CRYPTOCURRENCY

PIDE Working Papers
No. 2022:7

Cryptocurrencies: Review of Economics and Policy

Sonan Memon

Pakistan Institute of Development Economics
Islamabad, Pakistan

E-mail: publications@pide.org.pk
Website: http://www.pide.org.pk
Fax: +92-51-9248065

Designed, composed, and finished at the Publications Division, PIDE.

PIDE Working Papers
No. 2022:7

Cryptocurrencies: Review of Economics and Policy

Sonan Memon
Pakistan Institute of Development Economics, Islamabad.

PAKISTAN INSTITUTE OF DEVELOPMENT ECONOMICS
ISLAMABAD
2022

C O N T E N T S

List of Table

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"*. Key questions include how does crypto "currency" compare with traditional fiat currencies as a substitute? Which economic problems does it currently solve or have the potential to solve (e.g. lowers verification 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 the 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 summarise the design features of the technology that underlies cryptocurrencies.

JEL Classification: E00, E31, E40, E41, E42, E43, E44, E50-E58, E62, F33.

Keywords: Cryptocurrencies: Bitcoin, Ethereum, Tether etc. Blockchain Technology. Economics of Cryptocurrencies. Implications for Fiscal and Monetary Policy. Regulation of Crypto Market.

INTRODUCTION[1]

Satoshi Nakamoto[2] invented *"Bitcoin"*, the first successful peer to peer system for decentralised exchange of currencies (see, Nakamoto, 2008). Bitcoin is a particular cryptocurrency (crypto), and more than 18000 of these exist as of early 2022 Hayes (2022). 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 "decentralised 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[3] from accessing information privacy by allowing *secrecy* in transactions. It provides a substitute for *third party* involvement and a fully decentralised system for the exchange of digital currencies, free from government control. In principle,[4] it can make conventional banking largely irrelevant by replacing it with a technologically superior alternative. Such as alternative solves the problems of fraud, privacy violation, high verification costs, misuse of market power by dominant banking players and security that exist with conventional banking.

However, the decentralised 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 (2022). 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 their services. The crypto market capitalisation 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 averaged 3.9% of the global population, with over 300 million users worldwide. Over 18,000 businesses are already accepting crypto payments. Some top countries include India (100 million users), the USA (27 million), Nigeria and Vietnam triple-A (2022). Next, I will briefly describe the services offered by three major market players, apart from Bitcoin.

---

[1]See https://github.com/sonanmemon for LaTeX version.

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

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

[4]We are far from achieving this due to economic and technological constraints of current cryptocurrencies.

For instance, *Ethereum* is a decentralised platform that enables smart contracts and decentralised applications without downtime, fraud, or interference from a third party. It creates decentralised 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 large transactions. Huge transactions between banks and investment firms typically take several days, involving several intermediaries, and high costs can now be made nearly instantaneously Hayes (2022).

On the other hand, *Tether* and other "stable coins" attempt to smooth out price fluctuations to attract risk-averse users. Tether's price is tied directly to the price of the U.S. dollar. It allows convenient transfers from other cryptocurrencies back to U.S dollars in a timely manner than actual conversion to regular currency Hayes (2022).

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 triple-A (2022).

The State Bank of Pakistan (henceforth SBP) stated that "Digital currencies are neither recognised as a Legal Tender nor has it authorised for the issuance, sale, purchase, exchange or investment in Virtual Currencies" Khurshid (2022). 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 had become a source of significant fraud, targeting vulnerable subsets of the population to exploit their urge to earn quick profits, including the offer of Ponzi schemes. There are also concerns regarding the use for money laundering and terrorism financing. The anonymous nature of these coins makes legal recourse in the case of fraud almost impossible Khurshid (2022).

Meanwhile, Younus (2022) has argued that Pakistan's young talent base has the capability to innovate at home for the global *Web3*[5] 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.

