DEFENCE AND DIPLOMACY

IN PURSUIT OF NATIONAL SECURITY

VOL. 11 NO. 4 ISSN 2347 - 3703 JULY-SEPTEMBER 2022

JOURNAL OF THE CENTRE FOR AIR POWER STUDIES

DILUTING THE DETERRENCE: EVADING SANCTIONS THROUGH CRYPTOCURRENCY

KHYATI SINGH

Technology has been oxymoronic in its existence all throughout the human history. The more complex its inherent structure gets, the easier its outward operations become. This has specially been the case with cryptocurrencies. The complexities on the blockchain are invisible to the naked eye, but the feasibility of the currencies is on our fingertips. Cryptocurrency is a virtual, or digital currency still in the processing stage, and is yet to gain the legitimacy amongst governments around the world. Although the development of cryptocurrency was under way for a decade now, it is the recent outburst of the phenomenon coupled with the digital revolution that has put it in the centre of everyday affairs.

WHAT IS CRYPTOCURRENCY AND HOW IT WORKS?

The basic science behind cryptocurrency is that it is a non-printable currency, which exists virtually on the net. The technique that goes into processing of cryptocurrency is called 'cryptography'. It is a method through which intelligible data is obfuscated by the method of encryption. The process starts from the side of a sender to convert intelligible data into unintelligible data. The moment it

Ms **Khyati Singh** is Research Associate at the Centre for Air Power Studies, New Delhi.

reaches the receiver, the process of decryption begins. The receiver reverses the process by changing the data into intelligible form again. The entire process of encryption and decryption is done using algorithms, which are basically a set of commands for the computer. Unlike the fiat currency whose value is determined by multiple economic factors and government standardisation, the value of crypto strangely comes from 'faith'. It is amusing to believe that a currency that runs through the globe has no standardisation. It is decentralised and in the absence of a regulating body, it is the consensus of the people that adds value to the currency. In this sense, bitcoin is merely a software that creates a community of users who access the network to make payments around the world without any interference from the banks.[1]

New bitcoins come into existence by the process of 'mining'. An individual exploits the computing capacity of a computer to solve mathematical calculations thereby generating more coins, and validating the transaction in the process. To get to a new block, and to create new coins, the miner is required to crack through algorithm or puzzles and 'mine' for a nonce that will be used to generate an accepted hash. Nonce is a shorthand for 'Number Used Only Once', which is a unique 32-bit whole number that is produced every time a block is created. It automatically creates a 'block header hash' that summarises any information related to the block along with the transaction data, such as time of creation of the block, etc. Hash is a comparatively small 256-bit number tied to the nonce, and contains an identifier that connects it to the previous segment of the chain. In contemporary times, cryptocurrencies are used as a means and not as an end. It is bought as a token with fiat currency and is resold for fiat currency again and not exactly used to counter-trade for material goods or any services.

Cryptocurrency is paving a path that leads to the elimination of 'network of middlemen', and this decentralised model is increasingly gaining currency in the modern world. It allows people to transfer goods that have 'value' without bearing the cost of a middleman. For instance, before the coming of email, and e-messaging apps, people relied solely on state-run telegram and courier services. The coming

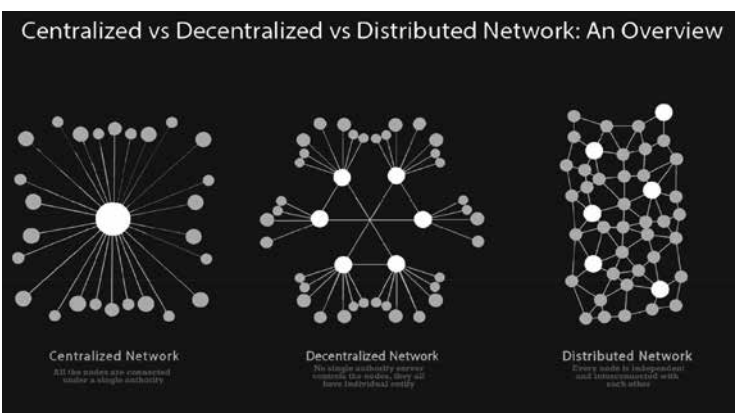
1. R. Lewis, *The Cryptocurrency Revolution: Finance in the Age of Bitcoin, Blockchains and Tokens* (Kogan Page, 2020).

of the internet completely abolished the operation monopoly of the state, and cryptocurrency was envisaged to play a similar role. However, what remains a major obstacle is the influence it has on the state power. Nation's economic strength is a direct indicator of their sovereignty and might in the international order. Hence, at no cost would they let go of the purse strings.

