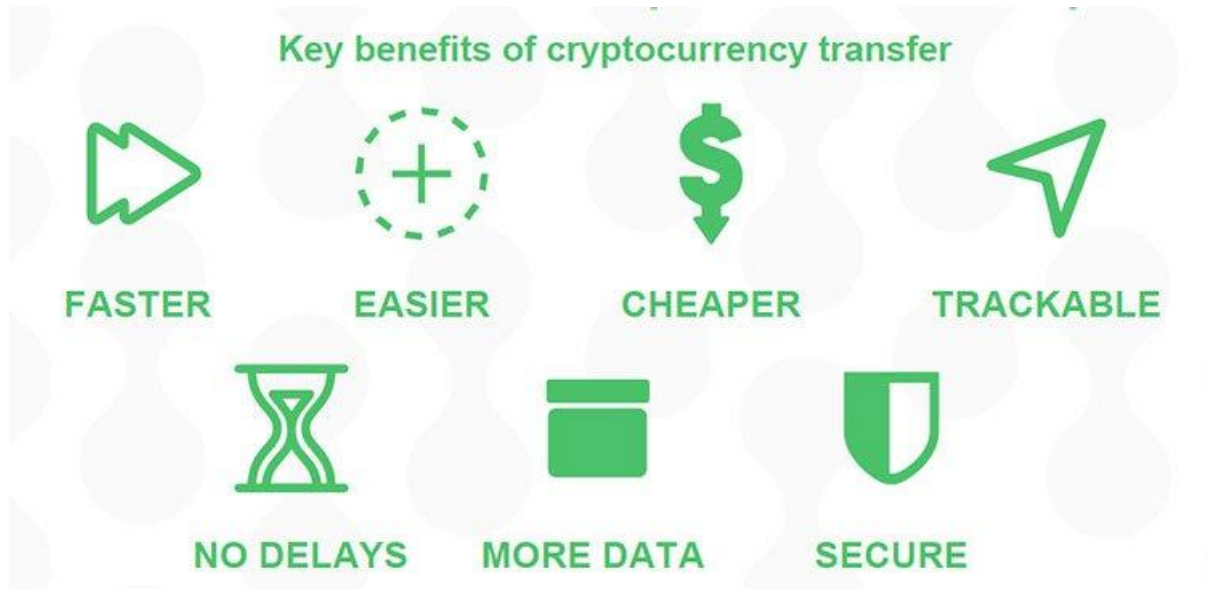


CRYPTOCURRENCIES AND THE REGULATORS DILEMMA

MAINS, GS 2: Awareness in the fields of IT, Space, Computers, robotics.



ADVANTAGES:

- **Privacy Protection:** Privacy and anonymity of the transacting parties was the prime concern of the proponents of cryptocurrencies when the idea was promulgated, and these became part of the underlying principles. The use of pseudonyms conceals the identities, information and details of the parties to the transaction – perquisites for privacy enthusiasts.
- **Cost-effectiveness:** Electronic transactions attract fees and charges, which is on the higher side when the transactions are transnational and undergo currency conversion, or attract processing fee levied by the banks, third party clearing houses or gateways. Cryptocurrencies solve this problem, as they have single valuation globally, and the transaction fee is extremely low, being as low as 1% of the transaction amount. Cryptocurrencies eliminate third party clearing houses or gateways, cutting down the costs and time delay. All the transactions over cryptocurrency platforms, whether domestic or international, are equal.
- **Lower Entry Barriers:** Possessing a bank account or a debit/credit card for international usage requires documented proofs for income, address or identification. Banks or financial institutions might have their own set of eligibility criteria for these facilities. Cryptocurrencies lower these entry barriers, they are free to join, high on usability and the users do not require any disclosure or proof for income, address or identity.

- **Alternative to Banking Systems and Fiat Currencies:** Governments have a tight control and regulation over banking systems, international money transfers and their national currencies or monetary policies. Cryptocurrencies offer the user a reliable and secure means of exchange of money outside the direct control of national or private banking systems.
- **Open Source Methodology and Public Participation:** A majority of the cryptocurrencies are based on open source methodology; their software source code is publicly available for review, further development, enhancement and scrutiny. The ecosystem of cryptocurrencies is primarily participation based, as software development, bug reporting and fixing, testing etc. are driven by the wider user base, rather than a closed set of individuals or an institution. They have their own consensus based decision making, built-in quality control and self-policing mechanisms for building frameworks, practices, protocols and processes.
- **Immunity to Government led Financial Retribution:** Governments have the authority and means to freeze or seize a bank account, but it is infeasible to do so in the case of cryptocurrencies. For citizens in repressive countries, where governments can easily freeze or seize the bank accounts, cryptocurrencies are immune to any such seizure by the state.

