GARP
GRI | Risk Institute

CRYPTOCURRENCIES, STABLECOINS AND CBDCs:

A Primer for Risk Managers

By Mark Carey,
Co-President, GARP Risk Institute

Risk managers must be attentive to the risks associated with digital currencies. What are the forms of these virtual currencies? What gives them value and how do transactions in the instruments work? What specific risks do they pose to financial institutions, non-financial firms, and investors?

All of these issues are addressed in this primer. The risks of these virtual assets are assessed, and background is provided about, among other things, their usefulness as investments and for conducting transactions.

Distributed ledger technology (e.g., blockchain) is not discussed in detail, because distributed ledgers have many applications beyond digital currencies. Similarly, while many parts of the digital currency ecosystem, such as custodians and exchanges, receive some attention, this primer does not systematically discuss the risks specific to every part of the ecosystem.

What is Included in "Digital Currency?"

In this primer, "digital currency" includes cryptocurrencies, stablecoins, and central bank digital currencies (CBDCs).

A typical cryptocurrency is a form of money for which transactions can be cleared with no trusted third party standing between payor and payee. It's designed to ensure that the payor has the funds, and that each transaction is completed. The most widely known cryptocurrency is Bitcoin.*

For most cryptocurrencies, a transaction record is an entry in a blockchain, which records that a cryptocurrency amount was transferred from payor to payee. Sometimes other things are recorded as well; for example, the blockchain for the Ethereum cryptocurrency can embed "smart contracts" that take actions when specified conditions are met. Although distributed ledgers and trustless transfer are innovations, they alone do not make a cryptocurrency a good form of money or a good investment.

A stablecoin is a cryptocurrency that is backed by assets that have independent value, such as gold or U.S. dollars. Tether is an example. The backers of a stablecoin often promise to convert the stablecoin into the backing assets, just as the U.S. government converted dollars into gold many years ago.

The most commonly discussed stablecoin does not yet exist. Originally called Libra but now known as Diem, this Facebook-led stablecoin project is having difficulty launching.

A central bank digital currency is not a cryptocurrency. Rather, it is central bank money that private parties can use to transact. (In most countries, apart from currency, central bank money can be used for transactions only among financial institutions. Most private transactions involve commercial banks at some point and use commercial bank money.) For example, a CBDC created by the Federal Reserve would be a form of U.S. dollars.

The design details of CBDCs may vary; two parties might have to use a commercial bank to, say, implement their CBDC transaction – or the whole transaction might occur across the central bank's books with no commercial bank involved. Few CBDCs currently exist, but many central banks are developing them.

Functional Purposes

HOW CRYPTOCURRENCIES WORK

Bitcoin is the cryptocurrency with the largest total value outstanding, and is used as the basis of explanations of cryptocurrency in this primer. It is a

* A detailed description of Bitcoin and its ecosystem can be found at https://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/

fiat* currency, meaning it is not linked to anything with intrinsic value and is not legal tender in just about every country. (El Salvador, which recently adopted Bitcoin as legal tender, is one exception.) Bitcoin therefore has value only where individuals and firms choose to accept it in exchange for other things (such as dollars).

The number of Bitcoins is growing slowly and cannot exceed about 21 million. With nearly fixed supply, Bitcoin's value may increase over time if demand for it grows, but its value may also go to zero at any time if individuals and firms stop accepting it in exchange for goods and services or other forms of money.

Any money is fiat money if not backed by other assets with intrinsic value.

In a Bitcoin transaction, the payor submits a transaction to the Bitcoin network using the payor's private ID ("private key"). The transaction record specifies the number of Bitcoins to transfer (which may be a fraction), the payor's public ID, the payee's public ID, and some other information.

The transaction is validated and transmitted throughout the Bitcoin network by many operators of Bitcoin "nodes." A Bitcoin "miner" aggregates several transactions into a "block," and then performs costly computations to gain the right to post the block to the Bitcoin distributed ledger, which is simply a compilation of all previous transactions.

Validation involves using the ledger's history to verify that the payor possesses the specified amount of Bitcoin and that all aspects of the transaction conform to the rules of Bitcoin. Crucial to the integrity of Bitcoin is that a miner will receive no value for blocks that contain an invalid transaction (and, thus, will have wasted their computational resources).