Economics of Cryptocurrencies

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

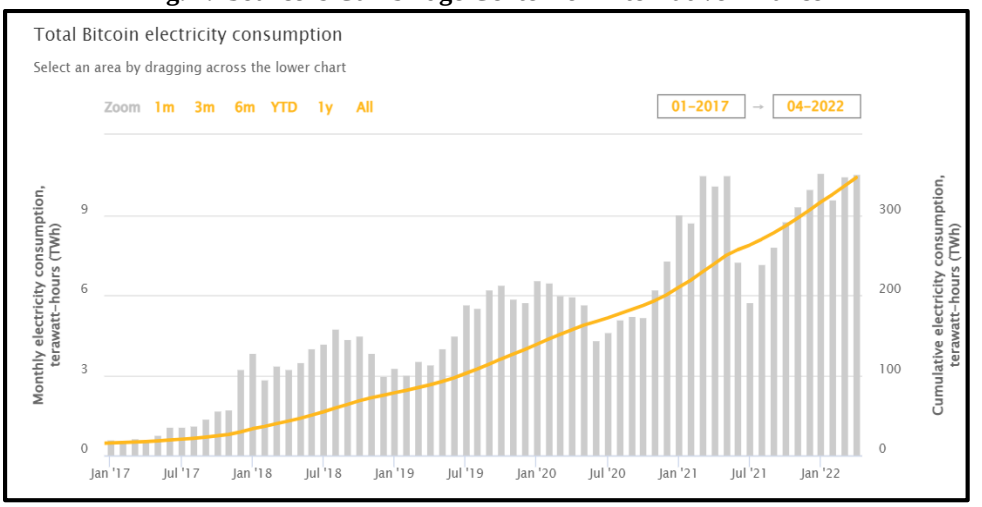
[5] *Web3* includes crypto and other blockchain innovations.

Energy Consumption

Electricity consumption of Bitcoin has become as high as electricity costs of countries like Denmark and Ireland Sarkodie and Owusu (2022) worldwide. 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 significant negative externalities of crypto-mining on the local economy, such as distortion of local wages and electricity prices. Given Pakistan's already existent energy crisis, the excessive use of crypto can exacerbate the energy supply shortfall.

The following figure uses data from the "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.

Fig. 1. Source is Cambridge Center for Alternative Finance



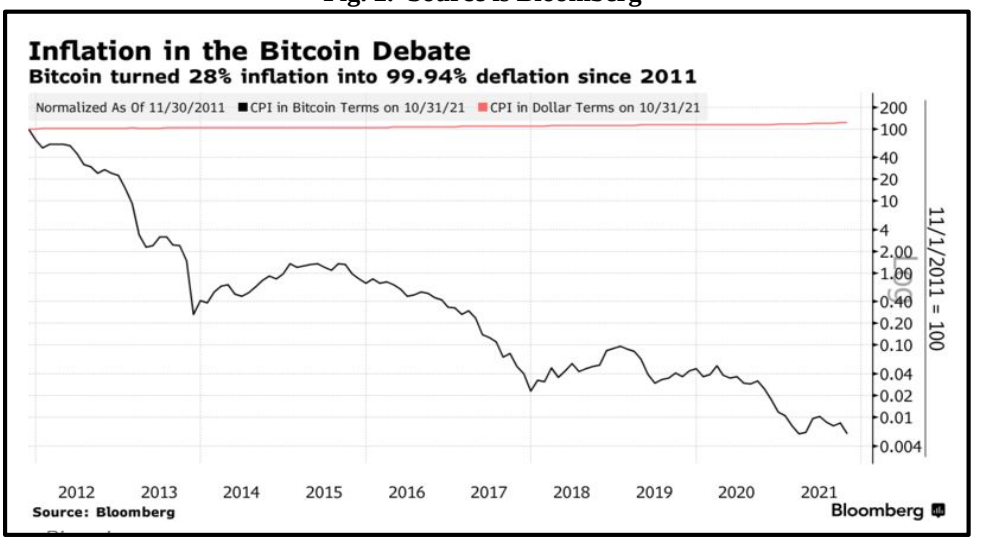
Bitcoins as Substitutes for Fiat Currencies

Bitcoin is fundamentally a *deflationary* asset, so citizens of countries with unstable fiat currencies are increasingly using it as a store of value to protect against hyperinflation and rising costs of living. Some major examples of such countries are Venezuela, 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 that will never exceed 21 million by design Nakamoto (2008), making it an attractive store of value. It 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 percent. However, there are concerns that Bitcoin is more volatile than traditional *inflation hedging* tools such as gold. Currently, there is not a sufficiently large sample of data to claim that Bitcoin is deflationary.

Fig. 2. Source is Bloomberg



There is also empirical evidence from time-series VAR models[6] 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).

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 the currency. When a transaction is performed online, financial intermediaries broker through 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 occur (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. Additional costs may stem from the intermediary having access to transaction data (*privacy risk*) and selecting which transactions to execute (*censorship risk*). These costs are exacerbated when intermediaries gain market power, often because of their informational advantage 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 part This allows an agent to verify that the information is accurate without full access to all background information Catalini and Gans (2020).

[6]Vector Autoregression Models.

Networking Costs

The cost of networking relates to the ability to operate a marketplace without assigning control to a centralised intermediary. Low networking costs are achieved by combining the ability to cheaply verify states with economic incentives to reward those state transitions that are particularly valuable from a network perspective. Blockchains that utilise network effects have the following economic returns.

