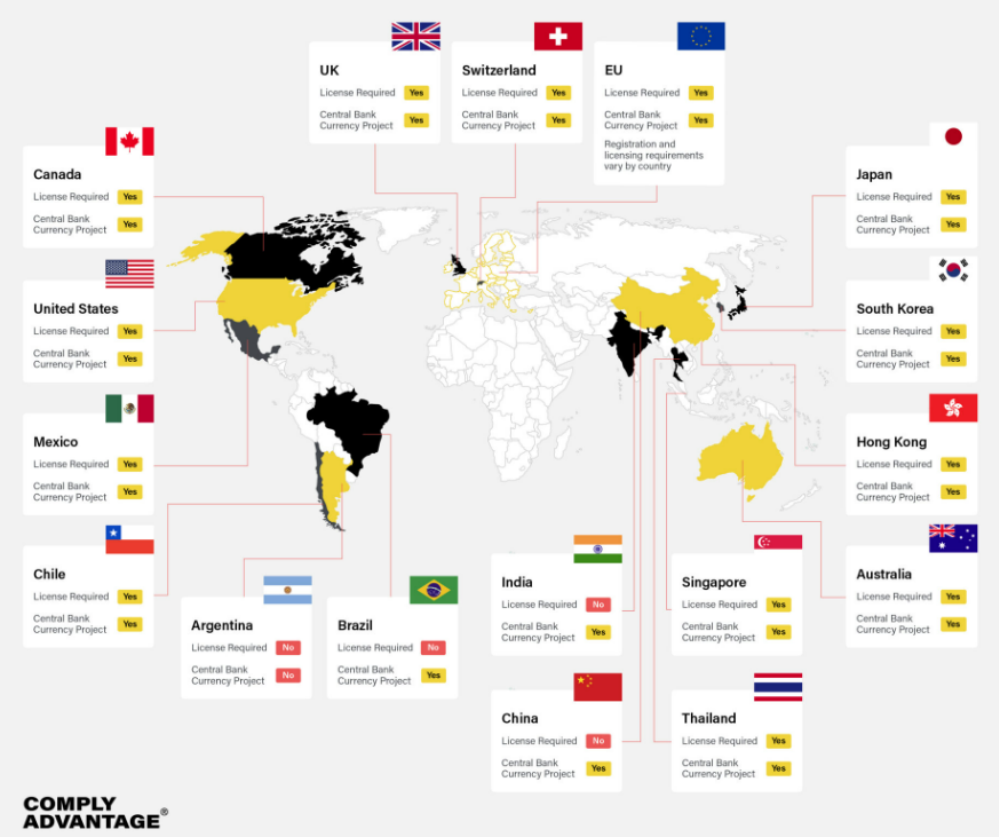

Figure 4: Source is https://complyadvantage.com/insights

4.1. Monetary Policy

Theoretically, there could be a very large impact on monetary policy if crypto replaces conventional currencies. For example, economies that switch heavily from the use of their national currency to crypto would face issues similar to the classic *dollarization* problem (see for instance Calvo (2002)). Such economies would find price levels and interest rates to be determined more by external factors than by national fiscal and monetary policies.

However, for crypto to replace official currencies, it would have to face various challenges. Firstly, the supply should effect the real economy and this will occur when pure economic transactions are performed using this technology. Secondly, in the presence of *fractional reserve banking*, the supply of crypto must respond to the liquidity crises, act as a lender of last resort and maintain financial stability. Thirdly, there is a *principal agent problem* since there needs to be a system of checks and balances to keep the agent i.e the crypto issuer accountable to the principal. However, it is currently not possible to achieve this because of decentralization. Hence, at this point, the official currencies controlled by

inflation-targeting, independent central banks still appear to be a far superior technology than crypto Claeys et al. (2018).

Nevertheless, if societies gain faith in crypto, countries might face a situation similar to the gold standard era when the value of national currencies were fixed to gold. This would also be analogous to a *global monetary union*. For instance, monetary policy could be simultaneously too loose for some countries and too tight for others, with a single policy having different effects on different nations Wyman (2018).

It is also possible that central banks develop their own cryptocurrencies and some have considered it in India for instance. These could be limited to financial institutions or it could be made widely available to the public. Both the Bank of Canada and Singapore Monetary Authority have run pilot projects on this, but have concluded that the technology is still too early to adopt. Policymakers may also look to collect data to monitor the growth of this new market activity and its linkages to the financial system. In the extreme case, regulators could forbid any linkages between the financial institutions and the crypto ecosystem Wyman (2018).

