ICAIE
INTERNATIONAL COALITION
AGAINST ILLICIT ECONOMIES

Central Bank Digital Currencies: Risks and Rewards

Global Finance and the Fight Against Money Laundering

John Cassara
David M. Luna

January 2025

In the financial world, there are few near term developments that will affect all of us more than a possible global implementation of central bank digital currencies (or "CBDCs"). As money and payments have become more digital around the world based on consumer and business transactional activities, central banks are exploring central bank digital currencies (CBDCs).

The widespread adoption of CBDCs could represent the most radical change to the world monetary system since the 1970s collapse of the Bretton Woods Agreement. They have the potential to upend the way people buy, spend, borrow, and save. Depending on their form, CBDCs could transform commercial payments and interbank transfers. CBDCs could also have significant impacts on international relations and international law enforcement operations to counter criminality and financial fraud.

New CBDC currency confederations and alliances could completely transform the current global financial order. On one hand, the CBDC model could give authoritarian governments absolute control of its citizenry. On another, perhaps most intriguing, CBDCs could move us from the theory of financial transparency to the actual ability to finally be able to follow the hidden money trails of kleptocrats, transnational organized crime, terrorists, and other illicit threat networks.

However, a critical consideration in the current debate over the next five years in the United States will be the policy positions taken by a re-elected President Trump, who while supporting decentralized cryptocurrencies such as bitcoin, has been critical of a digital dollar and the creation of CBDCs. Another influential vector will be President Trump's trade tariffs on imports and whether any geopolitical insecurity can alter the future viability of CBDCs, including factors related to the volatility of currency markets, possible dollar devaluation pressures, and international monetary policies. In December 2024, for example, Mr. Trump warned that he could place 100% tariffs on BRICS countries, which include Brazil, Russia, India, China and South Africa, if they try to replace the U.S. dollar as the main global currency. At the start of January 2025, Mr. Trump also said that he plans to establish a U.S. bitcoin strategic reserve. Similarly, China announced that in early 2025, that it had imposed new forex regulations to force banks to closely monitor and report transactions involving crypto assets in efforts to rein in illegal cross-border financial activities such as underground banking, cross-border gambling, and crypto trading.

This paper will explore some of these issues in greater depth. But first, we must begin any discussion with defining some key terms.

What is a Central Bank Digital Currency?

A CBDC is one category of digital assets, or a digital representation of value in digital form that is cryptographically secured, and recorded in a distributed ledger (e.g., block chain) or similar technologies.[1] Forms of digital assets may be exchanged across digital asset trading platforms, including centralized and decentralized finance platforms, online marketplaces, or through peer-to-peer technologies for transactional purposes. Digital assets can be used as a form of money or be a security, a commodity or a derivative of either.[2]

For example, digital financial assets include cryptocurrencies, non-fungible tokens (NFTs), and stablecoins. The best-known cryptocurrency is Bitcoin. Launched in 2009, it was the first cryptocurrency. Today, more than 21,000 different cryptocurrencies have evolved and have followed in Bitcoin's footsteps. Their increase in popularity is particularly pronounced among younger populations. Another type of cryptocurrency are stablecoins, whose value is pegged to an asset or a fiat currency like the U.S. dollar or euro.

Cryptocurrencies are used both as an alternative payment process to traditional payment methods or often as a speculative investment. Cryptocurrencies and stablecoins are issued by private groups or companies, sometimes as a protest against traditional monetary authorities. Cryptocurrencies, stored in digital wallets, operate across online networks without the need for a central authority, such as a bank or government. They use decentralized distributed-ledger technology. Multiple devices all over the world, not one central hub, are constantly verifying the accuracy of the transaction/s, recording them, and issuing new units. Counterfeiting and some financial frauds are prevented via cryptography or the practice of developing and using coded algorithms to protect and obscure transmitted information.[3]

Cryptocurrencies are gaining in popularity with retail and e-commerce sectors over traditional fiat alternatives.[4] They provide vendors secure, fast, and cost-effective payment processing with fairly robust traceability of a payment transaction. Unlike traditional payment systems such as the use of credit cards or checks, cryptocurrencies often do not require intermediary third-party processors and associated fees to facilitate transactions. In addition, cryptocurrencies promote access to an expanded customer base.

It is believed by many users (sometimes erroneously) that purchases and investments in cryptocurrencies are untraceable and offer anonymity. This is one reason why cryptocurrencies are the payment method of choice on the Dark Web and are also frequently used by fraudsters and scammers of all sorts that operate on social media and other platforms. However, while pseudonymous, it remains possible to trace and link activity to specific transactions and related cryptographic addresses.

Cryptocurrency accounts are not backed by governments. For example, in the United States cryptocurrency held in accounts is not insured. Within limits, the Federal Deposit Insurance Corporation does insure bank accounts. However, if something untoward happens to a crypto account or cryptocurrency funds — for example, the company that provides storage for a crypto wallet goes out of business or is hacked

— the U.S. government has no obligation to intervene.

Central bank digital currencies (CBDCs) are also a digital asset. Unlike cryptocurrencies, a CBDC is a digital version of a country's currency that is issued by a country's central bank/federal reserve. There are various forms of CBDCs (discussed below). They are all legal tender. They differ from cryptocurrencies and other forms of digital financial assets because they are the same as a country's traditional currency; i.e., they are centralized and a liability of the issuing central bank. CBDCs enjoy "the full faith and credit" of the issuing country's traditional national currency.