Firstly, blockchains that utilise 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 censor transactions or exclude participants from the network unilaterally 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, capitalising 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 A.I.[7] algorithms.

Moreover, blockchain implementations such as permission-less[8] 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 power, we can build creative and high, quality applications on top of shared data while preserving the privacy of information.

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: that 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 characterised by equation 1 below. Equation (1) is the standard characterisation of a *rent-*

[7]Artificial Intelligence.

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

seeking tournament: prize in the tournament P_{block} is dissipated by expenditures aimed at winning the prize N^*c.

$$N^*c = P_{block}$$

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 reward 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 "decentralised 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.

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

In the ideal equilibrium in which participants are honest, the amount of computational power devoted to maintaining the blockchain is characterised 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):

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

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).

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 Roubini 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 think the price will keep appreciating, so that 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, such as getting money out of China for instance Cochrane (2017). On top of this fundamental demand, it also has *speculative*

demand. Suppose that you know that Bitcoin will go up more before its inevitable crash. Someone speculating on Bitcoin for a week cares little about its fundamental value since they can make a lot of money in a volatile market over 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, unlike fiat money, crypto 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 worthless.

Blockchain Trilemma

While the ideal qualities of any record-keeping system are *correctness* of information during exchange, *decentralisation* 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. Decentralisation has three main costs: waste of resources, scalability problems and network externality inefficiencies.

To understand the blockchain trilemma, one must understand why blockchains require a waste of computational resources since this is the most significant of the three costs. Since virtually anyone can add a public blockchain, a consensus algorithm[9] determines the true history out of possibly different fraudulent reports. The solution proposed by Nakamoto (2008) was to force blockchain writers[10] to perform a computationally intensive *proof of work* [11].

The *free entry* in blockchains has important consequences for how the agents are incentivised. Traditional centralised intermediaries are incentivised against fraud because they lose their franchise value when fraud is detected i.e. they are incentivised *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 a one-time attack against the cost of adding the block i.e. the *flow* of fees paid to honest[12] participants. Therefore, decentralisation via free entry leads to a large waste of computational resources.[13]

Free entry is also related to the second cost of blockchains: the scalability problem. If a blockchain user does not trust any entity to report the information truthfully, 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 costlier it is to maintain truly decentralised 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

[9]See appendix Section 6.4.

[10]By writer, we mean agents who add blocks.

[11]See appendix Section 6.5.

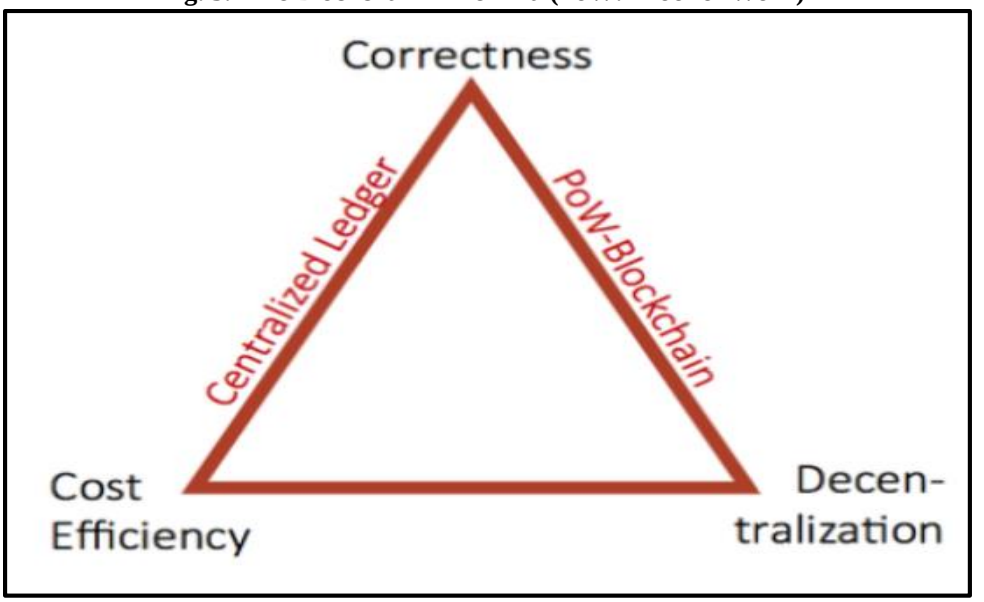
[12]Agents who are not part of the attack but following honest chain of original blocks.

[13]Also see Section 3.5 above.

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[14] 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) argued that there is essentially perfect competition among ledgers with this type of portability.

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. 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.