The stability and soundness of the financial system should be maintained through *prudential* regulations[14]. For instance, a cryptoasset that provides equivalent economic functions and poses the same risks compared with traditional assets should be subject to the same requirements as the traditional one. The prudential treatment should, however, account for any additional risks arising from crypt exposures Committee et al. (2021). Secondly, the design of the prudential treatment should be simple since this is still an evolving technology. A simple and cautious treatment could in principle be revisited in the future depending on the evolution of cryptoassets. Thirdly, any committee-specified prudential treatment of cryptoassets would constitute a minimum standard for internationally active banks. Specific jurisdictions would be free to apply additional and/or more conservative measures if warranted Committee et al. (2021).

4.1.1. A Simple Model of Monetary Policy and Cryptocurrency

In a world with only one currency, classical quantity theory yields $y_t = \frac{D_t}{P_t}$. Depending on output y_t, the central bank adjusts the dollar quantity D_t such that the desired dollar price level P_t realizes. If bitcoin is included in the standard model as a substitute for medium of exchange, then Schilling and Uhlig (2019) show that the equilibrium market clearing implies:

[14]Prudential regulation requires financial institutions to comply with requirements to cope with risks associated with their financial activities.

$$y_t = \frac{D_t}{P_t} + \frac{Q_t}{P_t} B_t \tag{4}$$

Holding P_t, y_t and Q_t constant, a deterministic increase in B_t (aggregate bitcoin stock) must be compensated by a corresponding decrease in D_t in equilibrium; in other words, bitcoin block rewards are financed by dollar taxes Schilling and Uhlig (2019). The block rewards, which are earned through mining effort are financed not by deflating the bitcoin currency but by the central bank, which has to accordingly decrease its dollar supply. It does so by imposing dollar lump-sum taxes on the population. Hence, the block rewards are not a tax on bitcoin holders but are financed through dollar taxes imposed by the central bank.

Suppose we start from the equilibrium at point A in Figure 5 below (left) for the dollar quantity D. What happens as the central bank issues the dollar quantity $D^{'}$ instead? One way to label the "conventional scenario" is to think of the Bitcoin price as moving exogenously: in figure 5 (left) this is fixed at $Q = \bar{Q}$. In this case, we get a version of the classic relationship in that the increase in dollar quantity from D to $D^{'}$ leads to a higher price level, moving the equilibrium from point A to point B. Another possibility though, which we label the "unconventional scenario" is to instead fix the price level of dollar at some exogenously given level $P = \bar{P}$: now, increasing the dollar quantity reduces the Bitcoin price, moving the equilibrium from point A to point C.

Conversely, and for the "unconventional" scenario, one may wish to think of the central bank as picking the dollar quantity as D or $D^{'}$ and thereby picking the Bitcoin price to be either Q or $Q^{'}$ (right end of Figure 5).

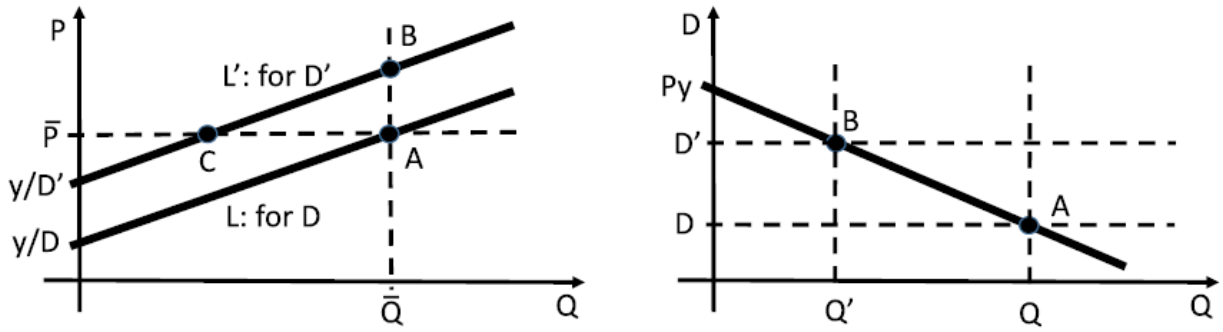

Figure 5: Source is Schilling and Uhlig (2019).