According to the U.S. Federal Reserve, "While Americans have long held money predominantly in digital form—for example in bank accounts or financial investments, payment apps or through online transactions—a CBDC would differ from existing digital money available to the general public because a CBDC would be a liability of the Federal Reserve, not of a commercial bank or financial investment firm." [5]

"Central bank-issued money," often called fiat money, refers to money that is a liability of the central bank in the form of cash or deposits. In the United States, there are currently two types of central bank-issued money: 1) physical currency not backed by a physical commodity such as gold or silver issued, and backed, by the Federal Reserve; and 2) digital balances held by commercial banks at the Federal Reserve.[6]

Why Are CBDCs Being Developed?

- The COVID-19 pandemic accelerated the shift to digital payments in general.
- Most developed countries are already moving away from cash-centric economies.
- As money and payments have become more digital, many of the world's central banks realized that they need to provide a public option.
- CBDCs would allow for real-time or instant payments/settlements.
- Cryptocurrencies like Bitcoin have grown dramatically. Their use is becoming normalized.
- Many governments and business interests are wary of cryptocurrencies because it is outside of their control; thus, the development of CBDCs is the established order's reaction to cryptocurrencies.
- Many developmental organizations feel CBDCs will provide financial inclusion and payment options to the general populace.
- CBDCs can reduce the need for cash handling and transportation, which can be expensive and pose security risks.
- Introducing competition in the domestic payments market might increase payment efficiency and lower transaction costs.
- Some observers feel CBDCs could be used to reduce cross-border friction in international transactions.
- Some economic and political blocs believe widespread use of CBDCs and currency federations or interoperability between select currencies could weaken the dollar and minimize the effectiveness of sanctions.
- CBDCs could be more secure than cash and other digital assets.
- CBDCs could provide issuing governments enhanced tax collection, cut down on forms of financial fraud, and provide transparency in capital flight.
- CBDCs could make it easier to identify and stop criminal activity.
- In theory, CBDCs would enable financial crimes investigators to follow the money trail.

How Many CBDCs Are There or Under Development?

According to the Atlantic Council's Geoeconomics Center,[7] as of May, 2020, 35 countries were in various stages of exploring the development and implementation of CBDCs. By September 2024, that number has grown to 134, including a near majority of Central Banks in the advance stage of development, rollout, or pilot.[8] The countries and currency unions involved represent 98% of global GDP.

The Bahamas were the first economy to launch its nationwide CBDC — The Sand Dollar. Today, Jamaica, Cambodia and Nigeria also have fully launched operable CBDCs. All four countries are focused on expanding the reach of their retail CBDCs domestically.

Every G20 country is exploring a CBDC, nearly all of them are in advanced

development. A digitalized Euro is under development. And European countries are increasingly testing wholesale CBDCs (see below), both domestically and across borders.

Some G20 countries are in the pilot stage of development, including Brazil, Japan, Turkey, Russia, and India. For example, India's CBDC is the digital rupee (e₹), which is a digital version of the Indian paper currency rupee. It is not a cryptocurrency. The digital rupee is issued by the Reserve Bank of India (RBI), the country's central bank. It is governed and managed by them. The digital rupee app allows users to load, collect, send, and redeem digital rupees. The RBI launched a pilot program for the digital rupee on December 1, 2022 in selected cities, including Mumbai, New Delhi, and Bengaluru. The pilot will be expanded to include more cities. Reliance Retail, the country's largest retail chain, began accepting payments in digital rupee in stores during a pilot stage in 2023.

China has the world's second largest economy. It's digital yuan (e-CNY) is the largest CBDC pilot in the world. In June 2024, total transaction e-CNY volume reached 7 trillion ($986 billion) in 17 provincial regions across various sectors. China's authoritative model CBDC will be discussed in more detail below.

Status of CBDC Development in the U.S.

On March 9, 2022 President Biden signed Executive Order 14067[9] that authorizes a national study on the responsible development and adoption of digital assets including a federal digital dollar:

> *While many activities involving digital assets are within the scope of existing domestic laws and regulations, an area where the United States has been a global leader, growing development and adoption of digital assets and related innovations, as well as inconsistent controls to defend against certain key risks, necessitate an evolution and alignment of the United States Government approach to digital assets. The United States has an interest in responsible financial innovation, expanding access to safe and affordable financial services, and reducing the cost of domestic and cross-border funds transfers and payments, including through the continued modernization of public payment systems. We must take strong steps to reduce the risks that digital assets could pose to consumers, investors, and business protections; financial stability and financial system integrity; combating and preventing crime and illicit finance; national security; the ability to exercise human rights; financial inclusion and equity; and climate change and pollution.*

Executive Order 14067 lays out a national policy for digital assets across six key priorities: consumer and investor protection; financial stability; illicit finance; U.S. leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation. E.O. 14067 places "the highest urgency on research and development efforts into the potential design and deployment options of a United States CBDC." Of course, the special status of the U.S. dollar as a world

currency presents many complicating factors on whether or not the Federal Reserve would adopt its own CBDC.

The United States is also participating in a cross-border wholesale CBDC project, Project Agora,[10] developed by the Bank for International Settlements (BIS), in partnerships with numerous central banks, and other private sector financial firms. The Project Agora's goal is to tokenize cross-border payments with an integrated, programmable infrastructure that brings together seven central banks and commercial banks; the Bank of France (representing the Eurosystem), Bank of Japan, Bank of Korea, Bank of Mexico, Swiss National Bank, Bank of England and the Federal Reserve Bank of New York. In May 2024, the project opened up calls for private sector participation.