Fig. 3. The Blockchain Trilemma (PoW: Proof of Work)



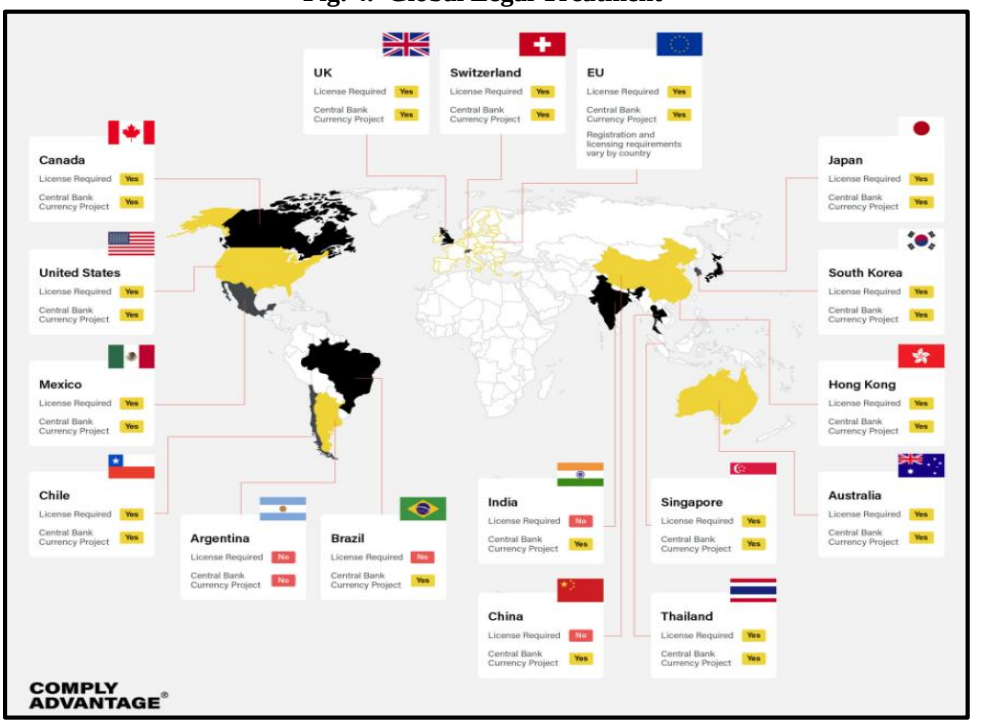
Economic Policy and Cryptocurrencies

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

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

[14]See Appendix 6.4.

Fig. 4. Global Legal Treatment



Monetary Policy

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

However, for crypto to replace official currencies, it would face various challenges. Firstly, the supply should affect 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 decentralisation. Hence, at this point, the official currencies controlled by inflation-targeting, independent central banks still appear to be a far superior technology to crypto Clayes, 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 cryptocurrencies, and some have considered it in India. These could be limited to financial institutions, or it could be made widely available to the public. The Bank of Canada and the 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[15]. For instance, a crypto-asset 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. However, the prudential treatment should account for any additional risks arising from crypt exposures Committee, et al. (2021). Secondly, the design of the prudential treatment should be uncomplicated 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 crypto-assets. Thirdly, any committee-specified prudential treatment of crypto-assets 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).

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 realises. If bitcoin is included in the standard model as a substitute for a medium of exchange, then Schilling and Uhlig (2019) show that the equilibrium market clearing implies:

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

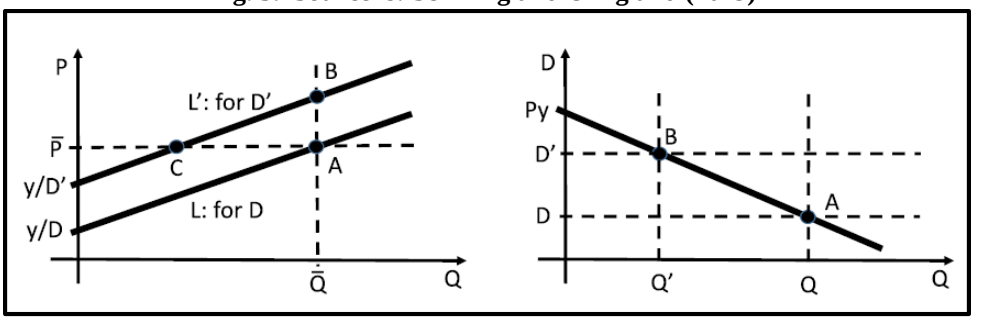
Holding P_t, y_t and Q_t constant, a deterministic increase in B_t (aggregate bitcoin stock) must be compensated by a corresponding decrease in D_t in equilibrium; in other words, bitcoin block rewards are financed by dollar taxes Schilling and Uhlig (2019). The block rewards earned through mining effort are financed not by deflating the bitcoin currency but by the central bank, which decreases 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 financed through the central bank's dollar taxes.

