The Digital Yuan: A Digital Currency/Electronics Payments System (DCEP) and its Role in Bypassing Data Privacy Initiatives to Enhance Information Collection Efforts

I. Introduction and Motivation

Cryptocurrencies have played an important role in disrupting the financial sector in the last decade, with their emergence as an alternative asset class merging the traditionally institution-bound financial system with the modern era. Cryptocurrencies have risen to the standards set traditional fiat currencies by meeting the three criteria required of money as commonly defined by economists, with cryptocurrencies increasingly acting as medium of exchanges, unit of accounts, and stores of value. Despite the implementation of concepts such as the blockchain, cryptocurrency mining, and decentralized public ledgers becoming increasingly prevalent, government institutions fallen far behind in their adaptation of financial technology. Keeping this in mind, many governments have begun to explore options to participate in the digital economy.

Through this exploration, many governments around the globe have been exploring self-backed digital currencies, with some potential options for development being central bank digital currencies (CBDCs) and digital currency electronic payment (DCEPs) systems. These forms of money range from being a true digital currency to simply mimicking fiat currencies, albeit in digital form, with these proposed currencies being issued and regulated by that specific country or region's central monetary authority.

CBDCs have a variety of benefits that come with proposed implementation, such as increasing public access to legal tender in the eventual phase-out of physical currency, improved efficiency of payment systems, and refined international business collaboration (Ward and Rochemont, 2019). However, CBDCs must also address multiple specific challenges, chief among them privacy concerns, lack of regulatory experience, as well as technological vulnerabilities (Allen et. al., 2020). These challenges present difficulties in the initial acceptance

phases of CBDCs, with many governments hesitant to implement such technological changes within their infrastructure despite a desperate need to increasingly participate within the digital economy. However, simply put, the benefits of CBDC implementation outweigh its detracting effects, though specific design choices are required to protect consumer privacy in the short and long-term.

Data and consumer privacy are topics that must be effectively addressed if governments plan to implement CBDCs in any way, shape, or form in the future. While Internet-of-Things (IoT) gadgets and other technology devices have certainly improved consumer quality-of-life in the past two decades, such devices provide a path for the increased exploitation of consumer data in the modern age. Consumer data can be exploited for crimes to include identify theft, industry disruption, and much more. However, more importantly, personal data, to include financial data, can be used to identify and coerce individual behavior. This is especially concerning given the current nature of Great Power Competition, with the People's Republic of China (PRC), Russia, and the United States increasingly competing with one another for global influence. Of these nations, the PRC has the most to gain through the implementation of a CBDC; China's ever-expanding Belt and Road Initiative (BRI) merged with a home-grown digital currency would provide the PRC with the ability to disrupt the American dollar, and to a lesser extent, the Russian rubble, as a primary asset within the realm of international trade and other global functions.

This paper seeks to examine different design choices for central bank digital currencies and explore their implementation through three primary use cases: the Caribbean Sand Dollar, Singapore's Project Ubin, and China's digital yuan.

II. Privacy Regulations in Traditional Finance

Privacy regulations in the traditional financial industry and its associated instruments have had their own stereotypes perpetuated by the media, with many individuals associating the term “privacy” to numbered Swiss bank accounts or Caribbean countries seeking to drive foreign investment. However, this stereotype is more fiction than truth, with privacy regulations in traditional financial sectors being closely tied to data privacy legislation throughout the world. Two examples of this can be seen in America’s financial privacy laws and the European Union’s General Data Protection Regulation (GDPR).

Before examining specific privacy laws utilized by specific governments, this paper acknowledges that traditional banking institutions simply cannot guarantee 100% data privacy from government oversight. A primary example of inevitable government oversight in the financial realm is through Know Your Customer (KYC)/anti-money laundering (AML) legislation. KYC/AML regulations are emphasized upon and ubiquitously utilized by governments to perform a variety of actions, some of which include managing currency flows, ensuring the capturing of tax revenues, and fighting illegal activities such as drug distribution and weapons trafficking. These regulations have often been criticized as extremely cumbersome, with 12% of companies specifically citing changing banking institutions due to issues with KYC/AML regulations, creating a compliance-focused industry worth $500 million dollars per year (Dickenson, 2019). However, the necessity of KYC/AML regulations are simply the cost of doing business with governmental support. Explicitly acknowledging this point highlights that while consumer protection and data privacy is important, governments do have certain working standards set in place under the auspices of public safety.