4.2. Impact on Fiscal Policy

When a government or its central bank, creates money, it is essentially able to buy things for little or no cost. This has an immediate fiscal benefit by reducing the need to borrow or tax to buy the same goods. Estimates of the annual value of this *seigniorage* in the US range from about $30 billion to $90 billion Wyman (2018), equivalent to about one or two percent of the federal budget. Total seigniorage from different sources has been an average of 164 billion rupees per year in Pakistan Rao (2011). This benefit would be at least partially at risk if cryptocurrencies come to substitute for national currency in the future.

The threat of crypto to the integrity of a country's fiscal policy is sustainable because of their high usefulness for tax evasion. They possess some of the most crucial characteristics of a traditional *tax haven* since there is no jurisdiction in which they operate due to anonymity and are not subject to taxation at source Obu (2021).

4.3. Regulation

4.3.1. Introduction

Earlier this year, the International Monetary Fund (IMF) released data indicating a correlation between bitcoin and the S&P 500 index Adrian et al. (2022). This raises fears of spillover of investor sentiments between the stock market and crypto. Moreover, the nature of underlying technology enables cross-border transactions without financial intermediaries, which creates risks for volatility and spill over effects White et al. (2022).

While some countries such as India have amended existing laws, other interventions seemingly favored by the European Union and UAE propose setting up entirely new regulators to deal with the industry. For a truly global, *coordinated* approach, countries must work together, leveraging best practices and learning from each other. As well as risk assessments and establishing common standards, there is also a pressing need to develop fit for purpose and inclusive solutions, through public-private collaboration White et al. (2022).

Nabilou (2019) argues that the focus of regulating decentralized crypto should be shifted toward the upper layers (i.e the application layers) upon which businesses are being developed. It is likely that certain levels of centralization in the upper layers would emerge, creating opportunities for regulators if the banking and payment systems play

the role of *policy surrogates*. This indirect regulatory approach can achieve decentralization along with increase in effectiveness and efficiency of regulation.

Next, I focus on options available for curbing illicit activities and consumer protection challenges emerging from cryptocurrencies.

4.3.2. Illicit Activities

Critical attention should be paid to the risk and prevention of illicit activity, such as *money laundering*, *tax evasion* and *terrorism financing*.

Policy tools include increasing the level of monitoring and tracking in addition to actions against various parties including criminal penalties or banning/shutting down certain market participants if they are guilty of illicit activity. It could also be helpful for transactions to flag risky activity and "blacklist" certain users, helping mitigate harmful activity without requiring traditional identity documentation WEF (2021a). Supervision of compliance with these obligations and building law enforcement capacity to investigate suspected illicit activity is needed. For instance, the Financial Action Task Force (FATF) recommendations of 2021 explicitly require regulation of digital currencies FATF (2021).

Moreover, public-private cooperation for sharing information on illicit finance risks could be constructive to address the risks. As an example, the US Treasury Department's "*FinCEN*" has established a virtual currency information-sharing initiative with participation from the private sector including virtual currency money transmitters WEF (2021a).

4.3.3. Consumer Protection

Most ordinary consumers do not understand the difference between public money (fiat currencies, backed by central bank) and private money (money held in commercial bank deposits). It is likely that firms in the blockchain industry will provide products and services that are similar in nature to those used by consumers today. This similarity can be misleading as consumers may not understand the different protections (or lack thereof) that apply to different payment services (see for instance WEF (2021a) and WEF (2021b)). The most pressing consumer risks from the technology are displayed in Figure 6 below and some of them are discussed next.

Figure 6: Source is WEF (2021a).

Depositor Protection

Deposit insurance protects consumers from the risk of bankruptcy of financial institutions. When it comes to digital currencies, there are two layers of consumer risks. Firstly, the risks of bankruptcy of the service provider and secondly the risk of bankruptcy of the deposit-taking institution. To address the first risk, countries often require service providers to be sufficiently funded and to set aside a certain percentage of their fund liabilities in a custodian account with a deposit-taking financial institution. In the case of the bankruptcy of depository institutions, consumers may only get back a subset of their money unless the currency providers are sufficiently capitalized WEF (2021a).

Payment Risks

Different payment methods carry different consumer protections. For example, cash is 100% guaranteed by a central bank, and typically carries the status of legal tender.