Operators of nodes that transmit invalid transactions are likely to be delinked from the network by other node operators, losing the informational advantages that accompany node operation. Consequently, payors are unable to spend more Bitcoin than they have previously received.

Node operators receive no fees, but miners receive both fees and newly-created Bitcoin for successful creation of a valid block. The cryptographic calculations performed by miners' computers are demanding and use large amounts of energy.**

No entity stands between the payor and payee in a transaction on the Bitcoin network, and the identity of both remains confidential. In other words, there are no Bitcoin "accounts" and participants are difficult to trace. This makes it a popular method of payment for those engaged in illicit activity. However, if a participant loses knowledge of his or her private key, that person's Bitcoin holdings cannot be accessed and are essentially lost.***

Many service providers have emerged to enable participants to operate in a more familiar account-based setup: some provide "wallets" that store the private ID, some verify a participant's identity, and others share that verification with the participant's permission - enabling organizations to comply with KYC/AML/ATF regulations.

---

* Many cryptocurrency devotees presume that national money is "fiat money" and that cryptocurrencies are something else. This is not the case. Any money is fiat money if not backed by other assets with intrinsic value, including cryptocurrencies. Stablecoins are not fiat money, except those backed by national fiat money (something backed only by fiat money must itself be fiat money).

** Bitcoin is a "crypto" currency because two bits of cryptography are essential to integrity of the ledger: one bit links private and public IDs in a way that keeps the private ID confidential but validates it, and the other bit underlies the miners' computations. Miners' computations have no intrinsic value; they are mainly a way to ensure that miners bear significant costs, so that they have an incentive to record only valid transactions in the ledger.

*** Recently, perpetrators of the Colonial Pipeline ransomware attack in the U.S. received payment in Bitcoin, but law enforcement authorities were able to recover some of the payment. Though details of methods have not been publicized, this could only be done if the authorities gained knowledge of one or more private keys. This sometimes might be possible by tracking IP addresses from which transactions originated.

Meanwhile, other service providers offer derivative products (such as futures) and/or custodial services. Still others provide interfaces that allow participants to trade Bitcoin without understanding the details of construction of a valid transaction; often, such providers are exchanges that permit Bitcoin to be exchanged for other digital currencies or national money.

Combined, the ecosystem of service providers has grown to the point that some nonfinancial firms and financial institutions are willing to participate in transactions or to offer digital-currency-related products such as cryptocurrency investment funds. Interestingly, more Bitcoin transactions occur on platforms of service providers than on Bitcoin's native network. (Service providers can net transactions that occur within their ecosystem.)

It is worth noting that cryptocurrencies generally do not provide protection against inflation. Nothing links their value to a basket of goods and services, and the value of many cryptocurrencies fluctuates a lot.

HOW STABLECOINS WORK

A stablecoin differs from a cryptocurrency in that a sponsoring entity has implied it will link the value of the stablecoin to some other valuable asset, via matching issuance of the stablecoin to reserves of that asset. For example, Tether Limited has "promised" that if a client gives it dollars, euros, gold, or a few other assets, it will issue an equivalent value of Tether stablecoins, while holding the dollars (etc.) as reserves.

Tether Limited has implied (but not made ironclad legal commitments) that it will redeem stablecoins on demand and return the valuable asset to the redeemer. Tether, which does not operate in the U.S., has no native network or blockchain of its own. Transactions are conducted largely on either "Omni" (a special part of the Bitcoin blockchain in which new assets can be created) or on the Ethereum blockchain.

Most stablecoin sponsors are unregulated. There have been instances of fraud at some, and some have been criticized for their management of reserves. Tether, for its part, has been criticized for holding a large fraction of reserves in commercial paper – an asset that would become illiquid in the event of a run and would therefore not support Tether Limited's ability to redeem its stablecoins.

HOW CBDCs WORK

Central banks that create CBDCs make design decisions, just as they made design decisions in creating their traditional payment networks. For example, a central bank might decide that it will clear all transactions in its CBDC and that it will maintain accounts for all holders of its CBDC, taking commercial banks out of the loop.

Alternatively, a central bank might decide that the transactions of nonbank private parties will be cleared by commercial banks (or some other set of financial institutions), with the commercial banks clearing interbank transactions at the central bank – much as the U.S. payments system works today.