However, in May 2024, the US House of Representatives also passed H.R. 5403, the "CBDC Anti-Surveillance State Act.[11] H.R. 5403 received broad support. The legislation blocks the creation and issuance of a U.S. CBDC without congressional authorization. The backers are afraid unelected officials would greenlight a U.S. CBDC that might infringe on Americans' financial privacy. The legislation specifically prohibits the Federal Reserve from offering certain products or services directly to individuals that rely on a U.S. CBDC. The bill restricts the possible use of CBDCs for monetary policy only. Backers of the bill are afraid that a U.S. CBDC might eventually incorporate aspects of the authoritarian surveillance model described below.

The CBDC policy moving forward in 2025? As cryptocurrencies have become increasingly mainstream, President-elect Donald Trump has changed his position and moved to embrace them. Mr. Trump campaigned on the right of every American to have "self-custody of their digital assets." Mr. Trump believes America should play a leading role in Bitcoin. He said the U.S. should not surrender related AI and blockchain technologies to other countries. But with respect to the creation of a U.S. CBDC, he stated during the recent campaign, "I am also making another promise to protect Americans from government tyranny. As your president, I will never allow the creation of a central bank digital currency."[12]

CBDC Technology is Based on Blockchain

Technological advances have ushered in a wave of new private-sector financial products, services, and e-commerce including digital wallets, mobile payment apps, and new digital assets such as cryptocurrencies and stablecoins. Proponents of CBDC innovation believe the various CBDC models (discussed below) can take advantage of the technology pioneered by crypto development to create a more efficient, central-bank-backed digital payment system.

Crypto currencies rely on distributed ledger technology. Blockchain is a specific type of distributed ledger technology where data is stored in blocks linked together in a chain, creating a decentralized and immutable record of transactions. Blockchain records confirm cryptocurrency transactions or trades, like a digital public ledger. It collects and stores information about buying, selling, or exchanging digital assets.

Blockchain technology, as we currently know it, was created for Bitcoin – the first and most recognized digital currency. With crypto currencies, every participant can verify transactions independently. Often individuals' accounts are protected using cryptography and pseudonymous.

Similar to crypto currencies, a CBDC integrates blockchain technology to securely record and verify all transactions. The difference is that instead of individual users having control and being able to independently verify the veracity of a transaction, a central bank/government controls its issuance and manages the system. Most CBDCs use "permissioned" blockchain where access to the network is restricted to authorized participants only, unlike public blockchains like Bitcoin.

Forms of digital payments are already widespread in the United States and most other developed countries. However, digital payments are not always fast, inexpensive, or widespread. In contrast, CBDCs would presumably allow for real-time or instant payments/settlements. A CBDC would allow holders to store value in their digital wallets and make instantaneous payments digitally. Similar to physical or fiat currency, the crypto currency would be backed by the central bank.

Proponents of CBDCs stress accessibility. For example, a digital dollar should be accessible to anyone, not just those with the latest smartphones. This could be done through chip-based cards, point-of-sale systems, or web accounts. Of course, features will vary. And all CBDCs, even those few that have been implemented, are still under development and being refined along the way. In many cases, some governance and operability issues still remain unresolved.

CBDC Models

There are four basic models for CBDCs. Each has variations. All CBDC models require modifications of the current division of labor between the central bank and private or traditional providers of money in respect of execution of traditional fiduciary relationships and recording of payments and client servicing. "Private money" is issued by commercial banks in the form of deposits and non-bank financial institutions in the form of electronic money (e-money).[13]

The four models vary in large measure by the amount of government control.

Wholesale

Wholesale CBDCs are for financial institutions to use for interbank transfers and holding reserves. Proponents argue that wholesale CBDCs should help banks make payments faster and more efficient and unlock new opportunities in streamlining cross-border payments, foreign exchange and cross-country securities transactions. Wholesale CBDCs represent less of a shift from the current way of doing things compared with retail CBDCs because domestic wholesale CBDCs operate similarly to the way commercial banks hold reserve funds with central banks today.

Retail

Retail CBDCs are designed for the general public including consumers and businesses. Retail CBDCs will encompass everyday buying, selling, saving and borrowing. They are, in effect, digital cash, but eliminate the need for physical or fiat currency. Traditional cash or fiat currency may or may not be allowed, and could be eased out over time with the global implementation of CBDCs. The customer may have an account or wallet directly with the central bank. Improving financial inclusion is a key reason that some governments are considering retail CBDCs. Some proponents argue that retail CBDCs will improve the efficiency and safety of payments.

Hybrid

As the name implies, hybrid CBDCs are more adaptable. They can be used by both the general public - primarily for large purchases - as well as by financial institutions. But the government via its central bank does not track the public's everyday personal debits, credits, expenditures, etc. In this model, the central bank issues and manages the CBDC and traditional financial intermediaries such as banks and money service businesses continue to provide customer onboarding and other services. Traditional financial intermediaries also handle financial transactions with customers as well as know-your-customer (KYC) and anti-money laundering (AML) requirements. The intermediary issues a claim to consumers and backs each claim with a CBDC holding at the central bank. Instead of having an account or e-wallet with the central bank, the customer uses the intermediary to access their CBDC.

Authoritarian

Over time, the authoritarian CBDC model completely does away with physical currency. Authoritarian CBDCs are the only allowable currency of the land. They are used for wholesale, retail, and cross-border purposes. In theory, there will be increased efficiency and ability to achieve financial transparency. In conjunction with social monitoring and scoring (see below digital yuan description) and digital identification, the authoritarian model gives government total control of its populace because it will monitor buying, selling, savings, investments and cross-border transfers. State surveillance and intrusiveness into personal privacy areas and citizens' financial activities also would arise and pose additional risks from data leakages, data abuses, cyberattacks, and potential cross-border payment data flows. Authoritarian controlled models could also restrict payments users can make with CBDCs, freeze or seize their assets more easily for any malign objective or capricious reason, or deny access or limit what people can buy or own, especially in jurisdictions where the rule of law is weak and institutions captured (operated) by the state for targeted policies. Internationally, an authoritarian model can be exploited, as it connects with other CBDC systems to destabilize markets or advance asymmetrical geopolitical dominance. A complete authoritarian model would rely entirely on digital, secured infrastructure.