A *push* transaction refers to a transaction initiated by the payer, who needs to know the name of the payee's financial institution and their account number. Meanwhile, *pull* transaction refers to a transaction where it is initiated by the payee and the payee needs

to know the name of the payer's financial institution and account information. While both types are subject to *cybersecurity* risks, a push transaction is fundamentally less risky than a pull transaction for both the payer and the payee, since only the account with sufficient funds governs the transaction. In contrast, a pull transaction could *bounce* because the payee has no visibility of the balance of payer. Currently, it is debatable among economists whether transactions made in crypto will be push-only transactions, given the technology may enable automatic payment upon fulfillment of certain conditions. Depending on their technical choice and how accounts are structured, crypto may facilitate either push or pull transactions WEF (2021a). If the latter are chosen, payment risks will increase.

Privacy Risk

Given that crypto is typically privately operated, it is vulnerable to business models prevalent in the technology industry. For example, this may include business practices developed in unregulated environments or include models without privacy protection. Given the highly personal nature of transaction data, transparency is of significant importance. Moreover, for some crypto markets, a further risk to privacy has emerged in the form of *surveillance* by blockchain analysis companies. These are organizations that analyze on-chain transactions and can match such data with other publicly available data. A variety of crypto ledgers are already under significant surveillance by such organizations (see WEF (2021a)).

Policy for Consumer Protection

The policy tools available for consumer protection include setting minimum standards for privacy protection, information sharing and safeguards against cyber-risks Wyman (2018). To minimize potential negative impacts of stablecoins on consumers, it is important to carry out *consumer education* to ensure people understand risks as well as their legal rights. Effective consumer education would include highlighting the different risks that stablecoins present compared not only to other stablecoins and digital currencies but also to existing currency options. Consumer education needs to be carried out by neutral and trusted parties to ensure a consistent and objective approach, free of marketing incentives WEF (2021a).

Setting limits to the size of transactions and wallet balances to limit the risk exposure of consumers is another option. As new firms come to market with a stablecoin, consideration should be given to the regulatory umbrella under which these services will be provided, as well as which functionaries will be responsible within this framework for the procedural implementation and authorization of regulations WEF (2021a).

5. CONCLUSION

Cryptocurrencies have massive potential to revolutionize the record-keeping of financial transactions and ownership data. Some have even argued that distributed ledger technologies have the potential to be as ground-breaking as the invention of double-entry book keeping in 14th century Italy Abadi and Brunnermeier (2018).

Some key economic issues are electricity costs, high costs of maintaining incentive compatibility and rent seeking, low scalability, high volatility and the Blockchain Trilemma. These constraints limit the extent to which the technology will penetrate the society but also create economic costs when there is widespread adoption. Meanwhile, some major potential economic benefits are substitution for un-trustworthy fiat currencies, low verification and potentially low networking costs, as well as privacy and secrecy in transactions, which are not attainable with current fiat currencies.

In the policy domain, widespread adoption of crypto has deep consequences for effectiveness of monetary and fiscal policy. Moreover, crypto introduces various other policy challenges such as cybersecurity, consumer protection risks and proliferation of illicit activities. Regulatory policies are needed to address these downsides. We need to learn a lot more about how to best design policy for the crypto domain at a brisk pace, given the rapidly evolving technology in Pakistan and beyond.

Appendix

6. BASIC FEATURES OF TECHNOLOGY

In their ground breaking paper Nakamoto (2008) described the basic principles of this system. I will provide a brief overview of the key technological innovations and design features of Bitcoin. If you have deep knowledge of the design features of cryptocuurency, you may skip this appendix. For more detailed understanding, one useful reference point is the MIT lecture series on Blockchain and Money:

(see https://www.youtube.com/watch?v=EH6vE97qIP4).

6.1. WHAT IS A BLOCKCHAIN?

A blockchain is a time stamped, append only data base, shared by nodes of a computer network and secured by cryptography.

It electronically stores information, making it secure and decentralized, requiring no trusted third party intervention. By structuring data into chunks or blocks that are strung together, it inherently makes an *irreversible* timeline of data when implemented in a decentralized nature. When a block is filled, it is set in stone and becomes a part of this timeline.

Each block in the chain is given an exact *time stamp* when it is added to the chain and new blocks can be added but previous ones cannot be edited, making it *append only*. Figure 7 illustrates this process where a chain of blocks has formed, with the help of hash functions.