RISKS INVOLVED IN CRYPTOCURRENCIES:

- **Key/Wallet/Exchange Security:** A virtual wallet stores the keys and transaction records of the user. The secure digital keys are used to access the public address and to sign or authenticate the transactions initiated by the user. In the entire chain of security, wallets and exchanges are found to be the weakest link, and that is where the attacks are commonly aimed at.
- **Hijacking/Routing Attacks/Distributed Denial of Service (DDoS) attacks on Cryptocurrency System:** Cryptocurrency systems are open source and the pooled in resources of the miners keeps these systems up and running. Some of the research efforts in the recent past have delivered proofs-of-concept for hijacking or Internet routing attacks to which cryptocurrency systems¹⁹ are vulnerable to.
- **Uncertain Regulatory Environment:** The future and further success of cryptocurrencies depends upon the way regulatory frameworks are devised. Different countries have approached this innovation in different ways, and therefore the regulatory environment remains uncertain.
- **Lack of Liquidity and Lower Acceptability:** Cryptocurrencies function outside banking systems, beyond the regulations or controls of the regulatory agencies. Although online exchanges facilitate exchange of cryptocurrencies with fiat currencies, but generally, this is restricted to the more popular cryptocurrencies only, basically, the ones with high market capitalisation. For the rest of cryptocurrencies, and for all of them in certain countries, there is an absolute lack of liquidity. Moreover, the acceptance of cryptocurrencies at merchant sites is also restricted.

- **Price Volatility:** Volatility, a measure of variance of the price of a financial instrument over a certain period of time, is associated with the risk level of the instrument. High volatility is regarded as risky, and cryptocurrencies are known to be extremely prone to price fluctuations.
- **Uncertainty over Consumer Protection and Dispute Settlement Mechanisms:** Cryptocurrencies are decentralised, that means, there is no single authority for mediation or dispute redressal. The miners are not responsible for any arbitration of disputes between the parties. The transactions are also irreversible, which, in the case of banks or payment gateways is reversible if the dispute is resolved, safeguarding the users from fraud. Cryptocurrencies lack these safeguards, exposing the users to the risks of fraud and bringing a sense of uncertainty over consumer protection and dispute settlement mechanisms.

THREATS ARISING FROM CRYPTOCURRENCIES

- **Potential use for Illicit Trade and Criminal Activities:** Cryptocurrencies are virtual and decentralised, well beyond the control or authority of the state. Probably, this has made their absorption quicker into grey and black markets, ransomwares and a host of other illicit activities of crime and money laundering. Regulatory bodies and law enforcement agencies have raised legitimate concerns that cryptocurrency accounts and wallets cannot be frozen, seized or examined.
- **Potential use for Terror Financing:** cryptocurrencies are also emerging as a new funding stream for terrorist outfits. Islamic State of Iraq and Syria (ISIS) had proposed using Bitcoins to raise funds. Cryptocurrencies have thrown open a whole new challenge towards which majority of the intelligence and law enforcement apparatus are inadequately prepared to tackle.
- **Potential for Tax Evasion:** Cryptocurrencies are not regulated or controlled by governments, making them a lucrative option for tax evasion. Sales made or salaries paid in the form of cryptocurrencies could be used to avoid income tax liability. Taxation rules and regulations may vary from state to state, and many countries do not yet have policies in place for cryptocurrencies. As taxation authorities are grappling with devising strategies and guidelines for tax compliance, tax evaders might find their tax havens in form of cryptocurrencies.

(Q) Discuss the possible challenges associated with the regulation of cryptocurrencies.

PREVIOUS YEARS UPSC MAINS QUESTIONS:

- Discuss the potential threats of Cyber attack and the security framework to prevent it. (2017)



ACHIEVERS IAS ACADEMY

- Use of Internet and social media by non-state actors for subversive activities is a major concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat. (2016)
- Considering the threats cyberspace poses for the country, India needs a “Digital Armed Forces” to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation. (2015)
- What is a digital signature? What does its authentication mean? Give various salient built-in features of a digital signature. (2013)
- What are social networking sites and what security implications do these sites present? (2013).
- Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country’s preparedness to deal with the same. (2013)