Possible Security Risks of CBDCs

- Power grid disruptions: a CBDC relies on a country's electronic infrastructure. The collapse of a power grid or power outages caused by natural disaster or man-made attacks could render the use of CBDCs inoperable.
- Cybersecurity risks: CBDCs are vulnerable to cyberattacks that could lead to the loss of sensitive information or the complete breakdown of the system.
- Privacy risks and compromised financial autonomy: CBDCs can be used to exert absolute surveillance over communities; and track individuals' personal and financial activities with associated privacy and civil liberty concerns.
- Disintermediation of banks: depending on the CBDC model, CBDCs could weaken the power of banks and possibly jeopardize financial stability.
- An authoritarian CBDC - in conjunction with digital identification, social control and scoring - could lead to "demonetization" as a medium of control, subversion, or punishment.
- Technical and regulatory complexity.

Authoritarian CBDC Model Example – Digital Yuan (e-CNY or e-RMB)

In 2017, the People's Bank of China announced the development of its CBDC. The digital yuan or e-CNY, also known as the digital renminbi or e-RMB, is the world's first digital currency issued by a major economic power. The digital yuan is the largest CBDC pilot in the world. In June 2024, total transaction volume reached nearly $1 trillion dollars equivalent in 17 provincial regions across many sectors such as education, healthcare, and tourism. The use of the Chinese CBDC is growing quickly. The 2024 transaction volume is nearly four times the 1.8 trillion yuan ($253 billion) recorded by the People's Bank of China in June 2023.[14]

The CCP's move towards a national digital currency is only one part of its tripartite digital authoritarian model. In addition to phasing in an all-inclusive and all-controlling authoritarian CBDC, China is phasing out cash while simultaneously embracing technology that promotes national digital identification merged with high surveillance technologies and social scoring, all controlled by advanced artificial intelligence (AI).

Chinese citizens and residents are issued a digital number. Personal identifying information (PII) facilitates the CCP's surveillance state. The communist government tracks individuals' employment, medical, criminal, and schooling records as well as their buying habits, online browsing records, voiced political views, and even—through GPS technology—the places they have visited in China, and possibly abroad.

For example, if an individual jaywalks, the forbidden activity will be picked up by one of the 700 million CCTV surveillance cameras installed throughout China. The

footage will then be run through facial recognition software. All the collected personal data is then combined and processed and the individual is given a "social credit" score. "Bad" citizens are punished, but "good" citizens are rewarded.

In China, the catalyst and enabler for its CBDC model is mobile payment technology. Mobile payments have been enthusiastically adopted by mainstream Chinese society. Chinese citizens, both urban and rural, use the ubiquitous mobile phone for almost all of their day-to-day communication and financial needs such as banking, shopping, and person-to-person (p2p) payments. In retail establishments, the most popular way to pay by phone is via QR code scanning. Even street beggars on Chinese streets hold signs with QR codes enabling them to solicit assistance. According to a 2023 survey by the Payment & Clearing Association of China, the penetration rate of QR code payments in China is 92.7 per cent.[15]

It is becoming increasingly difficult in some areas in China to buy groceries, pay for a taxi ride, or settle a bill at a restaurant without access to a mobile wallet. And, if by chance, a Chinese citizen doesn't happen to have a phone, that isn't going to be a problem much longer. A consumer just has to smile to pay for purchases. Facial recognition payment systems have been rolled out in over 100 Chinese cities. The system is designed to read nodal points in human faces which act as one's "facial signature." It is much the same technology used in the surveillance state's social credit scoring.

The implications are enormous. Without cash, the CCP could deny a citizen access to funds to travel, eat, pay rent, pay for utilities, buy clothing, or provide for his or her family. Controlling money digitally provides the power to cut off an individual completely from the centralized monetary and financial system. A dissident, or even a rebellion, can be put down with a few clicks on an interface. The victim's assets are frozen and possibly seized. He or she is left without financial means. Demonetization might make some jail sentences unnecessary.

The complete implementation of the CBDC authoritarian model will also help the CCP combat some major entrenched challenges including tax evasion, underground banks, capital flight, and money laundering.[16] But the primary CCP objective is to further increase state control over the economy, citizenry, and homeland security. Externally, CCP could do the same in other countries to increase and manifest its goals for geopolitical dominance.

Are CBDCs the "Silver Bullet" for Law Enforcement?

Outside of crimes of passion, illicit actors, criminal entrepreneurs, and criminal organizations commit crimes for money. Once they start collecting a lot of criminally-derived funds, they try to hide it or disguise it; in other words, they will launder the dirty money.

Nobody knows the magnitude of international money laundering. The International Monetary Fund (IMF) has estimated that the scale of global money laundering accounts for two to five percent of global gross domestic product (GDP), which surpassed $100 trillion in 2022. In short, the scale of today's money laundering around the world is approximately $2 trillion to $5 trillion. Some experts believe the total is far higher depending what is included in the count including monies related to global illicit economies and corruption. For example, the above estimates do not include underground financial systems. Tax evasion and capital flight are also not included – although in some countries they are considered a predicate offense for money laundering. Nor does the total amount of suspect funds include the tens of trillions of dollars of unproductive wealth hidden in offshore secrecy havens.