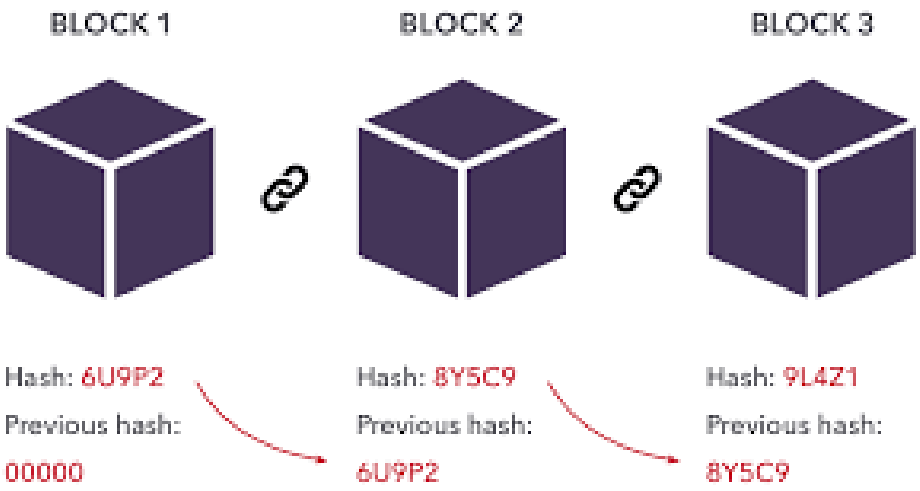

Figure 7

6.2. What are Hash Functions?

Hash functions allow appending the next blocks to previous blocks in a blockchain by compression of data, allowing tamper resistance and credibility.

It creates a digital footprint of the data by mapping the input data into a fixed array, similar to how zip codes work. A hash is a deterministic function, meaning that it always give the same hash for a given input. They make it infeasible though not impossible to determine the array of underlying private data from the public hash i.e it is infeasible that two sets of inputs x and y hash into the same output i.e $hash(x) = hash(y)$.

There is also an *avalanche* effect, implying that a small change in x changes the hash completely, which adds to its security. Figure 8 illustrates this process where the true, deep, underlying data is transformed and compressed into a hashed text by using the particular hash function, SHA-2. Refer to the following resource for further understanding: https://www.youtube.com/watch?v=160oMzblY8.

Figure 8

6.3. Public Key and Private Key

Several suitable mathematical functions such as *prime number exponentiation* and *elliptic curve multiplication* are used by Bitcoin. These functions are "practically" irreversible, meaning that they are easy to calculate in one direction and infeasible to calculate in the opposite one. Based on these functions, cryptography enables the creation of digital secrets and digital signatures, practically immune from forgery.

In bitcoin, we use public key cryptography to create a key pair that controls access to bitcoin. The key pair consists of a private key and *derived* from it is a unique public key. The public key is used to receive funds, and the private key is used to sign transactions to spend them. This signature can be validated against the public key without revealing the private key.

When spending bitcoin, the current bitcoin owner presents her public key and signature in a transaction to spend bitcoin. Through the presentation of the public key and signature, everyone in the network can verify and accept the transaction as valid, confirming ownership at the time of transfer Andreas et al. (2022). This *encryption* and *decryption* process is illustrated in Figure 9.

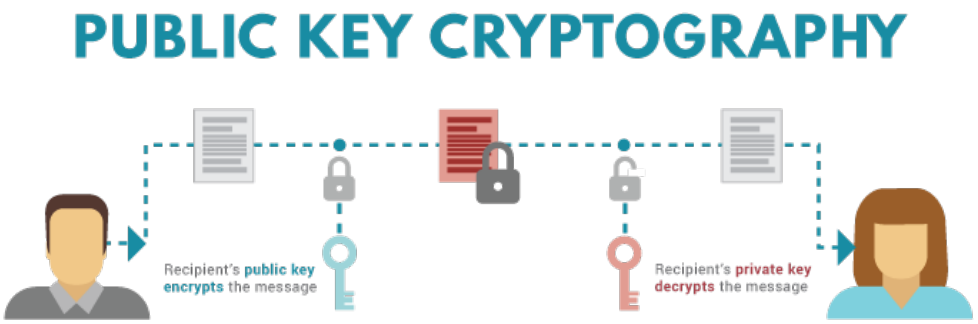

Figure 9

6.4. Majority Consensus

A majority social consensus will make stale blocks (for instance, the purple blocks in Figure 10) or *forks* irrelevant unless these forks continue a long time. Sometimes the alternative, purple block chain becomes so long that it forms its own native currency. Normally the majority consensus will make stale blocks irrelevant over time, which makes the system secure against attacks.