There are generally three kinds of systems that are used for transactions and processing the chain of finances. First, the Centralised system, which resembles a 'hub and spoke structure'. The key players are at the centre and have complete charge of all the traffic. The failure of hub leads to the failure of spokes and the system collapse. Whereas, in a decentralised system, there are multiple nodes at operation. Each node is in charge of variant's smooth functioning. Lastly, the latest evolution is of 'distributed systems'. In such a system, each node in the decision-making process is simplified, and automated into a series of yes/no.[2] Since each node is expected to give the same output, the decision-making process has to be identical.

The Figure 1[3] shows how the systems operate.

Figure 1: Representation of Centralised, Decentralised and Distributed Network



Source: blockchainengineer.com

2. B. Kelly, "*The bitcoin big bang: How alternative currencies are about to change the world*, 1st edn. (Wiley, 2014).
3. Centralized Network, at http://blockchainengineer.com/centralized-vs-decentralized-vs-distributed-network. Accessed on April 4, 2022.

Blockchain is a distributed system that works as a decentralised digital ledger. It stores the encrypted information, that is, a block, which gets linked and forms a chain. It is a tamper-proof system that doesn't allow anyone to change any confirmed transaction on it. Hence, the transparency and accountability of the system stays intact.

Every transaction on the net is protected using a digital signature, which is sent to the 'public key' of the receiver. The public key is like the 'email address' that the receiver can share. This transaction is digitally signed using a 'private key' which works like a 'password', and to spend any money this 'private key' is needed. For any payment to take place, this signature has to be verified. Once the transaction is made, it is broadcasted to all the nodes on the network, and is then updated on the public ledger.

EVADING THE SANCTIONS THROUGH CRYPTOCURRENCY

Borrowing from the liberal international discourse of how complex interdependence operates in international domain, it is crucial to comprehend the implications of this 'cooperation'. Economics is an indispensable feature of sovereign states, and lies at the core of state operations. This makes economic independence and a sound system of finance the cornerstone of stability for states. Therefore, economic sanctions have worked as a weapon that keeps the states intact within the system. Nevertheless, there are states that digress from this standing, and pay heavily due to the sanctions that follow.

Society for Worldwide Interbank Financial Telecommunication (SWIFT) has a key role to play in unleashing the weapon of sanctions. SWIFT was set up in the 1970s, and aimed at standardising payments worldwide. The majority of banks that operate SWIFT are either European or North American. With time, SWIFT has taken up an important role is the political discourse of international security circuit. It was used to figure out the financing channels for terrorist groups that were involved in the 9/11 attack on the Twin Towers. Ever since then, it has been an active tool used to further solidify the sanctions. In 2012, when Iran was on the path of making nuclear weapons, the USA through SWIFT disconnected Iran's banking system from the payment network. Likewise, North Korean banks served a similar fate following the instructions of the United Nations.

Therefore, it is safe to say that SWIFT has the power to 'swiftly' destroy state economies.

The use of sanctions as a means for a 'covert warfare' is not new to international politics. It was also used by the League of Nations, but the effectiveness was lacking. However, with the integration that came along with the strong forces of globalisation, the impact of these sanctions heightened. It is only in the recent past that states have started using cryptocurrency to circumvent these sanctions.[4] This has especially been the case with rogue regimes, or revival states that are desperately seeking to escape from the grips of the hegemony of the US system. China, Iran, Russia, North Korea, Sudan and Venezuela are the forerunners in this race. The cryptocurrency route not only allows them to dilute the deterrence, it also helps them weaken the US dollar global hegemony. The quasi-anonymity structure of cryptocurrency allows these states to override the financial controls that are there in the system. A trend that runs parallel and exposes this truth has been the increased use of cryptocurrency in states that the US had a sanction against. This raised alarms at all levels, and the literature that followed talked extensively about introducing 'crypto-sanctions' and 'crypto-regimes'.