Worldwide anti-money laundering (AML) norms were established in the late 1980s, promulgated primarily by the Financial Action Task Force (FATF). They have changed little over the years. Today, governments and law enforcement still rely primarily on financial intelligence to follow the dirty money trails. For example, in fiscal year 2022, Treasury's Financial Crimes Enforcement Network (FinCEN), the U.S. Financial Intelligence Unit (FIU), collected over 24 million pieces of financial intelligence including 4.3 million suspicious activity reports (SARs).[17] Globally, these numbers are multiplied untold times. In 2024, 174 countries are members of the Egmont Group of Financial Intelligence Units. Each FIU collects, warehouses, analyzes, regulates and disseminates financial intelligence to help law enforcement follow the money and value trails.

Unfortunately, decades of experience proves that our AML efforts are costly, inefficient and, on the whole, not very effective given the scale of the challenge and trillions of dollars laundered every year. Our current AML safeguards were designed during the drug wars of the 1980s where large amounts of dirty money were sloshing around through the Western financial system.

Our AML countermeasures have not kept up with the ever-changing nature of transnational crime. The bottom-line metrics that matter in measuring AML effectiveness are the amount of illegal proceeds recovered and forfeited and by the number of money laundering convictions. Out of the approximately $4 trillion dollars that are laundered every year, how much of the proceeds of crime are actually seized and forfeited? According to the UNODC, the answer is less than one percent or less than $40 billion annually worldwide.[18]

The amount of government mandated fines and penalties for AML compliance are comparatively minimal. The numbers vary, but in the United States penalties total a few billion dollars a year including recent $3.1B fine against the Canadian TD Bank for laundering funds for the Mexican cartels and Chinese criminal syndicates.[19] Adding insult to injury, most of the large fines imposed on banks get passed on to shareholders and probably claimed as a tax deduction. Not only that, the bank executives behind the schemes are often never prosecuted.

In addition to forfeitures, the other bottom-line metric that matters is the number of successful investigations, prosecutions, and convictions. While statistics of this nature vary markedly from country to country, are open to question, and sometimes do not include the money laundering activities of criminals convicted on other

charges, the sobering fact is given the magnitude of international money laundering, for a money launderer to be caught and convicted he or she has to be either very stupid (unsophisticated) or very unlucky.

Enforcement costs are staggering. For example, a 2024 study of annual AML compliance costs by industry totals $61 billion in the United States and Canada alone.[20] This is in addition to the tens of billions of dollars other governments and the financial services industry around the world pay annually to combat financial crimes.

As Raymond Baker, a longtime financial crime expert and the Founding President of Global Financial Integrity (GFI) has stated, "Total failure is just a decimal point away." In other words, the international community has failed to effectively combat money laundering around the world.

Suffice it to say that financial crimes investigations of all sorts are very challenging. The reasons for failure are many. Here are a few:

- The breadth and scale of dirty money being laundered globally is simply stunning.
- The lack of political will to investigate money laundering and corruption.
- There is a dearth of skilled anti-money laundering enforcement.
- Venue and jurisdiction are obstacles that are often difficult to overcome – particularly in international investigations.
- Criminals and criminal organizations are not encumbered by borders. Governments are.
- Criminals are attracted to weak links; i.e. those countries with weak rule of law and/or those that are havens for criminality or that do not cooperate in international investigations.
- Despite the massive amount of money spent on AML enforcement, it is still not enough.
- The proliferation of anonymous shell companies; beneficial ownership information is generally not transparent and still protected.

The metrics that matter and the inherent challenges of AML enforcement demonstrate we "are a decimal point away from total failure." A consensus is beginning to form among AML professionals that we should try radically new countermeasures to counter all forms of money laundering and the growing novel methodologies related to underground banking. It is a dream by many involved in financial crimes enforcement to be able to have some type of a "silver bullet" or a straight forward and effective solution for following illicit money trails.

In money laundering and other financial crimes, "cash is king." It is the most important means launderers have to ensure anonymity and finance further criminality. Depending on the model of CBDC and variables are involved, over time cash would assuredly be phased out. That development, coupled with the adoption of a fully integrated CBDC, would allow investigators for the first time to more fully follow a transparent "digital money trail."

Data on all types of financial transactions would be collected, stored, analyzed and disseminated. And, in contrast to cash, a CBDC could be designed to potentially

include a wealth of personal data, encapsulating transaction histories, user demographics, and behavioral patterns. Governments, working with Big Tech, would then link social scoring. Personal data could establish a link between counterparty identities and transactions. All of this goes hand-in-hand with government mandated digital identification.

Even without specific identity data, artificial Intelligence (AI) and other analytic tools can improve understanding of trends, patterns, and flows, and help law enforcement flag anomalies similar to the good practices in, for example, unraveling trade-based money laundering.

Depending on the model, the implementation of a U.S. CBDC might also enable novel national security capabilities. For example, sanctions enforcement could be more robust with new ways to freeze assets and track foreign investments in the United States.

Of course, criminals and terrorist financiers are inventive. They will assuredly find ways to work around CBDCs including trade-based value transfer and the classic, if not archaic, bartering of goods, values, and services. Black markets will always thrive. When law enforcement puts pressure on criminal operations, they use the expression "squeezing the balloon." With the adoption of CBDCs, the criminal balloon will surely pop up elsewhere – perhaps in unexpected ways. Nevertheless, criminal work-arounds should not be of sufficient scale to overcome all enforcement measures.