However, the possibility of a majority attack, i.e 51% attack always remains in principle. If the system becomes more centralized or attackers collaborate with each other, then a majority attack becomes more likely. If majority attacks occur, then the security of system becomes compromised.

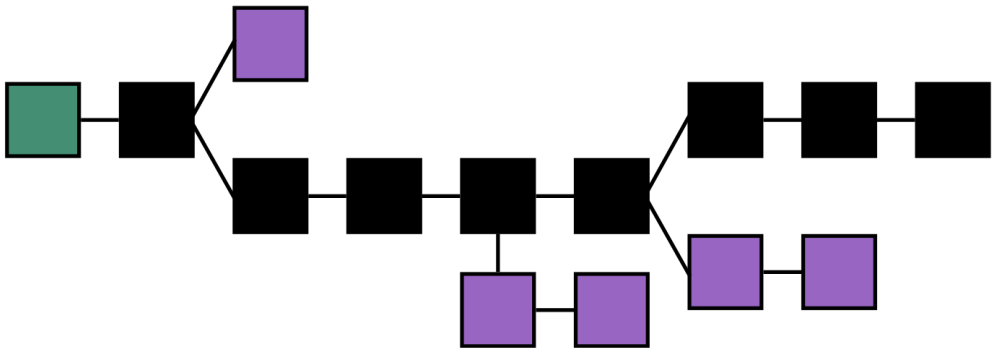

Figure 10: Black Path is Consensus

6.5. BYZENTINE GENERAL'S PROBLEM

A *Byzentine General Problem* (see Figure 11) occurs when malicious actors or somebody who doesn't get the right information can lead to coordination failures and defeat. This is fundamentally a game theory problem.

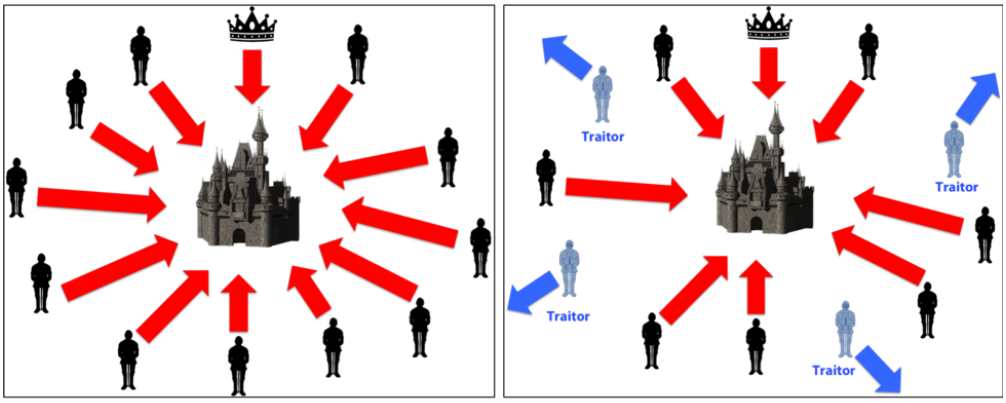

Figure 11

This concept captures the complexity of a decentralized system in achieving a consensus on one truth. The central banking system "solves" this problem by evading it or by allocating trust to a third party or central authority, which is vulnerable to corruption. For instance, the central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of this trust.

Bitcoin uses a proof of work mechanism (explained next) to solve the Byzentine General's Problem. As a monetary system, Bitcoin needed a way to manage ownership and prevent double spends[15]. If all members of the Bitcoin network, called nodes, could agree on which transactions occurred and in what order, they could verify ownership and establish a functioning, trust-less money without a centralized authority. By doing so, the *Byzentine General Problem* is solved.

6.6. PROOF OF WORK

In order to add blocks to the blockchain, a member of the network must publish *proof* that they invested considerable work into creating the block. This incentivizes them to

[15]When a single set of currency assets are used for multiple transactions, it is called the double spending problem.

publish honest information since the proof of work problem is computationally intensive and non-trivial to solve (see Figure 12).