Both clearing and verification of payors' balances might be immediate or done periodically. The anonymity of payors and payees might be protected to some extent, but, because CBDCs are likely to be account-based, the central bank is likely to be able to learn the identity of participants.

Design decisions interact with each other and are likely to influence the willingness of different types of actors to use the CBDC. There is no danger that the value of a CBDC will go to zero, as long as the national money has value. However, because a CBDC's value is locked to the value of its national money, it will be affected by inflation.

Infrastructure

As noted previously, many cryptocurrencies and stablecoins have an infrastructure of service providers, including:

- Exchanges and other organizations that stand ready to buy, sell or trade cryptocurrencies or stablecoins, to settle trades, and to exchange cryptocurrencies or stablecoins for national money such as dollars;
- Payment service providers that help nonfinancial firms accept cryptocurrencies and stablecoins in exchange for goods and services;
- Custodians that "store" cryptocurrencies or stablecoins (as a practical matter, this means either keeping track of the user's private key or commingling the user's holdings with those of other users, while maintaining accounts recording who owns what);
- Identity verification services that permit institutional clients to comply with KYC/AML/ATF and similar regulations; and
- Providers of derivative contracts, such as Bitcoin futures, and associated exchanges and custodians.

Though the list above is not exhaustive, a large fraction of owners of cryptocurrencies and stablecoins use such service providers. Since such use negates the no-trusted-third-party feature of cryptocurrencies, an implication is that many users do not place a high value on that feature.

Moreover, because transactions that involve buyers and sellers both using the same service provider may be netted, it is not clear that such users place high value on blockchain records of their own transactions. (Individual transactions made through exchanges generally do not appear on the native Bitcoin blockchain.) Many users may view cryptocurrencies and stablecoins as an investment, rather than as a means of payment.

Risks Associated with Cryptocurrencies and Stablecoins

Risks associated with digital currencies can be separated into five broad categories: (1) risks borne by financial institutions that provide services related to digital currencies, most of which are risks familiar to financial risk managers – such as legal risk, third-party and counterparty risks (e.g., failures of infrastructure), and loss of liquidity in periods of stress; (2) investment risk, meaning risk of loss of value of the digital currency itself, which is borne by any investor in digital currencies; (3) other risks borne by investors; (4) risks borne by nonfinancial firms; and (5) loss of a financial institution's or nonfinancial firm's investment in its capacity to do business related to digital currencies.

Risks associated with CBDCs, which are mainly borne by central banks, are also briefly discussed in this section.

RISKS TO FINANCIAL INSTITUTIONS

Financial services firms that offer crypto-related products, such as investment managers that provide clients with ways to include cryptocurrencies or stablecoins in their portfolios, bear the following risks:

REPUTATIONAL

If the value of a firm's crypto investments falls to low levels or if publicity is bad (for example, if key service providers are participants in market manipulation), its reputation may be damaged. Though this risk is familiar, given the lack of familiarity of many clients with crypto, it would be wise for financial firms to be particularly clear and comprehensive about such risks in pre-investment disclosures.

THIRD-PARTY

Service providers can potentially engage in theft or fraud – or might simply fail to function. Indeed, many service providers are relatively new and unregulated, so the risk of provider failures is material. Moreover, standards for providers are lacking.

Most financial firms are likely to use service providers (such as exchanges and custodians), both to limit their own expenditures on infrastructure and to support insurance coverage of losses associated with provider failures. This requires that the providers be recognized by insurers as reliable enough to support insurance. To manage the risk of provider failures, financial institutions should have a dialog with insurers when selecting service providers – and should buy appropriate insurance.

LEGAL

Some jurisdictions might choose to make cryptocurrencies illegal. Although a financial firm might seek to avoid this risk by investing only in instruments linked to cryptocurrencies (like futures), such instruments may also be subject to changes in legal status – potentially exposing a financial institution not only to legal risk but also to reputation losses.

Similarly, the regulatory status of ETFs and other crypto products might change in a way that would make them unusable by some financial institutions. These risks can be managed to some extent by informing clients that cryptocurrency-related products will be wound up if legal or regulatory status changes.

REGULATORY

Regulatory costs and restrictions may change. Most jurisdictions remain uncertain about whether and how they will regulate cryptocurrencies and related activities. When they decide, it is likely that regulatory costs will increase at financial firms that provide cryptocurrency-related products and services.