In short, one can argue that the adoption of an all-inclusive CBDC model could well be a "silver bullet" for governments to more effectively mitigate the global scale of money laundering, and be able to effectively control a wide variety of financial crimes including entrenched and heretofore unsolvable problems such as corruption, embezzlement, tax evasion, sanctions evasion, capital flight, and other illicit finance threats. Perhaps CBDCs will finally unlock the closed door of financial transparency and help investigators follow the hidden money trails. Of course, at this time, the above is only theoretical in the United States and other jurisdictions until some of the CBDC system come online in places where it is being implemented or piloted to have some data to analyze or case studies to review and make a preliminary assessment.

A Surprising Conclusion

"Give me control of a nation's money and I care not who makes the laws," is a quote generally attributed to German banker Mayer Amschel Rothschild. In the modern era, it captures the threat of authoritarian CBDCs. Even with limited retail, the creation of wholesale or hybrid CBDCs, no doubt with initial privacy "safeguards" used to sell CBDCs to the public, will undoubtedly begin an incremental move by many governments toward complete control of money and the global financial system. Authoritarian CBDCs, coupled with digital identification, social scoring, and a prohibition of anonymous cash, may also enable total financial surveillance over the populace. How will this CBDC model evolve over time or fit in today's digital world? In many Western democracies, personal freedoms are under multi-front attack. The past few years have seen signs of creeping totalitarianism and Big State control. During the COVID years, there was worrisome collusion between Big Tech and governments. Some countries have already implemented mandatory digital identification. When AI search and filter capability is merged with facial recognition and government metadata containing citizens' very personal identifiable information and all of this is enhanced by fractal computing power, the results should concern all that cherish civil liberties. It's only a matter of time before a power-hungry regime or government takes power and merges a CBDC with the above technological capabilities. As in the current designs of the China/authoritarian model, there will be near total control.

Even if a country adopts and implements a version of a CBDC that is not initially authoritarian in nature, when future governments feel threatened by foreign or domestic enemies, weaponize institutions or agencies, or want to oppress their real or perceived internal political foes, the temptation to move to an authoritarian CBDC might be too much to resist. It might not occur all at once, but the rules of bureaucracy make clear that there will be a slow but steady expansion.

So, despite the above promise of CBDCs, particularly in the area of financial crimes enforcement, it may be foreseeable that that a CBDC, at least for the United States, is simply not viable at this point in time based on current political sentiments. Moreover, associated civil liberties and personal privacy considerations will first have to be addressed. In the United States, there would also have to be a consensus and law that fiat currency or the paper dollar will not be completely replaced by any form of a CBDC. Internationally, this is also a contentious issue. For example, in December 2024, President-elect Trump threatened the BRICS countries, which has India, Russia and China as its key members, with "100 per cent tariffs" if it moved to create a new currency that would challenge the dollar's domination in world trade. Geopolitical issues could negate the promise of a theoretical "silver bullet" that law enforcement could use to fight entrenched forms of financial crimes.

Wholesale, retail, and hybrid CBDC models by themselves may be more feasible in the short term – although nobody has demonstrated a compelling need for them. But again, an all-inclusive CBDC based on the authoritarian model would inexorably become a financial Big Brother or FIU on steroids.

China is exporting its model of control to totalitarian regimes to other countries including Iran, Cuba, and Venezuela. In fact, China is marketing its police state surveillance systems around the world.[21] Russia's Vladimir Putin has harnessed digital authoritarianism to track, censor, and control the population, building what some call a "cyber gulag."[22]

Authoritarian regimes also believe that CBDCs, and by extension new currency federations, will further weaken the dollar, be an effective countermeasure to sanctions, and help do away with non-government backed cryptocurrencies such as Bitcoin that they are not able to control. A future financial alliance of authoritarian CBDCs could undermine the strength of the U.S. dollar abroad and open workarounds to established financial channels, or collude for nefarious purposes to blackmail other markets to adopt anti-democratic policies.

But it is very possible that the authoritarian CBDC model will solely be realized beyond despotic regimes. Many communities are already advocating for the adoption of more control. The United Nations is urging a "digital future" to include the adoption of "digital IDs linked with bank or mobile money accounts.[23] The IMF is promoting a comprehensive a worldwide CBDC platform.

Some central bank officials have tried to make the point that a CBDC would only exist alongside cash. The Federal Reserve has said it "is considering a CBDC as a means to expand safe payment options [like cash], not to reduce or replace them." The European Central Bank has said, "A digital euro would complement cash, not replace it." And the Bank of England has said a CBDC "would not replace cash."[24] However, it should be noted that central banks have often pointed to the decline of cash as a reason to create a CBDC.

Despite the inexorable multi-lateral push promoting CBDCs, upon careful reflection, some governments have simply tabled or shelved any proposed CBDC initiative. In 2024, officials from Canada's central bank said that their digital currency, or electronic "Loonie," will no longer be considered after years of investigating bringing one to market. Studies in Canada have revealed the move was very unpopular with the majority of Canadians. Privacy concerns were the primary stumbling block. Perhaps one reason for the turnaround is Canadian Prime Minister Justin Trudeau' actions in 2022 invoking the Emergencies Act to crack down on anti-vaccine mandate protesters by freezing their bank accounts – a first step towards the "demonetization" of political enemies that many civil libertarians fear. In 2024, Australia and Colombia have also halted plans to launch their respective CBDCs.

Norway and Sweden, benefiting from excellent high-speed internet coverage, high digital literacy rates, and fast-growing fintech industries have been on a fast track to a future without cash. Due to recent fears that fully digital payment systems and would leave them vulnerable to Russian security threats, both countries are now rethinking their moves towards cashless societies.[25]

As the above examples indicate, countries and confederations will continue to develop and implement models of CBDCs based on their own unique needs and national interests. However, the current trajectory may well be that an increasing

number of countries will follow the lead of Canada, Australia and Colombia and after a period of reflection, decide that CBDCs are not worth the risks.