In the United States, privacy regulations primarily stem from the federal level, affecting financial institutions no matter where they conduct business in the United States. American data privacy in the financial realm primarily takes form in legislation to include the Bank Secrecy Act, the Right to Financial Privacy Act, the Gramm-Leach-Bliley Act, and the Fair Credit Reporting Act. The Bank Secret Act, created in 1970, is used to identify money laundering by requiring financial institutions to provide documentation to regulators for suspicious cash transactions for sums of over $10,000. Additionally, the 1978 Right to Financial Privacy Act clearly states that "no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described." These laws are just some of the rules governing privacy regulations in the United States, with many of these laws focusing on securing financial organizations from cyberattacks and unauthorized breaches of data.

The European Union also has established their own set of legislation governing data privacy within the financial sector, with many of these laws being based in the GDPR framework. Much of the GDPR's emphasis is focused on institutional compliance with laws within the European Union and its member-states. The GDPR's various articles do offer some similarities in privacy protections to consumers, specifically through sections including Articles 5, 14, 15, 16, and 18 (European Parliament and Council of European Union, 2016). All told, the GDPR places a very significant responsibility on controllers and processors to respond to requests of data subjects, rather than placing emphasis on personal privacy and information security.

Privacy regulations in the PRC have lagged behand that of America's and the European Union's. One of the cornerstone pieces of legislation in China for ensuring consumer data

privacy is seen in the 1986 General Principles of the Civil Law and its' 2017 update, with Article 111 specifically protecting consumer data (Pernot-LePlay, 2020). However, many of the PRC's laws for data privacy borrow from different elements of American and European Union data protection legislation. This has resulted in the PRC melding of a vast combination of ideas that merely resemble a concern for data privacy while still holding to PRC principles of utilitarian control. The best examples of this phenomenon occurring can be found in China's Cybersecurity and National Intelligence laws. While China's Cybersecurity Law offers personal data protection, the PRC government simultaneously circumvents it through language forcing cooperation with PRC state entities, implying "backdoor access" into critical data systems (Ji and Fang, 2017). China's National Intelligence Law provides similar authoritarian guidance for companies, mandating similar levels of compliance with state organizations (Chinese National People's Congress Network, 2017). Therefore, it is easy to conclude that while notions of American and EU law do exist in PRC legislation, the PRC's ability to utilize its own laws to create legal loopholes for itself will result in a draconian level of oversight and authority regarding data privacy issues, to include financial information.

While privacy regulations exist throughout the world, their conception in China remains relatively new. Furthermore, the PRC's ability to utilize these laws to provide legal precedence for government access to personal information highlights the increasing notion of the PRC's attempts to establish a surveillance state in China, something that would undoubtedly be easier through the implementation of a DCEP such as the digital yuan.

III. CBDC Design Choices to Ensure Data Privacy

The distinction between different cryptocurrency systems, to include CBDCs and DCEPs, can be found first in the distinction between token-based and account-based digital currencies. Token-based systems operate exactly like current fiat currency by being exchanged for goods or services, with the biggest concern from token-based systems being whether the physical currency being used is valid or counterfeit. An example of an accounts-based system can be seen through the Fedwire Funds Service, where individuals submit instructions for sending funds to another individual, in direct compliance with the Reserve Banks' security procedures (Garratt et. al., 2020). The key distinction in an accounts-based system is the verification of identity of both individuals within a specific set of parameters.

Currently, Bitcoin fits into the definition of both token-based and account-based systems. From the token-based side, each Bitcoin transaction is validated by verifying its history, while from the accounts-based perspective, each account is a Bitcoin address and a private key (which verifies the user's identity) is required to transact to and from that account within the parameters of a specific exchange.

The digital yuan's classification as a DCEP makes it a token-based currency (Murray, 2020). In fact, the digital yuan currently does not have any implementation of blockchain, thus necessitating complete PRC central bank involvement in the formation and distribution of the digital yuan. Therefore, it is easy to conclude that the PRC is utilizing the digital yuan to simply digitize its currency. Digital currencies are much easier for central governments to track, with this digital effort enabling increased surveillance of capital flows within and out of China. There are certainly ways to create privacy standards specific to digital currencies. However, the digital

yuan is simply not one of them, which causes alarm specifically from the data privacy protection perspective.