An important facilitator of evasion has been the minimised role that the 'intermediaries' have come to play. There has been a controlled presence of intermediaries on the blockchain, and they have little to no real power to freeze any digital currency payment. Rather, they are benefited every time a cryptocurrency transaction takes place. This brings down the incentives to stop the transactions even if the intermediary is aware of the evasion. Moreover, there are no legal regulations on the part of states to keep an eye on the defaulters, or not to facilitate them. This, in turn, motivates them to gain the extra profit by supporting these evasions through the cryptocurrency.

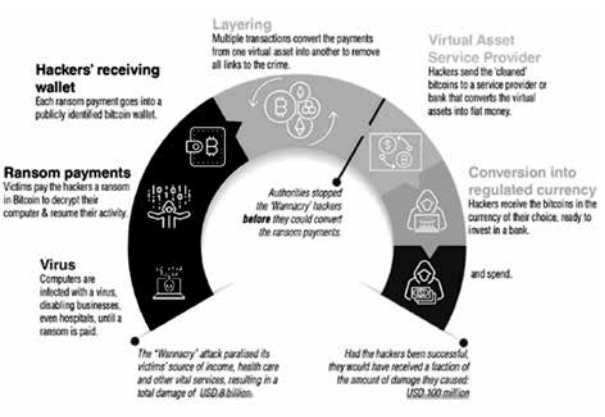
States like North Korea are increasingly penetrating sanctions via the crypto route. Furthermore, they are not only using this to stabilise their economies, rather they are using this route to fulfil the agenda they were sanctioned against in the first place. This dilutes,

4. P. H. Verdier, "A Hidden War: Sanctions Evasion", *Global Banks on Trial: U.S. Prosecutions and the Remaking of International Finance*, Oxford Academic (oup.com), pp. 109-46. Accessed on April 8, 2022.

or rather destroys, the entire motive behind sanctions. For instance, North Korea funds its nuclear programme through cryptocurrency. At one level, the individuals or actors that are engaging with these states are unaware of the sanctions that are in place, and in addition, it is extremely difficult to cherry pick the transactions belonging to a particular unit on the blockchain. Moreover, the North Korea and the trail of sanctions is not new. The United States have sanctioned North Korea, or companies or individuals associated with it in one way or the other. However, initially it didn't have an easy way to escape so it relied heavily on state-sponsored cybercrimes for it. The introduction of cryptocurrency changed the entire discourse. North Korea added the element of cryptocurrency to its infamous cybercrime trajectory and started hacking cryptocurrency exchanges. In 2017, the first such attack was traced when an exchange named Bithumb was hacked for nearly $7 million. This event was followed by another hacking of the exchange called YouBit that ended up bankrupt due to losing 17 per cent of its assets. In the same year, North Korea earned approximately $120,000 worth of Bitcoin by conducting a WannaCry Bitcoin ransomware attack.

The Figure 2[5] shows the process involved in WannaCry attack.

Figure 2: The WannaCry Attack Cycle



Source: Financial Action Task Force (FATF). Fatf-gafi.org. (2021)

5. Source: Documents—Financial Action Task Force (FATF), at https://www.fatf-gafi.org/. (2021). Accessed on April 8, 2022.

In 2018, North Korea was a key suspect in the heist of a crypto coin named NEM which is located in Japan. Hackers located in North Korea stole around $526 million worth of cryptocurrency. International Cyber Security Company Group IB identified that five major cryptocurrency attacks are directly linked to Lazarus, which is a North Korean state-sponsored hacking group. The amount that North Korea has amassed using these tactics is estimated to be around $670 million as per the UN Security Report 2019.[6] North Korea follows the same trajectory over and over again. It used state-sponsored cyber actors to steal cryptocurrency, thereafter it uses these proceeds to evade sanctions and finally through crypto-jacking mine these currencies to generate revenue. Moreover, to escape any detection, they send it through multiple transaction IDs and further complicate the route. The currency travels different countries before it is converted into fiat currency. This way it becomes next to impossible to catch hold of the leakages.