COMPLIANCE

Relatedly, financial firms must be careful to comply with host-country expectations connected to know-your-customer, anti-money-laundering, anti-terrorist-financing, and similar matters. Expectations may go beyond regulatory minimums, given the widely-held view that many illicit actors use cryptocurrencies.

Though it might appear that risks of failing to comply would be minimized by using only derivatives, pressure might nonetheless be applied. Dealers and exchanges providing the derivative products might have their business models disrupted by changes in expectations, with knock-on effects on their clients.

CYBER

Cyber risk is a constant threat to financial institutions, but variants are particularly important for cryptocurrency-related products. If a financial firm offers products that involve direct investments in cryptocurrencies (or invests for its own account), security of the private key is critical. If hackers are able to access private keys, then value will be lost and will be unrecoverable.

Relatedly, if service providers or custodians are used, audits of their cybersecurity – and careful scrutiny of their ability to compensate the firm for cyber-related losses – is important. Such losses might be large enough to cause service providers to fail.

EVENT DISRUPTIONS

The value of some cryptocurrencies can be disrupted by events such as forks or civil wars. For example, in the recent past, Bitcoin split into two types (a "fork"), because of a disagreement about the validity of particular transactions. If a financial firm finds its portfolio is affected by such events, exiting its positions may be difficult and may require rapid action.

MARK-TO-MARKET

Marking portfolios to market might become difficult if cryptocurrencies become illiquid, even temporarily. This is a familiar risk for many asset classes, such as real estate, but it is important that clients be informed at the time they invest and that clients understand the game plan in such an event.

REPORTING

Failure to comply with tax reporting requirements regarding client capital gains and losses may lead to fines and other penalties.

LIQUIDITY

Illiquidity is a major risk, particularly for stablecoins. Should the sponsor of a stablecoin lose credibility, a run on the stablecoin is likely, trading liquidity is likely to disappear, and investors may be unable to convert to the backing asset. In such circumstances, clients with investments in stablecoins are also likely to run.

This risk is extremely difficult to manage because the exchange rates between cryptocurrencies, stablecoins, and national currencies are likely to change rapidly during a run and liquid reserves of national-currency assets may provide only limited ability to meet client requests for redemptions. Moreover, unlike national money, there is little hope of support from central banks or national governments in the case of a run on cryptocurrencies or stablecoins.

Overall, the risks of digital currencies to financial institutions are manageable, but require unusually clear and complete communications between firms and clients. Financial services firms, moreover, must be prepared to react to realizations of digital currency risks quickly and effectively.

Investment Risks

A firm or individual that includes cryptocurrencies or stablecoins in its portfolio obviously loses if the value of such instruments falls a lot. This is normal investment risk, but the novelty of the instruments makes assessment of such risk more challenging than in the case of conventional assets.

Moreover, expected returns are difficult to estimate, so the risk-return tradeoff is difficult to evaluate. Past performance is not necessarily a reliable guide to the future.

CRYPTOCURRENCIES

Cryptocurrencies have no fundamental value, and therefore could drop to zero at any time. Let's now examine four factors that have sustained their value to date:

1. Some people and firms attach a positive probability to one or more cryptocurrencies substantially replacing national money in transactions. Cryptocurrencies are currently not widely used in transactions, but - since anything that is a preferred medium of exchange has fundamental value - there is some belief that they will eventually become widely used.

Cryptocurrencies have no fundamental value, and therefore could drop to zero at any time.

However, a major barrier to replacement of national money is that cryptocurrencies are usually a more expensive means of conducting a transaction than most national currencies (taking together the costs borne by both parties to the transaction). Consequently, there is little incentive for most private parties to use cryptocurrencies.

If costs of cryptocurrency transactions do not fall substantially, eventually claims that cryptocurrencies will replace national money will lose credibility and this source of value will be much weaker – at least in nations with well-functioning monetary and financial systems. In other nations, where many residents feel that the national money does not serve their needs (e.g., Venezuela), cryptocurrencies might play an important role in payment systems.

2. Few nations have made cryptocurrency illegal as an investment or medium of exchange. However, if a large number of nations do so – and particularly

if they enforce legal restrictions – public use and the value of cryptocurrency are likely to fall precipitously. Moreover, most financial institutions and businesses are likely to view use of an illegal cryptocurrency as undesirable.