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.

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

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).

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



Impact on Fiscal Policy

When a government or its central bank creates money, it can essentially 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 U.S. range from about $30 billion to $90 billion Wyman (2018), equivalent to about one or two per cent 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 become substitutes for national currency in the future.

The threat of crypto to the integrity of a country's fiscal policy is sustainable because of 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 not subject to taxation at source Obu (2021).

REGULATION

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 a spill-over of investor sentiments between the stock market and crypto. Moreover, 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 favoured by the European Union and UAE propose setting up entirely new regulators to deal with the industry. For a genuinely global, *coordinated* approach, countries must work together, leveraging best practices and learning from each other. As well as risk assessments and the establishment of common standards, there is also a pressing need to develop fit for purpose and inclusive solutions through public-private collaboration White, et al. (2022).

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

Illicit Activities

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

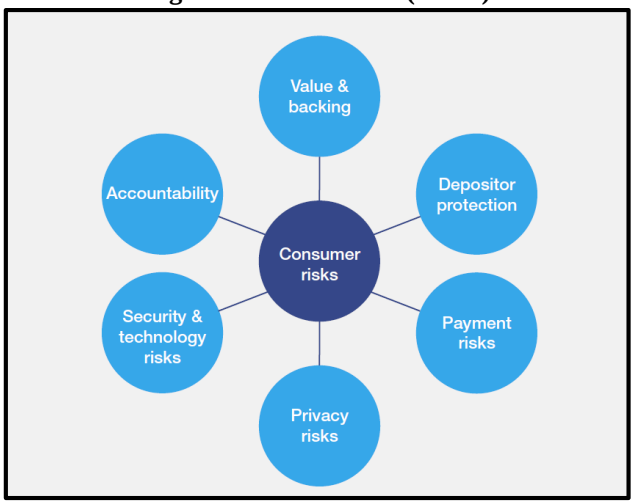
Policy tools include increasing the level of monitoring and tracking and actions against various parties, including criminal penalties or banning/shutting down certain market participants if they are guilty of illicit activity. It could also be helpful for transactions to flag risky activity and "blacklist" certain users, helping mitigate harmful activity without requiring traditional identity documentation WEF (2021a). Supervising 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. For example, the U.S. 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).

Consumer Protection

Most ordinary consumers do not understand the difference between public money (fiat currencies backed by a central bank) and private money (money held in commercial bank deposits). Firms in the blockchain industry will likely provide products and services similar 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, 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.

Fig. 6. Source is WEF (2021a)



Depositor Protection

Deposit insurance protects consumers from the risk of bankruptcy of financial institutions. There are two layers of consumer risks when it comes to digital currencies. 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 capitalised WEF (2021a).

Payment Risks

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

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. 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 the payer. Currently, there is debate 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 push or pull transactions WEF (2021a). If the latter is 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 has significant importance. Moreover, for some crypto markets, an additional risk to privacy has emerged in the form of *surveillance* by blockchain analysis companies. These organisations analyse 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 organisations (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. To minimise potential negative impacts of stable coins on consumers, it is important to carry out *consumer education* to ensure people understand risks and their legal rights. Effective consumer education would include highlighting the different risks that stable coins' present compared not only to other stable coins 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 stable coin, consideration should be given to the regulatory umbrella under which these services will be provided and which functionaries will be responsible within this framework for the procedural implementation and authorisation of regulations WEF (2021a).

CONCLUSION

Cryptocurrencies have massive potential to revolutionise financial transactions and ownership data record-keeping. Some have even argued that distributed ledger technologies have the potential to be as ground-breaking as the invention of double-entry bookkeeping 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 society and create economic costs when widespread adoption occurs. 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 the 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. Given the rapidly evolving technology in Pakistan and beyond, we need to learn a lot more about how to best design policy for the crypto domain at a brisk pace.

APPENDIX

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 cryptocurrency, you may skip this appendix. For more detailed understanding, one useful reference point is the MIT lecture series on Blockchain and Money:

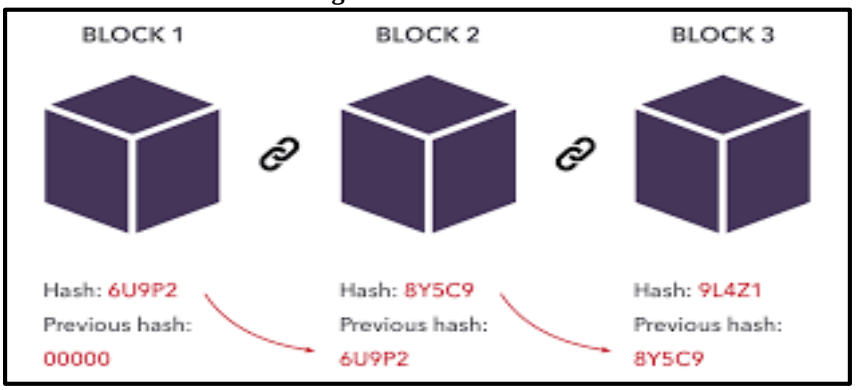
(see, https://www.youtube.com/watch?v=EH6vE97qIP4).

