

SECTION IV

POLICY

Blockchain is a fundamentally borderless technology that exists in a world with many borders.

The tension that this reality creates will continue to lead to difficult policy decisions for governments. The most successful jurisdictions will find a way to balance anti-money laundering/know-your-customer (AML/KYC) requirements, consumer protection, taxation, and more with innovation. But it is not enough for individual governments to develop effective regulatory frameworks as delineated in the DCAR section; governments must work together, facilitated through [international bodies](#) (See Appendix B), to minimize frictions that stand to hamper blockchain technology's potential. The GSMI Policy Working Group examined two crucial cross-border policy topics that are currently at the forefront: AML/KYC and CBDCs.

AML/KYC

Cryptocurrency users carry out many transactions around the world every day; the Bitcoin and Ethereum blockchains facilitate around 260,000⁸⁸ and 1,260,000⁸⁹ transactions daily. The active universe of transactions conducted in cryptocurrency, however, remains stymied by a variety of policy challenges. According to the Bank for International Settlements (BIS,) the key challenges facing the use of cryptocurrency in cross-border transactions include “aligning regulatory, supervisory and oversight frameworks for cross-border payments, Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) consistency, Payment versus Payment (PvP) adoption and payment system access.”⁹⁰ The BIS has framed the problem with two perspectives: (a) the “practical perspective” for how one would set up a cross-payment infrastructure; and (b) the “macro-financial perspective,” including “examining the potential increase in cross-border flows, possible financial stability risks and currency substitution, and reserve currency configurations and backstops.”⁹¹

The “practical” concerns related to anonymous payments are largely associated with money laundering and terrorist financing. The “macro-financial” concerns involve the difficulty in coordinating the relationship between central banks to allow for access to, and settlement of, funds transfers to facilitate the cross-border use of digital currency from two or more jurisdictions. Such an arrangement would require strong cooperation among central banks, and a network of relationships that is not currently sufficiently robust to handle cross-border cryptocurrency transactions, especially if adoption becomes more widespread.⁹² The BIS has recognized that an international system of cross-border transactions in cryptocurrency requires countries to agree on the design of a transfer system that limits the risk of currency substitution.

Central banks are also concerned that cross-border transactions would create volatility in the flow of capital that will upset markets as well as “contagion risk,” or the fear that financial instability in one country will spill over into another country through high numbers of these transactions.

A lack of standardized definitions of virtual currencies, cryptocurrencies, and cryptoassets poses further challenges for cross-border transactions and regulations. India offers a prime example of

these challenges. Indian law defines “currency” with a specific list of categories, including currency notes, money orders, cheques, and credit cards.⁹³ But virtual currencies are not included in this list. In 2015, the Reserve Bank of India issued a regulation interpreting the statute which added to the definition of currency to include “debit cards, ATM cards or any other instrument by whatever name called that can be used to create a financial liability.”⁹⁴ The challenge here is that “in the case of virtual currencies such as Bitcoin, there is no entity that is accepting financial liability in connection with the instrument.”⁹⁵

HOW COUNTRIES AND ORGANIZATIONS ARE ADDRESSING THESE ISSUES

National regulators and organizations around the world are working to develop rules to govern digital assets. The G20 is focused on enhancing cross-border payments and has endorsed a comprehensive program to address challenges.⁹⁶ Regulators also see the value of digital currency in the world economy. According to the BIS, “Faster, cheaper, more transparent and more inclusive cross-border payment services would deliver widespread benefits for citizens and economies worldwide, supporting economic growth, international trade, global development and financial inclusion.”⁹⁷

The consistent theme, however, indicates that while some governments have become increasingly receptive to virtual currency and cryptocurrencies, many have yet to develop laws that specifically regulate virtual currency. The lack of clarity in the marketplace has made accepting virtual currencies for cross-border payments difficult because their use still involves risk under some laws. Moreover, it is unclear how and whether enforcement authorities would apply these laws to cryptocurrencies.

Some countries, such as India, have attempted to regulate the transfer of cryptocurrency across borders through their customs laws. Several commentators have suggested that

cross-border transfers of cryptocurrency may fall under India’s Foreign Exchange Management Act, which would regulate cross-border cryptocurrency transactions as a movement of “goods.”⁹⁸

Despite ongoing debate about whether certain cryptocurrencies are securities, some regulators treat virtual currency under the current regulatory framework for “goods” or “property” as part of their efforts to apply existing rules applicable to guard against money laundering and terrorist financing to virtual currency.⁹⁹

FATF AND CROSS BORDER CONSIDERATIONS

According to the FATF guidance, Virtual Asset Service Provider (VASP) is defined as any natural or legal person who, as a business, conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

- Exchange between virtual assets (VA) and fiat currencies.
- Exchange between one or more forms of virtual assets.
- Transfer of virtual assets.
- Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets.
- Participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.