3. Some cryptocurrencies support illicit activity by allowing illicit actors to conceal their identify when transactions are conducted on the cryptocurrency's native network – i.e., without the aid of service providers like exchanges. As an example, the perpetrators of the May 2021 ransomware attack on the Colonial petrochemical pipeline in the United States demanded payment in Bitcoin.

   This source of value of cryptocurrencies is not likely to disappear. However, illicit actors may find cryptocurrency less valuable in the future if legitimate actors become less willing to exchange goods and services for cryptocurrency. Under that scenario, illicit actors will have more difficulty converting their cryptocurrency into other forms of money or into goods and services.

4. Some people have an aversion to national money, which is often associated with anti-government views. Such people may prefer to use cryptocurrencies in transactions, even if doing to is more expensive than use of national money. The fraction of the population in this category is unlikely to fall to zero.

STABLECOINS

The appeal of stablecoins is that their value fluctuates much less than cryptocurrency values. However, a stablecoin's value can easily go to zero, if the entities operating the backing mechanism lose credibility.

For example, if owners of a stablecoin believe that its sponsor does not actually possess the assets that back it, they will run to the sponsor en masse and request conversion of the stablecoin into the backing asset. This almost surely will cause the sponsor to fail and the value of the stablecoin to drop to zero.

Regulation can reduce the likelihood of such situations, but only if the regulator is credible. Complicating matters further, stablecoin sponsors are generally unregulated. Tether Limited, for example, does not operate in the United States and nominally will not do business with U.S. entities. Moreover, Tether's legal documents are worded in a way that makes ambiguous the firmness of its commitment to convert Tether coins into backing assets.

Other Risks to Investors

Aside from valuation risk, investors in cryptocurrencies and stablecoins should also be aware of several other potential hazards.

The tax status of cryptocurrencies, for example, might change. Currently in the United States, they are property, not money, and thus subject to capital gains tax treatment. Service providers often are expected to report transactions to tax authorities.

U.S. investors, meanwhile, bear compliance risks related to reporting of overseas holdings, accounts, and transactions. Reporting requirements are not always clear, because many cryptocurrencies are not tied to any jurisdiction – and stablecoins have such ties only if the home country of the sponsor is used as the nationality of the stablecoin. Moreover, if a service provider operates outside the home country of a stablecoin investor, it may offer little support – partly because it may be unfamiliar with the stablecoin's country-specific requirements.

Ownership of cryptocurrencies is also unenforceable in court, so an investor has no recourse if their cryptocurrency or stablecoins are stolen or lost. Similarly, an investor typically has no legal recourse if transactions are completed on terms that differ from those to which they agreed.

Lastly, poor-quality information about many qualities of cryptocurrencies and stablecoins complicates an investor's task of optimizing its investments. For example, much volume on cryptocurrency exchanges is reportedly not between arm-length parties, and transaction volumes therefore are reportedly overstated.

Overall, these risks imply that investors must be very attentive to operational details and to changes in law and regulation.

Risks to Nonfinancial Firms

Nonfinancial firms that accept cryptocurrency or stablecoins in payment for goods and services mainly bear four risks:

- **A sudden inability to convert into national currency**. This risk can be managed by retaining only small balances of cryptocurrency or stablecoins.

- **Legal exposure, if participating in transactions is declared illegal**. This risk is particularly material for firms operating in jurisdictions where the legal system is such that sanctions can be applied to behavior that occurred before it became illegal. Even where that is not possible, some damage to nonfinancial firm reputation may occur if legal status changes.

- **Failure to perform by service providers, such as cryptocurrency exchanges**. For example, if a payment service provider fails, balances that a firm had at the provider may be lost or inaccessible. This is no different than the situation with many national currency payment service providers, and can be managed similarly.

Accounting rules may be developed for cryptocurrencies and stablecoins that differ from current practice.

- **The potential revision of regulatory requirements related to reporting and registration**. For example, currently, a nonfinancial firm operating in the U.S. may accept cryptocurrencies and stablecoins in payment or use them to pay suppliers - with no registration and no reporting apart from tax-related reporting of any incidental capital gains and losses. But if requirements are instituted, nonfinancial firms will have to be aware of the changes and comply promptly.