The PRC has long been attempted to develop its own digital currency, highlighting democratized finance and ease-of-accessibility as key selling points to drive adoption by potential consumers. China's mobile-first approach to development supports this move, with Chinese technology giants facilitating the growth of global mobile payments. However, this ease-of-use comes at a cost for consumers; by utilizing the PRC's DCEP, users are essentially opening themselves up for government scrutiny, as evidenced by the PRC's past usage of legislation such as its Cybersecurity and National Intelligence Laws to conduct such activities. Therefore, consumers must be careful if choosing to utilize the digital yuan, particularly as their information becomes captured by entities at the mercy of PRC state entities.

IV. Privacy Implementation in Digital Currencies

Implementation of data privacy protocols are certainly possible for DCEPs despite their value proposition of centralization being against the principles of cryptocurrencies and decentralized finance. Two examples of this include the Bahamian Sand Dollar and Singapore's Project Ubin, which both leverage a token-based system for DCEP implementation.

A. The Sand Dollar in the Bahamas

The Central Bank of the Bahamas has sought to implement digital transformation initiatives beginning in the early 2000s, with these efforts taking hold in recent years through 2017's publication of the Payments Instruments Oversight Regulations (The Block, 2020). The publication of these documents, along with other factors emphasizing payments and technology

innovation within the space, led to a 2018 CBDC announcement by Governor John A. Rolle (Mancini-Griffoli, 2018). In 2019, the Central Bank of the Bahamas launched a pilot of this digital currency on the island of Exuma, with full roll-out of the Sand Dollar in 20220 (Wyss, 2020).

The Sand Dollar's token design choice takes form in the fact that "all digital payments would occur in a secure tokenized environment," as described by the Central Bank. Aimed at promoting financial inclusion and access, the Sand Dollar acknowledges compliance with KYC/AML standards (Wyss, 2020), which prevents 100% anonymity and privacy. Furthermore, the Sand Dollar has implemented several policy controls to mitigate risks, limiting the amount of Sand Dollars individuals can hold, tying digital wallets to domestic bank accounts, and requiring corporate bank accounts for businesses dealing in Sand Dollars (The Box, 2020). The Central Bank of the Bahamas has highlighted consumer privacy as a significant area of emphasis for the Sand Dollar, releasing statements saying how the "Sand Dollar infrastructure incorporates strict attention to confidentiality and data protection" (McKenzie, 2020). Ensuring stakeholders of continued privacy protections regarding transactions is critical for the Sand Dollar to drive adoption, with government oversight of transactions taking place only during the KYC/AML process (Central Bank of the Bahamas, 2019). This allows users to transact in relative freedom between individuals and businesses after successful KYC/AML establishment, much like traditional financial systems today.

The Central Bank of the Bahamas' use of a token-based system demonstrates a clear example of a working DCEP that prides itself on consumer privacy in interactions. With government oversight of transactions taking place primarily only at the KYC/AML level and through several other risk mitigation factors, users in the Bahamas can transact in a manner like

cash. While no centralized digital currency can replace cash at a 100% solution, the Sand Dollar does come close, and its emphasis on individual financial privacy must be applauded.

B. Project Ubin in Singapore

Project Ubin's origins began in late 2016, with the Singaporean government announcing a five-stage plan to test and experiment with a DCEP system within Singapore (Monetary Authority of Singapore, 2021). This five-step process involved key government, technology, and user stakeholders, all of whom were able to explore a variety of commercial use cases for the Project Ubin digital token.

Project Ubin's key value proposition in design choice was exploring the implementation of a blockchain-enabled DCEP. This emphasis on using distributed ledger technology (DLT) has a variety of benefits, including increased transaction times, improved regulatory efficiency, and operational simplification, among many others (Deloitte, 2018). Some specific use cases for DLT also took form through smart contracts and cross-border payments, both of which were tested between businesses during Project Ubin's lifecycle. Government intervention and oversight over day-to-day transactions remained limited except for identify verification in compliance with KYC/AML processes (Deloitte, 2018). In short, Project Ubin's emphasis on token-driven applications of its form of the digital Singapore dollar for commercial applications proved to be a success, with a payments prototype network being developed and utilized to test different DCEP concepts to this day.

One of Project Ubin's main efforts in ensuring data privacy was to implement and test Quorum, an Ethereum privacy model implementation. Quorum introduces both on-chain and off-chain transactions while ensuring data confidentiality. Quorum works by enabling private

transactions which are addressed to a subset of nodes, with a zero-knowledge proof protocol resulting in an anonymous extension which allows the sender to hide themselves and the transaction recipients in a larger group of parties (Allison, 2019). Therefore, Quorum's benefits include increased privacy due to the Constellation encryption enclave, faster performance, and a voting based-consensus protocol. In the example of Project Ubin, the successful deployment of privacy-focused blockchain frameworks highlight the successful implementation of privacy-focused DCEPs.