As set out above, the definitions do not depend on the technology employed by the service provider. The obligations in the FATF Standards stem from the underlying financial services offered without regard to an entity’s operational model, technological tools, ledger design, or any other operating feature. One key advantage of the FATF guidelines is that they focus on the types of services provided, not on terminology or nomenclature used to describe the services, which could lead to greater consistency within the global regulatory framework.

However, the FATF recognizes that its

approach can bring practical challenges to competent authorities in identifying which entities are VASPs and defining their regulatory perimeter. Launching a service that will provide virtual asset services, for instance, does not relieve a provider of VASP obligations, even if those functions will proceed automatically in the future, especially, but not exclusively, if the provider will continue to collect fees or realize profits, regardless of whether the profits are direct gains or indirect. For purposes of determining VASP status, launching a self-propelling infrastructure to offer VASP services is the same as offering them, and similarly commissioning others to build the elements of an infrastructure is the same as building them.

Where there is a central developer and governance body which is a financial institution (FI) or a VASP, it could be held accountable for the implementation of AML/KYC controls across the arrangement and for taking steps to mitigate ML/TF risks. These organizations should consider taking steps to limit the scope of customers' ability to transact anonymously and/or ensuring that AML/KYC obligations are fulfilled on an ongoing basis (e.g., by using software to monitor transactions and detect suspicious activity). Not all stablecoins may have a readily identifiable VASP/FI central body once launched. However, it may be more likely that a party needs to exist to drive the development and launch of such an arrangement before its release. If this entity was a business and carried out VASP functions, this would create scope for regulatory or

supervisory action in the pre-launch phase.

NEXT STEPS FOR CROSS-BORDER COLLABORATION

The law, and technology, is constantly changing, and there will need to be an effort to provide more direct guidance to users of virtual currencies. The international community will need to reach a consensus on whether regulation should focus on stopping the use of virtual currency or on monitoring and reporting on its use.

Cryptocurrencies are facing increased regulation in several countries, including the United States. The focus of the regulations, however, has largely been on increasing transparency and central management in exchanges rather than structuring more efficient means of exchange. U.S. regulators proposed reducing the threshold for transaction reporting from \$3,000 to \$250 because of claims that

"[c]riminals are using smaller value transfers and virtual currencies to facilitate terrorism financing, narcotics trafficking and other illicit activities, like cybercrime."¹⁰⁰

It will be important, as regulation moves forward, to have accurate data on actual use patterns by both legitimate users and illicit actors. Some have argued, however, that this feature is built into cryptocurrency



transactions.¹⁰¹

It is still early, but there is technology being developed to improve and manage processes for KYC and AML compliance, including some which offer zero-knowledge proof (ZKP) solutions that protect personal information without having to sacrifice safety and functionality. These and other “reg tech” offerings seek to leverage the security and verifiability of blockchain technology and provide regulators with assurance that bad actors are not using decentralized systems to conduct illicit transactions. Companies like Coinfirm, Chain Analysis, and Ciphertrace are among the burgeoning field of crypto analytics companies that monitor blockchain transactions and provide real-time alerts to flag potential sources of risk, among other services.

In July 2021, a group called the Global DeFi Coalition, which includes a half-dozen international blockchain-related trade groups, representing more than 350 companies,

issued an open letter to FATF calling for “well-balanced” regulations, including ways to streamline AML and KYC requirements; for example, by allowing financial intermediaries to collaborate when identifying clients so that these checks don’t have to be run multiple times to execute a single transaction.¹⁰²

CBDCs

In a relatively short period of time, CBDCs went from a niche technological idea to a concept that over 80 countries representing over 90 percent of global GDP are investigating.¹⁰³

While most central banks are first considering the domestic implications of CBDCs, there have been numerous cross-border experiments. Central banks are interested in CBDCs for a variety of reasons, including limiting the influence of private stablecoins, improving financial inclusion, and reducing costs. As the response to COVID-19 demonstrated, CBDCs could also be used to improve the efficiency of “helicopter drops,” as stated by the U.S. House



of Representatives Committee on Financial Services:

"In CBDC models where every citizen has a digital wallet, or the government has visibility into wallet ownership, the speed at which these distributions can be made increases considerably while also ensuring that those who are traditionally not served by the banking sector and most in need of countercyclical assistance would be able to benefit."¹⁰⁴

WHAT ARE THE MAIN ISSUES THAT CBDCs PRESENT?