  Similarly, accounting rules may be developed for cryptocurrencies and stablecoins that differ from current practice, which would affect both nonfinancial and financial firms. Today, accounting practices vary, mainly because uncertainty exists about proper accounting treatment of cryptocurrencies and stablecoins. For example, they are considered property, not money, so balances should not be reported as cash.

Overall, the risks for nonfinancial firms are routine for experienced risk managers.

Capacity to Do Business

Financial and non-financial firms that accept cryptocurrencies or stablecoins as a form of payment - or that offer related products or services - typically must make investments to be able to do so. If the willingness of clients to use or invest in cryptocurrencies or stablecoins wanes, such investments will produce a smaller return (or none). When such investments are large, this is a material risk.

At the time of investment decision-making for a digital currency, the rewards must be weighed against the potential risks.*

* Waiting to invest, which is almost always possible, reduces the popularity of cryptocurrencies and stablecoins at the margin. So, management of the risk of overinvestment in capacity tends to reduce the value of digital currencies.

Risks Associated with CBDCs

Since CBDCs are a form of national money, they are subject to different types of risks than the cryptocurrency and stablecoin hazards discussed previously.

The main risks that affect them differently than other forms of national money are cyber and system-failure risks that are somehow specific to the CBDC. Management of such risks is almost entirely the responsibility of central banks, not private financial institutions.

Central banks and national governments also bear the risk of underinvestment in CBDCs. Should CBDCs prove popular with the public and be easy to use across borders, it is possible that nations that lag in implementation of CBDCs might experience less demand for their national currency. Indeed, if individuals and firms were to migrate to the use of foreign CBDCs, this could influence the value of a nation's exchange rate, as well as its monetary policy.

Parting Thoughts

Many of the aforementioned risks are familiar to risk managers, because they are at least somewhat similar to those associated with other instruments or businesses. Other hazards – like risks to the continued existence of cryptocurrencies and stablecoins – are less familiar. As always, risk managers should be alert to the risks that affect their portfolios and businesses – and should develop new ways to manage such risks, as necessary.

ABOUT THE AUTHOR

Mark Carey is the co-president of the GARP Risk Institute. In this role, he helps lead research and thought leadership for GARP and the broader risk community.

Currently, he is also an editor of the Journal of Financial Services Research and a co-director of the National Bureau of Economic Research's Risks of Financial Institutions Working Group – a mixed group of academics and financial professionals that focuses on risk management.

Prior to joining GARP, he was associate director in the Division of International Finance at the Federal Reserve Board in Washington, D.C., leading some of the Fed's work on issues related to the financial services industry, systemic risk and the financial crisis. He has written many technical papers on credit risk and corporate finance.

GARP | Global Association of Risk Professionals

garp.org

ABOUT GARP | The Global Association of Risk Professionals is a non-partisan, not-for-profit membership organization focused on elevating the practice of risk management. GARP offers role-based risk certifications — the Financial Risk Manager (FRM®) and Energy Risk Professional (ERP®) — as well as the Sustainability and Climate Risk (SCR®) Certificate and on-going educational opportunities through Continuing Professional Development. Through the GARP Benchmarking Initiative and GARP Risk Institute, GARP sponsors research in risk management and promotes collaboration among practitioners, academics, and regulators.

Founded in 1996, governed by a Board of Trustees, GARP is headquartered in Jersey City, N.J., with offices in London, Washington, D.C., Beijing, and Hong Kong. Find more information on garp.org or follow GARP on LinkedIn, Facebook, and Twitter.

HEADQUARTERS
111 Town Square Place
14th Floor
Jersey City, New Jersey
07310 USA
+1 (201) 719.7210

LONDON
17 Devonshire Square
4th Floor
London, EC2M 4SQ UK
+44 (0) 20 7397.9630

WASHINGTON, D.C.
1001 19th Street North, #1200
Arlington, Virginia
22209 USA
+1 (703) 420.0920

BEIJING
1205E, Regus Excel Centre
No. 6, Wudinghou Road
Xicheng District,
Beijing 100011, China
+86 (010) 5661.7016

HONG KONG
The Center
99 Queen's Road Central
Office No. 5510
55th Floor
Central, Hong Kong SAR, China
+852 3168.1532