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 decentralised, 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 decentralised 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: Blockchain



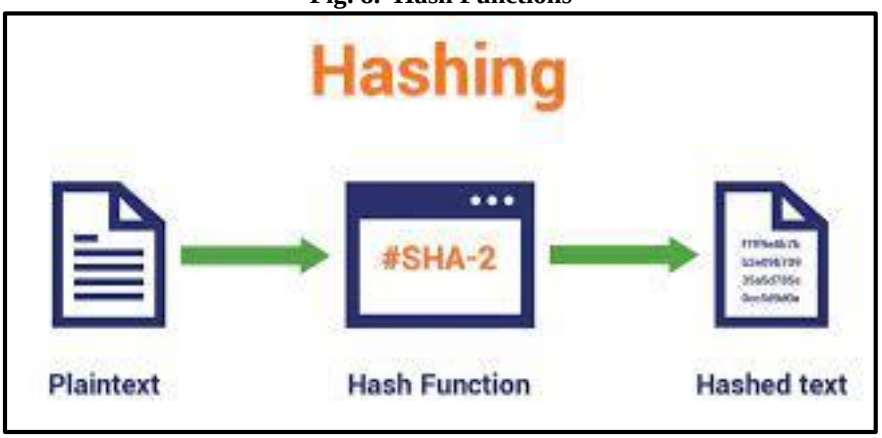
What are Hash Functions?

Hash functions allow appending the subsequent 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 gives 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—i.e. $hash(x) = hash(y)$.

There is also an *avalanche* effect, implying that a slight 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 hash function SHA-2. Refer to the following resource for further understanding: https://www.youtube.com/watch?v=160oMzblY8.

Fig. 8. Hash Functions



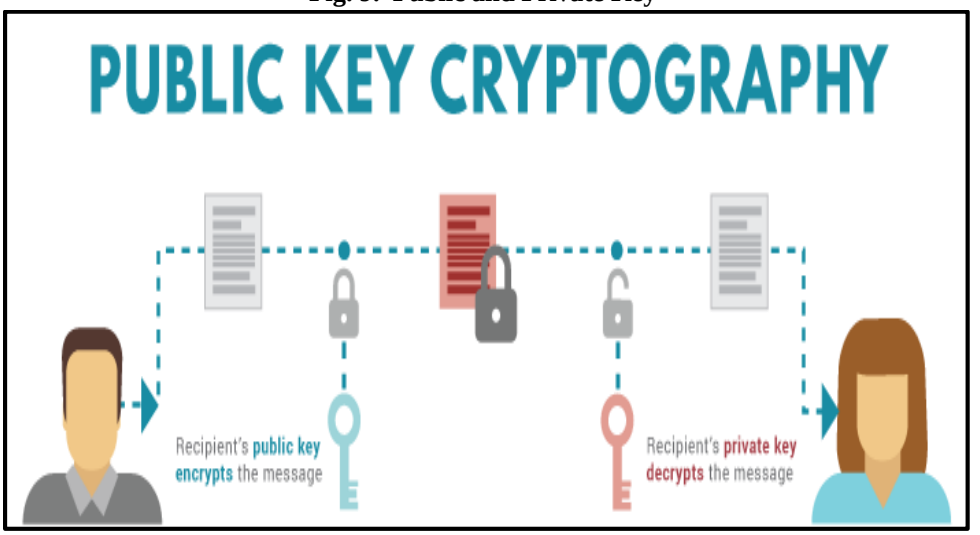
Public Key and Private Key

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. By presenting the public key and signature, everyone in the network can verify and accept the transaction as valid, confirming ownership at the time of transfers Andreas, et al. (2022). This *encryption* and *decryption* process is illustrated in Figure 9.