Much like North Korea, another state that never had cordial ground of operation with the USA is Russia. However, Russia's sanction tussle started following its annexation of Crimea in 2014. This saw a sudden rise in mining activity, especially in Siberia. Russia initially planned to have its own cryptocurrency named "Crypto-Ruble", but realised that it is relatively feasible and cost-effective to manufacture asset-backed cryptocurrencies in place of creating crypto-ruble.[7]

The United States sanctions in West Asia are not new. It has been there since 1979, but it is Iran in particular that has suffered the most. The sanctions that came its way during the Trump era dismantled the Iranian economy. To recover from this, Iran chose the 'e-way'. Initially, it was sceptical of using cryptocurrency but subsequently joined the bandwagon with other sufferers like Russia and North Korea. It developed a blockchain, namely, 'IranRescueBit' with the agenda of making donations using cryptocurrencies like Ethereum, Litcoin,

6. United Nations Report of the Panel of Experts, S/2019/171, 2019, at https://documents-ddsny.un.org/doc/UNDOC/GEN/N19/028/82/PDF/N1902882.pdf. Accessed on April 8, 2022.
7. T. Clautice, "Nation State Involvement in Cryptocurrency and the Impact to Economic Sanctions", LaSalle University, 2019, at https://digitalcommons.lasalle.edu/ecf_capstones/43/. Accessed on April 10, 2022.

Bitcoin feasible. Iran was caught in a fix as it initially banned crypto mining because of the extra load that it creates on the subsidised state electricity, but in the same year it announced that it would introduce a nationwide digital cryptocurrency that will facilitate in freeing the frozen assets and accounts. This led to exclusive rights to Iran's own cryptocurrency, and removed the rest prevalent currencies from the picture. Initially, cryptocurrencies were used for payment in medium and small-sized companies to keep the business going. It was only in 2019 that central bank of Iran issued a notice concerning the use of cryptocurrency inside the country, this led to the creation of the PayMon. It is a digital currency backed by gold and was created by four Iranian banks. Provided Iran stabilises relations with China and Russia along with a financial structure in place, this will prove to be a good move. Armenia recently signed a trilateral agreement with Russia and Iran for blockchain cooperation.[8]

Iran has made huge profits by exporting barrels of oil through mining. It is only a couple of years back that Iran has recognised crypto-mining officially and has laid guidelines for the same. It has also established a proper licence system that requires miners to register themselves. However, a strange case in point remains that a lot of these people who carry out Bitcoin transactions and pay commissions to miners in Iran are located in the United States. Hence, exposing the lack of regulations at the system level.

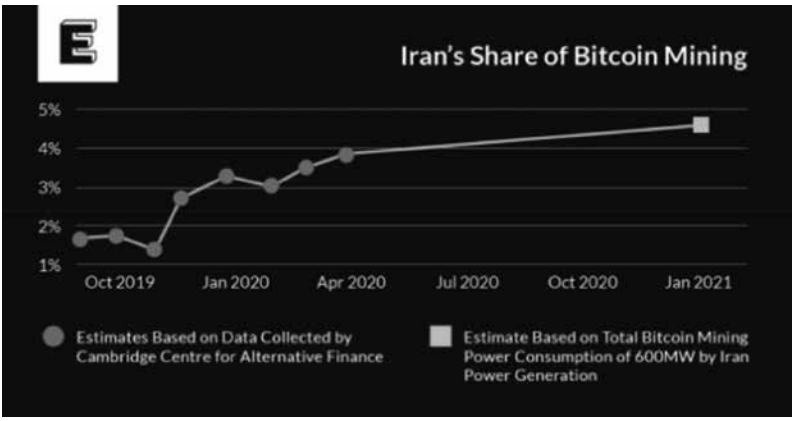
The Figure 3[9] shows the increase in Bitcoin mining in Iran.

This implies that around 4.5 per cent of the entire Bitcoin mining solely takes place in Iran. This signals that the yearly turnover is around $1 billion. Thereby helping any of the West Asian states to evade sanctions.

Venezuela is also in the list of countries that launched its indigenous cryptocurrency called Petro under President Maduro. This move came following US sanctions against Venezuela in 2017,

8. R. Mogielnicki, "Cryptocurrencies could help evade U.S. sanctions on Iran", *Axios*, at https://www.axios.com/cryptocurrencies-could-help-evade-us-sanctions-on-iran-c6a68e07-03c3-4b99-8dde882d6f729130.html. Accessed on April 10, 2022.
9. T. Robinson, "How Iran Uses Bitcoin Mining to Evade Sanctions and 'Export' Millions of Barrels of Oil", Elliptic.co, 2019, at https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions. Accessed on April 10, 2022.