Project Ubin's take on DCEPs highlights the opportunities that are possible if data privacy emphasis is a notion that governments wish to pursue. By using a distributed ledger and doing tests with Quorum, the Singapore government has demonstrated that privacy within DCEPs is certainly feasible, at least to the largest extent possible within a commercial DCEP framework.

IV. Privacy Implementation in Digital Currencies: Conclusion

All in all, the examples of the Bahamian Sand Dollar and Singapore's Project Ubin demonstrates the possibility of privacy implementation in DCEPs. While the concept of DCEPs seem to go against the ideation of cryptocurrencies, the fact remains that if there is such an emphasis placed on ensuring data privacy, technology will surely be able to facilitate this movement. As a result, these use cases, among many others, showcase the fact that privacy implementation is possible in DCEPs, as much to the extent as is possible given AML/KYC regulations.

V. The PRC's Surveillance State

The surveillance state that the People's Republic of China has created is one that grows increasingly powerful over time. From establishing a social credit system to monitoring its Uighur population, the PRC's ability to conduct mass surveillance shows the effectiveness of a governance system aimed at collecting data from those within its borders. However, the PRC's surveillance state extends even further than its domestic borders, with its effects having far-reaching implications for those in the international community. This desire to influence a new world order in the PRC's view has resulted in its ever-expanding influence, whether through initiatives such as the BRI or through other ways to continually exert power over other nation-states.

A. Use of the Digital Yuan to Manipulate Global Markets

The PRC has utilized monetary policy tools such as currency devaluation to ensure its competitive trade advantage previously. The implementation of the digital yuan would result in a more efficient and near-instantaneous ability to conduct similar economic movements. In turn, this would result in different world economics bearing the full brunt of such a potential economic shock to global economies if a digital yuan devaluation should occur.

With China's status as one of the world's largest economies and exporter of goods, the previous yuan devaluation resulted in Chinese-produced goods suddenly being cheaper when compared to other economies. This would disrupt the value of other countries' currencies, with a digital yuan being able to significantly impact the preeminence of the American dollar if utilized in such a fashion. While other countries may have been able to similarly devalue their own currencies to absorb the initial economic shock, the long-term implications of the ability to

conduct monetary policy in such a fashion has severe implications for smaller countries that have primarily export-driven economics. This would be because these nations would be forced to compete with Chinese goods which possess an unfair competitive trade advantage. The devaluation of the yuan also resulted in a variety of second-and-third order effects, with many of these actions being in growth industries such as manufacturing, energy, and much more (Investopedia, 2020).

Furthermore, the ability to inflate or deflate the value of the digital yuan would increase its power over other digital currencies, potential shaping the global cryptocurrency market in the digital yuan's favor. The PRC has already acted to limit competing digital currencies by enacting legislation limiting their use (Reuters, 2021). The act of eliminating competing digital currencies in any form highlights the strict control the PRC wishes to have over its digital yuan. Therefore, the full implementation of a homegrown DCEP would only serve to strengthen the PRC's emphasis on creating a global surveillance state, with the PRC able to better understand other nations' response to significant economic shocks for future policy implications if tested through the digital yuan. This would result in a PRC able to manipulate global markets through specialized targeting, whether this be through industry-specific disruption or through general exercises of domestic monetary policies aimed at influencing global economies.

Additionally, adoption of the digital yuan would certainly increase if its technology proves to be more efficient than current implementations of networks like the Society for Worldwide Interbank Financial Telecommunication (SWIFT) system. Often criticized for its long transaction times, high maintenance needs, and other inefficiencies, the SWIFT system is the current de-facto standard for most financial transactions, to include commercial ones. With its mobile-first approach to digital payments combined with first-mover market entry as a DCEP,

the digital yuan could have the potential to bypass international norms such as SWIFT, and rightfully so, particularly if proven to be more efficient than SWIFT. However, the digital yuan is ultimately controlled by the PRC government, thereby putting such assets converted to the digital yuan in potential jeopardy for disuse at any time. Therefore, while potentially more efficient in the short-term, the usage of the digital yuan will ultimately result in both overt and covert PRC global market manipulation in the long-term.