Fig. 9. Public and Private Key

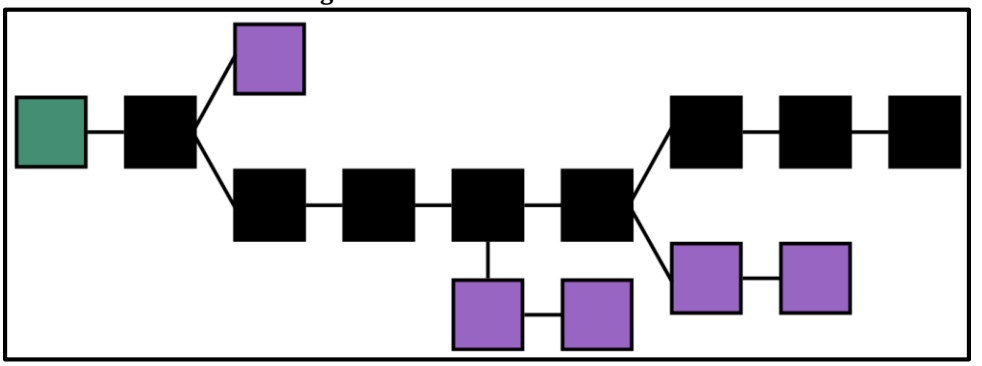


Majority Consensus

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

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

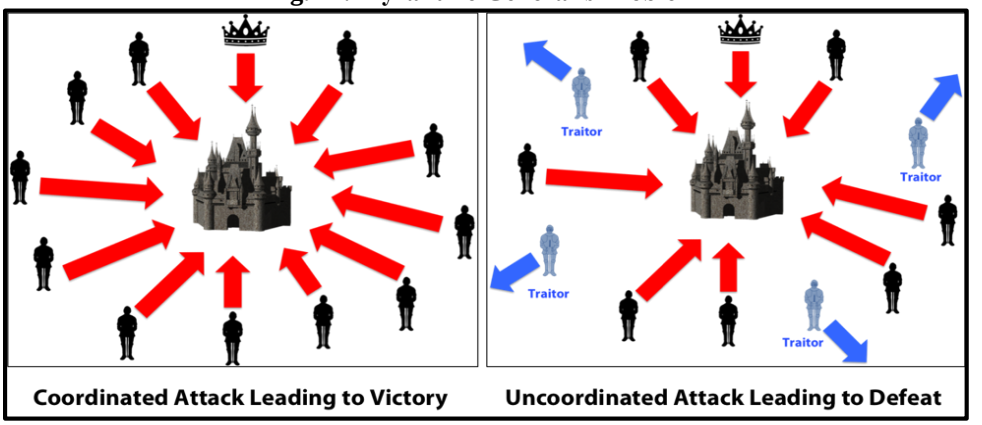
Fig. 10. Black Path is Consensus



Byzantine General Problem

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

Fig. 11. Byzantine General's Problem



This concept captures the complexity of a decentralised 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.

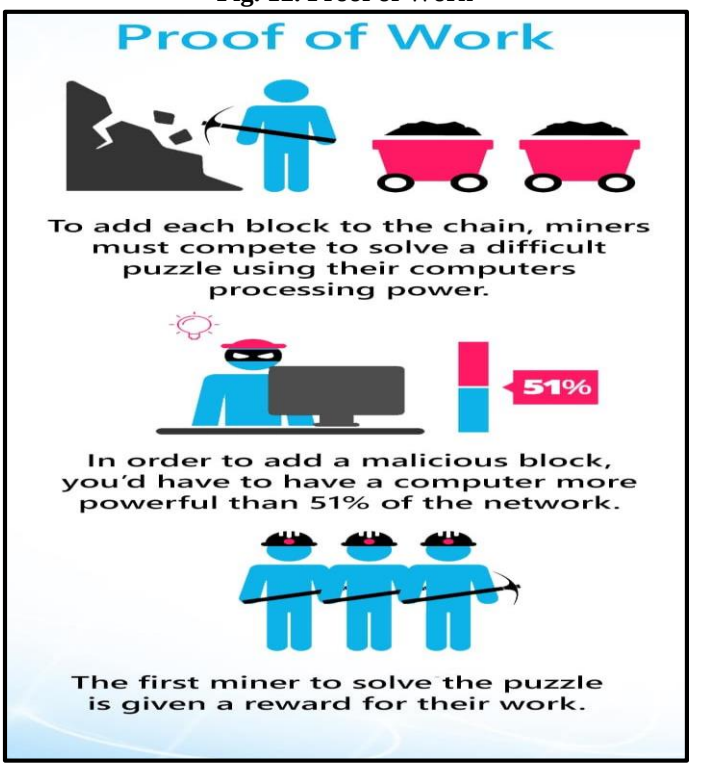
Bitcoin uses a proof of work mechanism (explained next) to solve the Byzantine General's Problem. As a monetary system, Bitcoin needed a way to manage ownership and prevent double spends.[16] If all members of the Bitcoin network, called nodes, could agree on which transactions occurred and in what order, they could verify ownership and establish a functioning, trust-less money without a centralised authority. By doing so, the *Byzantine General Problem* is solved.