As detailed in a joint BIS, International Monetary Fund (IMF), and World Bank Group report to the G20 on CBDCs for cross-border payments, the proliferation of CBDCs has a wide variety of opportunities and consequences which will vary widely depending on the design of each CBDC. The report states that "cheaper and more accessible remittances will benefit senders and recipients, help to buffer economic shocks, and stimulate growth. Markets should also become more integrated, thus offering investment and risk-sharing opportunities. This would facilitate hedging, though it could increase contagion risks."¹⁰⁵

Additionally, as CBDCs could make it easier and cheaper to store and spend foreign currency, "already established international currencies [could become] even more attractive... This would contribute to more widespread currency substitution via the adoption of a foreign CBDC, especially in countries with high inflation and volatile exchange rates." This could have significant effects on countries' ability to control their monetary policy and "increase risks for runs on both domestic banking sectors and currencies." The report speculates that currency substitution could also undermine central banks' ability to act as a lender of last resort.

These represent just some of the manifold risks associated with the proliferation of CBDCs. Other risks include consumer protection, privacy, tax avoidance, and

increased volatility in FX rates.

HOW COUNTRIES AND ORGANIZATIONS ARE ADDRESSING THESE ISSUES

Perhaps most significantly, China has undertaken a number of pilots, including a trial with the BIS and the central banks of Hong Kong, Thailand, and the U.A.E, called the mCBDC Bridge. According to the post-phase two report, the prototype tested enabled the central banks "to control the flow of their CBDC and to monitor transactions and balances of their issued CBDC, with programmable levels of transaction privacy and aspects of automated compliance. The prototype demonstrates a substantial increase in cross-border transfer speed from days to seconds, as well as the potential to reduce several of the core cost components of correspondent banking."¹⁰⁶ The next phase will involve "further experimentation with design choices and technology trade-offs and a future roadmap from prototype to a production-ready network that can serve the broader central banking community as a public good through open-sourcing."

This is just one example of central banks collaborating to test cross-border CBDCs. In July 2021, the Banque de France and the Monetary Authority of Singapore completed an experiment that "simulated cross-border and cross-currency transactions for Singapore Dollar CBDC and Euro CBDC, and was conducted using a permissioned, privacy-enabled blockchain based on Quorum technology."¹⁰⁷

Recently, the central banks of Australia, Malaysia, Singapore, and South Africa announced that they would be conducting a cross-border CBDC trial.¹⁰⁸

Reflecting the general attitude towards current CBDC research, China's e-CNY whitepaper stated that "cross-border payment involves various complicated issues such as monetary sovereignty, foreign exchange policies and arrangements, as well as regulatory and

compliance requirements... Therefore, though technically ready for cross-border use, e-CNY is still designed mainly for domestic retail payments at present.”¹⁰⁹ President Xi Jinping has also called on the G20 to “discuss developing the standards and principles for central bank digital currencies with an open and accommodating attitude, and properly handle all types of risks and challenges while pushing collectively for the development of the international monetary system.”¹¹⁰

NEXT STEPS FOR CROSS-BORDER COLLABORATION

It is encouraging to see central banks, especially those of some of the largest economies in the world, are closely examining the risks associated with CBDCs. Countries engaging in cross-border research and experimentation should continue these efforts, and more countries should join the effort. Thoughtful and deliberate planning and design, including information sharing between central banks, will become more critical as larger economies, such as Nigeria,¹¹¹ begin to release their CBDCs on a wider scale.

In October 2021, the G7 released a statement on CBDCs, stating that strong “international coordination and cooperation on these issues helps to ensure that public and private sector innovation will deliver domestic and cross-border benefits while being safe for users and the wider financial system.”

The statement further notes “the importance of considering interoperability on a cross-border basis,” while also recognizing “a shared responsibility to minimise harmful spillovers to the international financial system.”

The G7, G20, Financial Stability Board, BIS, regional blocks, and other international organizations must facilitate international coordination and ensure that countries are not rushing to release a CBDC in competition with one another, creating a race to the bottom that could have serious consequences.

MARKET MANIPULATION

Today’s digital assets market closely resembles the capital markets that existed a century ago.¹¹² Cross-border transactions of digital assets can add yet another layer of complexity, making manipulative transactions more difficult to track and flag. While it has been confirmed that intentional market manipulation does occur, there are also instances where market manipulation



Figure 2: Geographic Distribution of Market Manipulation Activity (Source: [Amplyfi.com/insights](https://amplyfi.com/insights))



occurs through unintentional transactions.¹¹³ Either way, regulation and surveillance are paramount in ensuring equality and fairness in newly emerging exchanges, while ensuring that cross-border transacting is not used to camouflage intentional manipulation.