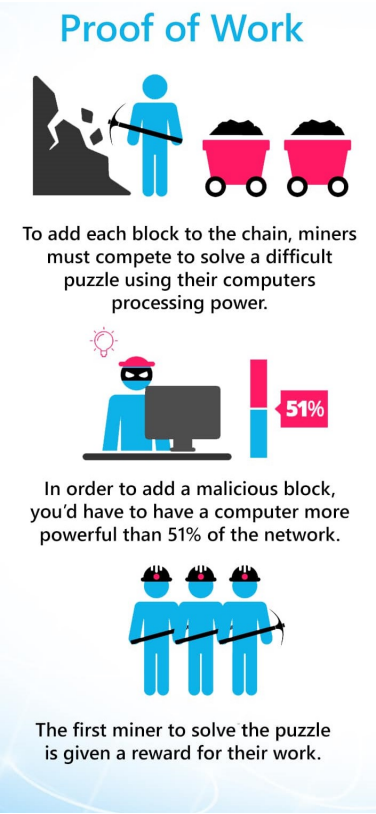

Figure 12

If any member of the network attempts to broadcast false information, all nodes will immediately recognize it as objectively invalid and ignore it. Since each node can verify all information on the Bitcoin network itself, there is no need to trust other members of the network, making Bitcoin a trust-less system. However, if oligopolistic miners control most bitcoin mining Roubini (2018) and many are out of reach for law enforcement in places such as China, Russia and Belarus, it will limit the extent to which the system is decentralized.

The Bitcoin *proof of work* difficulty is defined with respect to leading zeros in the hash function. Nakamoto (2008) designed it such that after every two weeks, the difficulty increases. For example, the mining difficulty in February 2022 hit an all time high of 27.97 trillion hashes while the hash rate was 186.77 (EH/s) (where 1 exahash (EH) = 1 quintillion hashes) Vaca (2022). The difficulty has exponentially increased over time; for instance, it was 7 trillion times harder to solve the puzzle in 2019 as compared to 2010

Hacioglu (2020). Figure 13 below shows the recent increase in network difficulty level Vaca (2022).

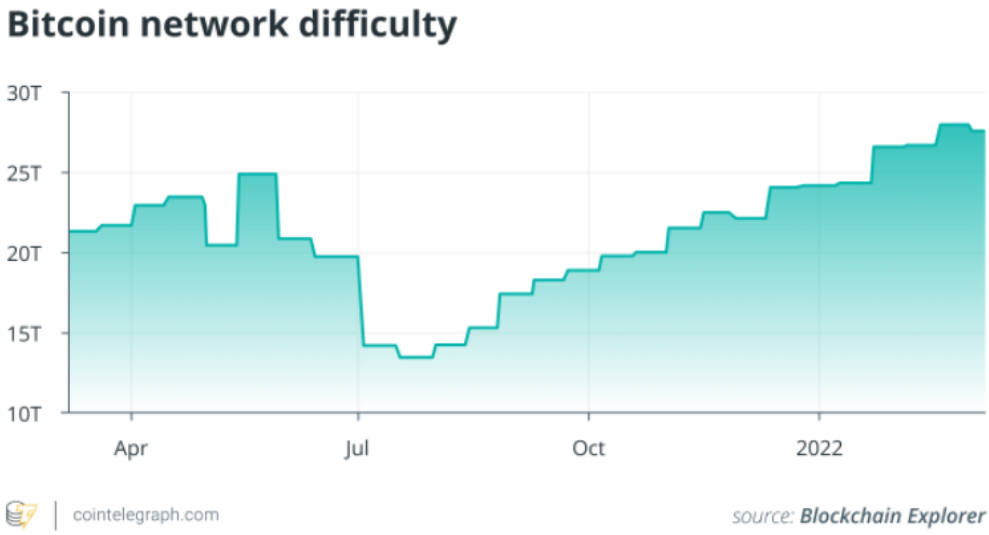

Figure 13: T refers to trillian hashes

REFERENCES

Abadi, Joseph and Markus Brunnermeier, "Blockchain economics," Technical Report, National Bureau of Economic Research 2018.

Adrian, Tobias, Tara Iyer, and Mahvash Qureshi, "Crypto Prices Move More in Sync With Stocks, Posing New Risks," *IMF, January*, 2022, *11*.

Andreas, M et al., "Mastering Bitcoin Programming the Open Blockchain," 2022.

Benetton, M, Compiani G, and A. Worse, "Cryptomining: Local evidence from China and the US," *Working Paper*, 2019.

Blau, Benjamin M, Todd G Griffith, and Ryan J Whitby, "Inflation and Bitcoin: A descriptive time-series analysis," *Economics Letters*, 2021, *203*, 109848.

Budish, Eric, "The economic limits of bitcoin and the blockchain," Technical Report, National Bureau of Economic Research 2018.