So where will the United States ultimately end up in the current international CBDC policy environment? As noted above, there are strong signals in the United States against its adoption. Additionally, some warning signs have arisen over the last few years in the private sector that warrant some introspection. For example, some major U.S. financial institutions have "debanked" both individuals and institutions with whom they disagree, whether politically or religiously, and where access to financial services was denied.[26]

In summary, despite the global push towards the development and adoption of CBDCs and the promise they represent for law enforcement to finally have an effective countermeasure to entrenched forms of financial crimes, it will be revealing on where the United States ultimately arrives on any policies on whether to adopt or not a "digital currency" or a compulsory "digital ID" system.

The conversation will involve financial efficiency and technology considerations. But in the end, the decisive factors will be about a need to balance convenience with absolute government control. In the end, do societies acquiesce to the reign of a creeping authoritarianism CBDC model and potential threats to privacy and civil liberties; or do the potential gains and benefits of digital currencies outweigh a more intrusive approach with enormous market risks and more limited freedoms?

Do societies acquiesce to the reign of a creeping authoritarianism CBDC model and potential threats to privacy and civil liberties; or do the potential gains and benefits of digital currencies outweigh a more intrusive approach with enormous market risks and more limited freedoms?

1 IRS, "Digital Assets", accessed at: h4ps://www.irs.gov/businesses/small-businesses-self-employed/digital-assets#:~:text=A%20digital%20asset%20is%20stored,Infrastructure%20Investment%20and%20Jobs%20Act)./

2 "Combatting the Illicit Use of Digital Assets," The United States Secret Service; https://www.secretservice.gov/investigations/digitalassets

3 "What is cryptography," IBM; https://www.ibm.com/topics/cryptography

4 John Cassara, David Luna, Dr. Layla M. Hashemi, "E-Commerce and Digital Marketplaces: The Booming Business of Cross Border Transaction Laundering," International Coalition Against Illicit Economies, September 2024; https://icaie.com/wp-content/uploads/2024/09/ICAIE-Policy-Report- September-2024%E2%80%93%E2%80%93Compressed-FINAL.pdf

5 "Central Bank Digital Currency," U.S. Federal Reserve; https://www.federalreserve.gov/cbdc-faqs.htm

6 h4ps://www.federalreserve.gov/faqs/what-is-a-central-bank-digital-currency.htm

7 Atlantic Council Geoeconomic Center, Central Bank Digital Tracker; https://www.atlanticcouncil.org/cbdctracker/

8 Manu Iyer, Muralikrishnan Puthanveedu, and Sid Zalaki, "Central Bank Digital Currencies; What's really in them for the Banks?", October 25, 2024, accessible at: https://www.thoughtworks.com/en-us/insights/articles/central-bank-digital-currencies.

9 "FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets," March 9, 2022; https:// www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible- innovation-in-digital-assets/

10 https://www.bis.org/about/bisih/topics/fmis/agora.htm.

11 Assad Jafri, "Congress passes bill banning Federal Reserve from creating a CBDC," Cryptostate, May 23, 2024; https://cryptoslate.com/congress-passes-bill-banning-federal-reserve-from-creating-a-cbdc/

12 Nicholas Anthony, "Where Trump and Biden Stand on CBDCs," Cato Institute, February 1, 2024; https://www.cato.org/blog/where-trump-biden- stand-cbdcs

13 Central Bank Digital Currencies, BIS, August 31, 2023; https://www.bis.org/fsi/fsisummaries/cbdcs.htm

14 Atlantic Council's Central Bank Digital Tracker

15 Kimberly Long, "China opens QR payments for tourists, but pushes citizens towards CBDC," The Banker, October 2, 2024; https:// www.thebanker.com/China-opens-QR-payments-for-tourists-but-pushes-citizens-towards-CBDC-1729754744

16 John Cassara, "China – Specified Unlawful Activities: CCP/Inc., Transnational Crime and Money Laundering," Kindle Direct Publishing, 2023

17 FinCEN Year in Review for FY 2022; https://www.fincen.gov/sites/default/files/shared/FinCEN_Infographic_Public_2023_April_21_FINAL.pdf

18 John Cassara, "Modernizing AML Laws to Combat Money Laundering and Terrorist Financing," Testimony to the United States Senate Judiciary Committee, November 28, 2017; https://www.judiciary.senate.gov/imo/media/doc/Cassara%20Testimony.pdf See also, John Cassara, "Money Laundering and Illicit Financial Flows," Chapter 2 – Sobering Statistics, Kindle Direct Publishing, 2020.

19 International Consortium of Investigative Journalists (ICIJ). "TD Bank Hit with $3B Penalty in U.S. Money Laundering Settlement". October 18, 2024. https://www.icij.org/investigations/fincen-files/td-bank-hit-with-3b-penalty-in-u-s-money-laundering-settlement/.