B. The Digital Yuan Enabling Sanction Evasion and Money Laundering as Part of the PRC's Surveillance State

The PRC's creation of the digital yuan could also enable sanction evasion efforts by threat actors seeking to subvert the global world order. The digital yuan's role in being a trusted transaction medium would play an important role in this regard, helping threat actors to pay for illicit goods or activities without a truly traceable way to hold such actors accountable.

With American sanctions affecting countries deemed risks to "national security," the PRC has immense potential to gain access and placement in other countries that pose great threats to global security. The PRC's capabilities in weapons manufacturing have resulted in a transition shift from being arms exporter to a major exporter, with a potential to become one of the world's leading arms exporters" (Raska, 2017). This ability to export weapons at a low cost have increased PRC influence in militaries across the world, with many of these other countries being subject to sanctions as well. The use of a centrally controlled digital yuan would enable currency usage outside off any true international system aimed at preventing such instances from occurring such as American sanctions. Therefore, the development of the digital yuan would help sanctioned actors avoid such roadblocks to trade, with the result being an increase in PRC

global influence and maligned actors being able to expand their ability to threaten global safety and security.

Additionally, the PRC is known to have utilized its state-owned banking structure to funnel money to threat actors including North Korea and Iran (Lehren, 2020). These cases represent just some of the known instances of the PRC utilization of its banks to support threat actors, with the full-fledged implementation of a PRC-backed CBDC serving only to further such efforts. Other significant examples of money laundering by PRC elements with an emphasis on digital currencies include a case in 2021, where Chinese nationals utilized cryptocurrencies, banks, and an informal Chinese network to launder over $30 million in drug profits for the Sinaloa Cartel (Simms, 2021). A 2020 case also saw Chinese nationals laundering over $100 million dollars in stolen cryptocurrencies from a 2018 North Korean cyberattack on cryptocurrency exchanges, with nine Chinese banks helping to move $68 million dollars. The implementation of a digital yuan would serve only to further ease such money laundering efforts between different threat actors and nations, with the PRC acting as the facilitator for such transactions.

Combined with the BRI, the ability to evade international law enforcement creates immense potential for the PRC to influence countries from a military, infrastructure, and economic lens, among many others. The ability to evade sanctions and launder money is particularly important threat actors like North Korea and Iran. This ability to evade law enforcement by transacting strictly through the digital yuan offers the PRC increased surveillance opportunities on other nations around the world, threat actor or not.

C. Using the Digital Yuan for Data Collection to Enhance the PRC's Surveillance State

Data and information collection efforts remain an important part of the PRC's surveillance state. Whether through the implementation of a social-credit system within China or through various hacks on other governments, the PRC has pursued a policy of data collection to "identify and categorize US citizens of interest, whereupon they may be targeted of intelligence gathering purposes" (Chen, 2019). The digital yuan's implementation throughout China and the world will only further these goals, particularly if individuals are forced to utilize the digital yuan to conduct transactions with Chinese citizens and companies.

As the PRC becomes increasingly embroiled in efforts relating to Great Power Competition, its desire to maintain a competitive advantage becomes increasingly apparent. The PRC's BRI efforts can only go so far in influencing other nations, and the PRC's desire to compete with the United States and Russia have resulted in a need to target individuals for intelligence-gathering purposes by accessing their data. Whether it be healthcare information or government databases, the ability to identify and target specific individuals holding critical decision-making positions in foreign policy, military, intelligence, and other sectors bodes well for potential future PRC influence operations. The implementation of a digital yuan would accelerate these efforts, with the PRC no longer necessitating high-visibility data intrusions to discover information about individuals. Instead, this information would flow naturally to the PRC by virtue of digital yuan use, enabling the PRC to continuously collect information on subjects of interest to help its cause within the realm of Great Power Competition.

While the damaging effects of such efforts may not necessarily be seen in the short-term, the long-term implications of such actions remain to be seen, if ever they become uncovered. Therefore, it is important to note how the implementation and use of the digital yuan could help

facilitate increased information collection of foreign individuals by PRC-backed entities. While the digital yuan has a variety of practical uses, its ability to collect information on individuals by violating data privacy agreements presents a national security risk for the globe too great to ignore.