Figure 3: Iran's Share of Bitcoin



Source: Elliptic.co

when the US through an Executive Order prohibited oil companies from accessing the US financial market. Since Petro was introduced from the state's end, it was convertible into fiat currency. The main use of Petro was to export oil without using the US dollar. Turkey was one of the first countries to accept Petro as a legitimate means of payment.[10]

STRATEGIES OF EVASION

Cryptocurrency lays down a series of opportunities that can be exploited to evade sanctions. The cases discussed above help us track the possible strategies for the same. The most commonly used is 'Crypto-theft'. Stealing cryptocurrency from exchanges using cyber weapons is the strategy that has helped nations that are well-knit into the cyberspace system, and know how to tweak it for their benefit. States like Russia and North Korea are best known for their cyber offensives. Generally, this can be done by either directly hacking the computer and stealing the cryptocurrency, or by demanding a ransom so that the system can return to usual. This method was used in WannaCry attack.

10. F. Cozzi, "Will Blockchain Technologies Strengthen or Undermine the Effectiveness of Global Trade Control Regulations and Financial Sanctions?", *Global Jurist*, July 6, 2020, at https://www.degruyter.com/document/doi/10.1515/gj-2019-0047/html. Accessed on April 10, 2022.

Another strategy in place is related to cryptocurrency mining. The process of mining is resource extensive as it used numerous servers, investment in technology, constant and large power supply, heavy computers, special weather conditions, and marginal electricity cost. Using this trajectory, capital is produced outside the ambit of the financial system. Russia has an edge in this regard because of the state control over resources with its unique computer technology and money laundering expertise.

The strategy of introducing indigenous cryptocurrency has been in place as well. Increasingly, states are taking this route and experimenting with this space. However, its success depends on the technological advancement and cyber capabilities that states like Venezuela lack at present.

In addition, a fourth strategy deals with creating a 'Common Cryptocurrency', that is, multiple states can come together and agree to the use of a common cryptocurrency, much like the EU has done for its currency Euro. In terms of crypto, BRICS has taken the lead. It is working to develop a common cryptocurrency called BRICSCoin to counter the dollar hegemony. This currency will be backed by their own gold, and national currencies. This is a strong strategy, and if it operates to its maximum potential, it can certainly bring down the US dollar supremacy precisely because major economies of the world, such as China, India and Russia would no longer operate on the financial chains created by the US. Thus, it will also have political implication as it creates alternative centres of power and decentralises the system of finances.

Lastly, the strategy to motivate citizens and business owners within a sanctioned state to shift to cryptocurrency. However, this strategy runs the risk of undermining fiat currency as the operations start moving onto the digital space. Generally, states take this risk due to the impact of sanctions on their economies. Therefore, if the impact is higher, the states' risk factor also increases, particularly in the cases where this helps in stabilising domestic economy.

The only challenges that mount against all the strategies is the conversion of cryptocurrency into fiat currency.

INDIA'S TAKE ON CRYPTOCURRENCY

India has been partially welcoming of the cryptocurrency and there has been no clear picture from the end of government that spells its future trajectory. In 2018, the Reserve Bank of India issued a notice that put a ban on all the banks in dealing with cryptocurrency. Following this, in 2019 the government drafted a bill that bans "mining, holding, selling, trade, issuance, disposal or use of cryptocurrency in the country." However, in March 2020 the Supreme Court nullified RBI's ban on cryptocurrency and that kindled a massive rise in crypto trading. The government on various occasions have expressed concerns over the misuse of cryptocurrency, especially its use to fund terrorists. Moreover, the budget session of 2022-2023 introduced 30% tax on cryptocurrency along with 1 per cent TDS. Although, this TDS can be settled towards the end with total income tax calculations. This tax also takes into account the profits that are derived from sale or purchase of Non-Fungible Tokens (NFTs).

The tax on cryptocurrency is not new, several countries like Australia, Canada, Germany, Italy, Netherlands, USA, UK have crypto tax in place. Albeit, some states like Belarus, Cayman Islands, El Salvador, Portugal, Singapore, Switzerland, Malta, Malaysia, and Puerto Rico have made cryptocurrency tax free.