20 "Study Reveals Annual Cost of Financial Crime Compliance totals $61 billion in the United States and Canada," LexisNexis, February, 21, 2024; https://risk.lexisnexis.com/about-us/press-room/press-release/20240221-true-cost-of-compliance-us-ca

21 Angeline Tan, Chinese firms show off latest police-state surveillance tech at security expo, Life Site, September 27, 2024; https:// www.lifesitenews.com/news/chinese-firms-show-off-latest-police-state-surveillance-tech-at-security-expo/?utm_source=most_recent&utm_campaign=usa

22 Dasha Litvinova, "The cyber gulag: How Russia tracks, censors and controls its citizens," AP, May 23, 2023; https://apnews.com/article/russia-crackdown-surveillance-censorship-war-ukraine-internet-dab3663774feb666d6d0025bcd082fba

23 Emily Mangiaracina, LifeSite," UN proposes bank-linked digital IDs in 'Global Digital Compact'", June 22, 2023; https://www.lifesitenews.com/ news/un-proposes-bank-linked-digital-ids-in-global-digital-compact-plan/?utm_source=top_news&utm_campaign=usa1

24 Nicholas Anthony, "Will CBDCs Mark the End of Cash?" Cato Institute; https://theeconomicstandard.com/will-cbdcs-mark-the-end-of-cash/

25 Miranda Bryant, "Sweden and Norway rethink cashless society plans over Russia security fears," The Guardian, October 20, 2024; https:// www.theguardian.com/world/2024/oct/30/sweden-and-norway-rethink-cashless-society-plans-over-russia-security-fears

26 Susan Quinn, "Banks Escalate Punishment on Conservative Organizations," American Thinker, October 22, 2024; https:// www.americanthinker.com/blog/2024/10/banks_escalate_punishment_on_conservative_organizations.html

The **International Coalition Against Illicit Economies (ICAIE)** is a national security-centric NGO based in Washington DC that brings together committed champions across sectors and communities, including former members of the public sector, companies and prominent organizations from the private sector and civil society to mobilize collective action to combat cross-border illicit threats. ICAIE advances innovative energies through public-private partnerships, policy dialogues, and transformative threat intelligence and risk management solutions to counter illicit economies.

With an eye towards full-spectrum investigations, our ICAIE team bridges the gap between private industries and the government public sector. ICAIE Labs generate deeper investigation and supports judicial action. We leverage communications, financial, geospatial, artificial intelligence, federated learning, and other advanced analytics and technologies to investigate suspicious behavior and map networks. Ultimately, we use counter threat network operations to provide actionable intelligence, forensics, and enhanced security across the globe

John Cassara, an ICAIE Senior Advisor, is a retired federal government intelligence and law enforcement officer with a 26-year career. He is considered an expert in anti-money laundering and terrorist financing, with particular expertise in the areas of money laundering in the Middle East and the growing threat of alternative remittance systems and forms of trade-based money laundering and value transfer. He invented the concept of international "Trade Transparency Units," an innovative countermeasure to entrenched forms of trade-based money laundering and terrorist financing.

A large part of his career was spent overseas. John is one of the very few to have been both a clandestine operations officer in the U.S. intelligence community and a Special Agent for the Department of Treasury. His last position was as a Special Agent detailee to the Department of Treasury's Office of Terrorism Finance and Financial Intelligence (TFI). His parent Treasury agency was the Financial Crimes Enforcement Network (FinCEN), the U.S. Financial Intelligence Unit (FIU). He worked at FinCEN from 1996-2002. From 2002-2004, John was detailed to the U.S. Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) Anti-Money Laundering Section to help coordinate U.S. interagency international antiterrorist finance training and technical assistance efforts

Since his retirement, he has lectured in the United States and around the world on a variety transnational crime issues. John has consulted for government and industry. He has testified seven times before Congressional committees on matters dealing with money laundering, threat finance, and transnational crime. John is on the Board of Directors of Global Financial Integrity (GFI) and the International Coalition Against Illicit Economies (ICAIE). He is a fellow at George Mason University's Terrorism, Transnational Crime and Corruption Center (TraCCC). John has authored or co-authored several articles and books.

David M. Luna is the Founder and Executive Director of the International Coalition Against Illicit Economies (ICAIE) working across sectors to advance public-private partnerships to tackle hubs of illicit and threat convergence vectors around the world. A former US diplomat and national security official, David is a globally-recognized strategic thought leader, advocate for security of humanity, and a leading voice internationally on cross-border security threats, international affairs, geopolitical risks, illicit trade, organized crime, terrorism, threat finance, and illicit economies ("dark side of globalization") that fuel greater insecurity and instability around the globe.

David held numerous senior positions with the U.S. Department of State, Bureau of International Narcotics and Law Enforcement Affairs (INL), including directorships for national security, transnational crime, and anti-corruption and good governance; and advisor to the Secretary's Coordinator for the Rule of Law. David also served as an Assistant Counsel to the President, Office of the Counsel to the President, The White House; and other positions with the U.S. Department of Labor and U.S. Senate. David is currently the Chair of the Business at OECD Anti-Illicit Trade Expert Group (AITEG); Chair of the Anti-Illicit Trade Committee (AITC), United States Council for International Business (USCIB); Chair of the Peace & Security Committee, United Nations Association of the USA – National Capitol Area (UNA-NCA); Member of the Business Twenty (B20/G20); Advisory Council Member, Transparency International US, and Chair of a Summit for Democracy (S4D) Kleptocracy and Illicit Finance Working Group.

David is a Senior Fellow for National Security and Founder/co-Director of the Anti-Illicit Trade Institute (AITI) at the Terrorism, Transnational Crime, and Corruption Center (TraCCC), Schar School of Policy and Government, George Mason University. David is a graduate (M.S.S.) of the U.S. Army War College, and received his B.A. from the University of Pennsylvania, J.D. from The Columbus School of Law, The Catholic University of America, and awarded numerous certificates from the Harvard Business School (HBS).

ICAIE

INTERNATIONAL COALITION
AGAINST ILLICIT ECONOMIES

ICAIE.COM