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

Proof of Work

To add blocks to the blockchain, a network member must publish *proof* that they invested considerable work into creating the block. This incentivises them to publish honest information since the proof of work problem is computationally intensive and non-trivial to solve (see Figure 12).

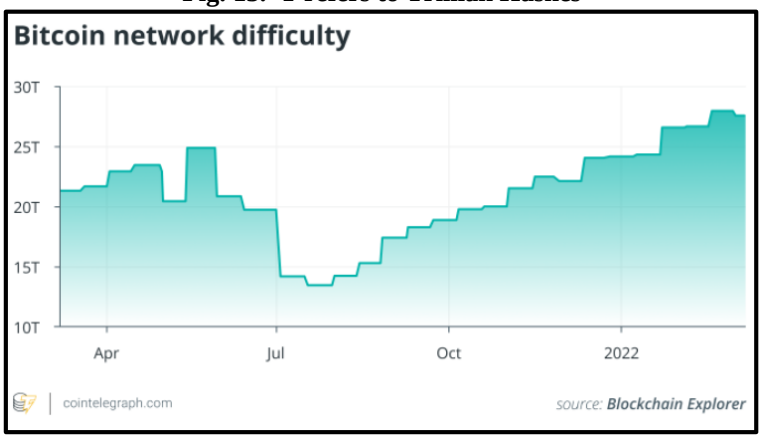
Fig. 12. Proof of Work



If any network member attempts to broadcast false information, all nodes will immediately recognise 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 network members, 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 decentralised.

The Bitcoin *proof of work* difficulty is defined concerning 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 (E.H.) = 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 than 2010 Hacioglu (2020). Figure 13 below shows the recent increase in network difficulty level Vaca (2022).

Fig. 13. T refers to Trillian Hashes



REFERENCES

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

Adrian, Tobias, Tara Iyer, and Mahvash Qureshi (2022). Crypto prices move more in sync with stocks, posing new risks. IMF, January, 11.

Andreas, M. et al. (2022) Mastering bitcoin programming the open blockchain.

Benetton, M., Compiani G., and A. Worse (2019). Cryptomining: Local evidence from China and the U.S. (Working Paper, 2019).

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

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

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

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

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

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

Cochrane, John (2017). Bitcoin and bubbles. The Grumpy Economist.

Cochrane, John H. (2009). *Asset pricing:* Revised edition, Princeton University Press.

Committee, Basel et al. (2021). Prudential treatment of cryptoasset exposures. Basel Committee on Banking Supervision. BIS Consultative Document.

Comply, Advantage (2022). Cryptocurrency regulations around the world. In "in", Comply Advantage.

Crypto (2020). A deep dive into blockchain scalability. crypto.com.

FATF (2021). Financial action task force (FATF). Updated guidance for a risk-based approach for virtual assets and virtual asset service providers. Available at SSRN 3995013.

Goldgar, Anne (2008). Tulipmania. In "Tulipmania". University of Chicago Press.

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

Hayes, Adam (2022) 10 Important cryptocurrencies other than Bitcoin. Investopedia.

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

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

Korpal, Gaurish and Drew Scott (2022). Decentralisation and web3 technologies.

Krugman, Paul (2018) Transaction costs and tethers: Why I am a crypto skeptic. *The New York Times*, 21.

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

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

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

Obu, Osiebuni (2021). Fiscal policy and private money. Available at SSRN 3995013,

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

Reiff, Nathan (2021). How fiat currency crises drive nations toward cryptocurrencies *Investopedia*.

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

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

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

Stiglitz, Joseph E. (2002). Information and the change in the paradigm in economics. American Economic Review, *92*(3), 460–501.

triple A. (2022). Cryptocurrency across the world.

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

WEF (2021). Digital currency governance consortium. White Paper Series. World Economic Forum November. (Technical Report).

WEF (2021) Navigating cryptocurrency regulation: An industry perspective on the insights and tools needed to shape balanced crypto regulation. Global Future Council on Cryptocurrencies, World Economic Forum September 2021. (Technical Report).

White, Kathryn, Arushi Goel, and SandraWaliczek (2022). Cryptocurrency regulation: where are we now, and where are we going? World Economic Forum (Technical Report).

Wyman, Oliver (2018). Cryptocurrencies and public policy: Key questions and answers. Marsh and McLennan Companies. (Technical Report).

Younus, Uzair (2022). Realising the promise and potential of "Web3" for Pakistan. Atlantic Council, South Asia Center.

Pakistan Institute of Development Economics
Post Box No. 1091, Islamabad, Pakistan

www.pide.org.pk