The reasons for the introduction of taxes on cryptocurrency can be understood in the light of acceptance and risk that comes with cryptocurrency. While, on the one hand, it is increasingly becoming a currency of trade, the risk that comes along with it makes it important for the state to track its movement. Hence, the 1 per cent TDS that has been introduced tracks the route that cryptocurrency takes as it goes from one person to another. Likewise, with 30 per cent tax bracket, the usage has been discouraged with limiting the window of sale-purchase to the ones who can bear the brunt of huge losses. Thus, safeguarding the economic ecosystem. In addition, adding cryptocurrency in the tax bracket also signals to the fact that the government is coming to terms with the reality of cryptocurrency and how banning it would not be a feasible option. Therefore, by taxing it, the government has introduced some level of institutionalisation and regulation with regard to cryptocurrency.

WAY AHEAD

There are so many actors involved at each level during the passage of cryptocurrency that it becomes increasingly difficult to keep a track of evasions. The strategy to combat these evasions requires transparency on the part of individuals and entities like intermediaries. Unfortunately, there is no mechanism in place to ensure that. Therefore, as the actors involved in the process increase, the ways to combat it also become difficult.

Office of Foreign Assets Control (OFAC), a department of the US Treasury, works to enforce economic and trade sanctions imposed by the United States. It was created back in 1950 when the Korean War was roaring and China chose to enter it. President Harry Truman considered it a national emergency and went on to freeze all Chinese and Korean assets. Taking into account the risk of cryptocurrency and how it evades sanctions, OFAC has declared that it will take into account measures that counter these evasions. Although it is still in the embryonic stage, the fact that it has come to realise this is a step in the right direction.[11]

Financial Action Task Force also has a role to play in this regard. It recently published its new draft that encompassed in its fold guidance on virtual assets (VAs) and Virtual Asset Service Providers (VASPs). The guidelines it rolled out included Customer Due Diligence (CCD) and Know Your Customer (KYC) to keep a check on money laundering and combating financing of terrorism. Increasingly, it is also incorporating new aspects like Non-Fungible Tokens (NFTs). However, not all countries have applied FATF requirements.

The most prominent concern has been regarding the impact of cryptocurrency on government's ability of revenue generation, and to regulate monetary policies of the banks. There has been this constant question whether the virtual currency should be allowed to take up the space of fiat currency, or should it be allowed to coexist in the same space with the same level of legitimacy that the fiat currency have.

11. B. Mosman and D. Mortlock, "OFAC Sanctions Considerations for the Crypto Sector", Willkie Farr & Gallagher LLP, 2019, at https://www.willkie.com/-/media/files/publications/2021/08/ofacsanctionsconsiderationsforthecryptosector.pdf. Accessed on April 11, 2022.

CONCLUSION

The inherent nature that makes cryptocurrency different from any other currency that is out there in operation has been the anonymity that comes along with it. The dilemma that the countries of the world face at present is to monitor something which was essentially created to escape this monitored regime. Hence, as Jacobs put it, "how to govern something born not to be governed?".[12] Until Cryptocurrencies were not as prevalent as they are today, it allowed for sanctions to work as an instrument to keep in check the international order and punish the states that go out of their way to introduce chaos to this system. Cryptocurrency clubbed with cyber-offensive capabilities have worked as a panacea for states that are under sanctions.

Cryptocurrency helps the state run a parallel economy that is entirely virtual and anonymous in its operations. This way they continue to build on their hawkish agendas, finance terrorist groups, buy arms, and unleash cyber-attacks on other states without coming under the radar. Moreover, the spillover of these capabilities can introduce complete anarchy into the system. As more and more terrorist organisations access and exploit the mechanism of blockchains, the more difficult it becomes to catch hold of them. The introduction of crypto on the world platform has opened the Pandora's box, and every day there is a new evil evasion act that pops out. Taking note of these circumstances, it is the need of the hour that nations that are invested in keeping the strength of the deterrence intact should work tirelessly to develop Cyber and Crypto defensives. Financial watchdog organisations should take the lead in understanding and encrypting the 'norms' for the new normal of digital space. States need to pool in resources, contribute to R&D along with filtering the domestic channels to combat the challenges posed by cryptocurrency. The road ahead is treacherous but like always "technology can be beaten by technology alone". The only question that remains in place is, "who gets to attack first"?

12. G. Jacobs, "Cryptocurrencies & the Challenge of Global Governance", *Cadmus*, 2019, (PDF) "Cryptocurrencies & the Challenge of Global Governance", researchgate.net. Accessed on April 11, 2022.