VI. Conclusion

The utilization of the PRC's digital yuan, also known as a digital currency electronics payment (DCEP) platform, highlights the potential for the digital yuan to be utilized to further the PRC's information collection efforts to establish a global surveillance state within the realm of Great Power Competition. While privacy expectations to a centrally controlled currency must be managed, to include the efforts of governments to implement KYC/AML measures, the digital yuan's lack of emphasis on blockchain encryption or data privacy models points significantly to the digital yuan being nothing more than a digital tracking mechanism for PRC-backed entities. Whether through a token-based, account-based, or combined design choice, the potential to have a DCEP with successful privacy features is possible. The case of the Bahamian Sand Dollar and Singapore's Project Ubin highlight this very fact, with both projects taking pains to highlight their desire to ensure consumer confidentiality in a manner as feasible as possible. Therefore, despite the value proposition of the digital yuan enabling a more effective, and henceforth, growth-driven Chinese economy, the digital yuan still has major steps to go if consumers are to be assured that it is not simply a tool to extend the PRC's surveillance state to a truly global level.

References

Allison, Ian. “JPMorgan Adds Privacy Features to Ethereum-Based Quorum Blockchain,” CoinDesk, 2019.

Allen, Sarah, et. al. “Design choices for central bank digital currency,” The Brookings Institute. 2020.

The Block. “A Global Look at Central Bank Digital Currencies,” KPMG, 2020.

Central Bank of the Bahamas. “Project Sand Dollar: A Bahamas Payments System Modernisation Initiative,” Central Bank of the Bahamas, 2019.

Chinese National People’s Congress Network. “National Intelligence Law of the People’s Republic of China,” 12th National People’s Congress, 2017.

Chen, Ming Shin. “China’s Data Collection on US Citizens: Implications, Risks, and Solutions,” Journal of Science Policy & Governance, 2019, 15 (1), 1-14.

Deloitte. “Project Ubin: SGD on Distributed Ledger,” Monetary Authority of Singapore, 2018.

Dickenson, Kelvin. “The Future of KYC: How Banks Are Adapting to Regulatory Complexity,” Opus, 2019.

European Parliament and Council of European Union. Regulation (EU) 2016/679,” European Union, 2016.

Garratt, Rod et. al. “Token or Account-Based? A Digital Currency Can Be Both,” The Federal Reserve Bank of New York, 2020.

Huo, Jingnan. “EU’s new data privacy law creates headaches for U.S. banks.” American Banker, 2017.

Hsu, Spencer and Ellen Nakashima. “Two Chinese nationals indicted in cryptocurrency

laundering scheme linked to North Korea." The Washington Post. 2021.

Investopedia. The Impact of China Devaluing the Yuan in 2015," Investopedia, 2020.

Ji, Hannah and Jerry Fang. "Costs and unanswered questions of China's new cybersecurity regime," International Association of Privacy Professionals, 2017.

Joshi, Naveen. "The Ultimate guide to the Quorum blockchain," Allerin, 2020.

Lehren, Andrew and Dan De Luce. Secret documents show how North Korea launders money through U.S. banks. NBC News. 2020.

Murray, Robert. "Understanding China's Digital Yuan," Foreign Policy Research Institute, 2020.

Mancini-Griffoli, Tommaso et. al. "Casting Light on Central Bank Digital Currency," International Monetary Foundation, 2018.

McKenzie, Natario. "Central Bank: Sand Dollar nationwide rollout set for October 20," Eyewitness News, 2020.

Monetary Authority of Singapore. "Project Ubin: Central Bank Digital Money using Distributed Ledger Technology," Singapore Government, 2021.

Pernot-Leplay, Emmanuel. "Data Privacy Law in China: Comparison with the EU and U.S. Approaches," 2020.

Raska, Michael. "Strategic Contours of China's Weapons Exports," *RSIS Commentary*, 2017, 165 (1), 1-3.

Reuters. China bans financial, payment institutions from cryptocurrency business. Reuters. 2021.

Sharma, Yogesh and Nageshwaran R. "Understanding Data Privacy in the Financial Services World," *TCS BANCS Research Journal*, 2018, 12 (1), 30-36.

Sharma, Rakesh. "Understanding China's Digital Yuan," Investopedia. 2020.

Simms, Jonathan. “Chinese nationals used US banks to launder millions in drug profits for Sinaloa Cartel.” Yahoo News. 2021.

Ward, Orla and Sabrina Rochemont. “Understanding Central Bank Digital Currencies (CBDC),” Institute and Faculty of Actuaries, 2019.

Wyss, Jim. “Bahamas Plans E-Currency to Connect Far-Flung Island Beaches,” Bloomberg, 2020.