Calvo, Guillermo A, "On dollarization," *Economics of transition*, 2002, *10* (2), 393–403.

Catalini, Christian and Joshua S Gans, "Some simple economics of the blockchain," *Communications of the ACM*, 2020, *63* (7), 80–90.

Choi, Sangyup and Junhyeok Shin, "Bitcoin: An inflation hedge but not a safe haven," *Finance Research Letters*, 2022, *46*, 102379.

Claeys, Grégory, Maria Demertzis, and Konstantinos Efstathiou, "Cryptocurrencies and monetary policy," Technical Report, Bruegel Policy Contribution 2018.

Cochrane, John, "Bitcoin and bubbles," *The Grumpy Economist*, 2017.

Cochrane, John H, *Asset pricing: Revised edition*, Princeton university press, 2009.

Committee, Basel et al., "Prudential Treatment of Cryptoasset Exposures," *Basel Committee on Banking Supervision, BIS Consultative Document*, 2021.

Comply, Advantage, "Cryptocurrency Regulations Around The World," in "in," Comply Advantage, 2022.

crypto, "A Deep Dive Into Blockchain Scalability," *crypto.com*, 2020.

FATF, "Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers," *Available at SSRN 3995013*, 2021.

Goldgar, Anne, "Tulipmania," in "Tulipmania," University of Chicago Press, 2008.

Hacioglu, Umit, "Digital business strategies in blockchain ecosystems," *Springer International Publishing, DOI*, 2020, *10*, 978–3.

Hayes, Adam, "10 important Cryptocurrencies Other Than Bitcoin," *Investopedia*, 2022.

Jin, Xuejun, Keer Zhu, Xiaolan Yang, and Shouyang Wang, "Estimating the reaction of Bitcoin prices to the uncertainty of fiat currency," *Research in International Business and Finance*, 2021, *58*, 101451.

Khurshid, Jamal, "State Bank did not declare crypto currency illegal, SHC told," *The News*, 2020.

Korpal, Gaurish and Drew Scott, "Decentralization and web3 technologies," 2022.

Krugman, Paul, "Transaction costs and tethers: why IâĂŹma crypto skeptic," *The New York Times*, 2018, *21.*

Nabilou, Hossein, "How to regulate bitcoin? Decentralized regulation for a decentralized cryptocurrency," *International Journal of Law and Information Technology*, 2019, *27* (3), 266–291.

Nakamoto, Satoshi, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008, p. 21260.

Noveck, Beth Simone, "The single point of failure," in "Innovating government," Springer, 2011, pp. 77–99.

Obu, Osiebuni, "Fiscal Policy and Private Money," *Available at SSRN 3995013*, 2021.

Rao, Nasir Hamid, "Seigniorage Revenues in Pakistan," *SBP Research Bulletin*, 2011, *7* (2), 43–50.

Reiff, Nathan, "How Fiat Currency Crises Drive Nations Toward Cryptocurrencies," *Investopedia*, 2021.

Roubini, Nouriel, "Blockchain's broken promises," *Project Syndicate*, 2018, *26.*

Sarkodie, Samuel Asumadu and Phebe Asantewaa Owusu, "Dataset on bitcoin carbon footprint and energy consumption," *Data in Brief*, 2022, p. 108252.

Schilling, Linda and Harald Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, 2019, *106*, 16–26.

Stiglitz, Joseph E, "Information and the Change in the Paradigm in Economics," *American economic review*, 2002, *92* (3), 460–501.

tripleA, "Cryptocurrency Across the World," 2022.

Vaca, Inigo, "While Bitcoin price starts 2022 with a slump, mining difficulty is on the rise," 2022.

WEF, "Digital Currency Governance Consortium, White Paper Series," Technical Report, World Economic Forum November 2021.

_ , "Navigating Cryptocurrency Regulation: An Industry Perspective on the Insights and Tools Needed to Shape Balanced Crypto Regulation," Technical Report, Global Future Council on Cryptocurrencies, World Economic Forum September 2021.

White, Kathryn, Arushi Goel, and Sandra Waliczek, "Cryptocurrency regulation: where are we now, and where are we going?," Technical Report, World Economic Forum 2022.

Wyman, Oliver, "Cryptocurrencies and Public Policy: Key Questions and Answers," Technical Report, Marsh and McLennan Companies 2018.

Younus, Uzair, "Realizing the Promise and Potential of "Web3" for Pakistan," *Atlantic Council, South Asia Center*, 2022.