Other than some anecdotal events, little research has been done to confirm the intentional manipulation of cryptocurrency across borders, or to identify how traders may leverage the lack of regulation across borders to gain quick wins. However, what is known is the potential that cross-border transactions have to cause more confusion around both intentional and unintentional transactions, resulting from the lack of transparency among the various regulated and non-regulated exchanges, and across regulatory bodies.

HOW CRYPTOCURRENCIES ARE MANIPULATED BY MARKETS

There are several known strategies used by some nefarious traders to intentionally manipulate the cryptocurrency markets. Some will use initial coin offerings (ICOs) to gain leverage on a particular exchange, especially where ICOs are not regulated to prevent unfair leverage through large purchases of digital assets. These ICO events, if not properly regulated, can lead to unfair leverage and temporary spikes in market price that will work to the advantage of the buyer. Some will use the classic pump and dump strategy to create the illusion of an artificial increase in market activity, also leading to temporary spikes in market prices, which can lead to quick gains through the sudden selloff of digital assets.¹¹⁴

Other manipulation strategies involve setting up ghost accounts that can help disguise large trade volumes by a single company or individual, thereby manipulating market prices. This is known as wash trading, which takes advantage of the anonymity associated with some cryptocurrency accounts. Spoofing is yet another strategy; it uses illegitimate orders, often leading to manipulated spikes and dips in prices. The introduction of leveraged derivatives has made these price-impacting strategies even more effective, especially when combined with the ability to quickly sell on the spot market. The combination of wash trading, spoofing and leveraged derivatives can potentially have an impact on cross-border manipulation, and can potentially be used as an act of international political aggression if not properly regulated.

CHALLENGES WITH TRACKING AND CONTROLLING MANIPULATION EVENTS

The digital currency marketplace has evolved so quickly that regulators continue to struggle to keep up.¹¹⁵

Additionally, transactions can occur so rapidly that it is virtually impossible to detect intentional acts of manipulation and prevent them from happening in real time. New trading instruments and services are constantly being created, thus perpetuating the complexity and difficulty to regulate. To add to the challenges of regulation, traders will often use multiple exchanges and instruments, and transact across multiple borders. With all of these avenues for potential fraud and abuse, it can be difficult, or impossible, to detect legitimate transactions and trades from those that are done with the intent of fraudulent manipulation.

NEXT STEPS IN PREVENTING MARKET MANIPULATION ACROSS BORDERS

Regulation alone will not provide the security and safety for all traders and investors in this space. Addressing this problem will require transparency and cooperation among various national regulatory bodies, exchanges, and service providers. For example, the formation of one centralized governing body, or the expansion of an existing cooperative work group like the Financial Action Task Force (FATF), that can work to oversee the activities of all exchanges in all countries and provide guidance and tools towards enhanced regulation and control within the exchanges.¹¹⁶

In any type of financial market, there are two approaches used for internal control. These are preventive and detective controls. While the latter attempts to quickly identify and prevent an unauthorized transaction from occurring, the latter relies on the belief that such a transaction cannot be prevented, but can be detected, and followed up with a reversal of that transaction, or a penalty, thus discouraging such events from happening. Applying such controls around those areas most likely to be abused, such as leveraged derivatives, spot markets, etc., could be a first line of defense for regulators.

Exchanges themselves must provide real-time surveillance and monitoring of transactions,

so that events showing signs of deception can be flagged and addressed.¹¹⁷ Self-certification requirements in spot markets can also thwart devious activities, as well as imposing tighter controls and requirements around highly leveraged crypto derivatives.

Artificial intelligence and machine learning technologies offer another means of actively monitoring the transaction landscape across diverse trading platforms. Vetted AI and machine learning algorithms could be used to detect nefarious patterns in trading. This can be done at a pace and consistency level that would be impossible for humans to achieve, potentially leading to a more preventive type of control mechanism.

CONCLUSION

The cross-border nature of blockchain, cryptocurrencies, and CBDCs is creating novel problems and opportunities for legislators, regulators, businesses, and organizations to address. When crafting guidelines for this new industry, it is important that governments do not become fixated on cryptocurrency as a tool for criminals. Its illicit use is a problem, but as the FATF estimated in 2015, “between hundreds of billions and a trillion U.S. dollars” are laundered each year in cash, with a majority of countries surveyed indicating “that cash smuggling is an increasing problem.”¹¹⁸ This is not intended to serve as whataboutism, but rather to indicate the vastly different scopes of the problem: the total crypto market cap is \$2.5 trillion as of this writing, with an estimated \$10 billion in criminal activity in 2020.¹¹⁹ Governments therefore must attempt to balance innovation and regulation, ideally in communication with other governments so as to harmonize regulations and learn from mistakes and successes.