OLIVER WYMAN

CRYPTOCURRENCIES AND PUBLIC POLICY
KEY QUESTIONS AND ANSWERS

FEBRUARY 2018

AUTHORS

Douglas J. Elliott, Partner

Larissa de Lima, Engagement Manager

Ryan Singel, Associate

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

INTRODUCTION

Responding to the growth of "cryptocurrencies" has shot up the list of priorities for policymakers and regulators in recent months. Given the intense confusion surrounding this topic, we present here a primer that explores the topic from a public policy viewpoint, starting with the most basic points. We constructed this in Q&A format to make it easy to read and to jump to the points of greatest interest. It is intended for an intelligent non-specialist and therefore required a fair amount of simplification, for which we apologize to any technical experts who would have explained things differently.

TABLE OF CONTENTS

THE BASICS OF CRYPTOCURRENCIES

What is a cryptocurrency?

There is no one commonly accepted definition of cryptocurrencies and indeed observers differ even on whether a specific mechanism counts as a cryptocurrency. Bitcoin was the first and remains the best known example, designed to be a "peer-to-peer version of electronic cash,"[1] but there are many other examples described further below. The Bank for International Settlements (BIS) offers a broad definition of cryptocurrency as a means of payment with the following characteristics (reworded here for simplicity):[2]

- Electronic: Cryptocurrencies are stored and used in transactions digitally.
- Use of peer-to-peer (P2P) transactions: Cryptocurrencies can function like cash, in that any two people can transact directly with each other, but they differ from the typical electronic payments system, in which an intermediary financial institution facilitates the transaction.
- Not the liability of anyone: Cryptocurrencies are different from virtually all other paper or electronic money, which are obligations of the issuers. Conventional currency (also called "fiat currency") is money issued and owed by a government or central bank, while deposits, which are often treated as money, are issued and owed by financial institutions. Note that gold, when viewed as a currency, and to some extent coins, do not represent a liability of anyone either.

Please note that, other than in passing references, this report will not examine proposals for central bank-issued digital currencies, which are also sometimes referred to as cryptocurrencies. We focus solely on privately-issued cryptocurrencies, particularly those that are openly traded.

Why do cryptocurrencies exist?

There are now thousands of cryptocurrencies, with differing overall purposes and reasons for being. Broadly speaking, they fall into a few categories, based on the problems they tackle in their design. The design goals described below may not be exhaustive, as new cryptocurrencies are being created each week.

- **Digital cash coins** (such as Bitcoin, Monero and Bitcoin Cash): Provide a digital currency alternative to cash that is free from the control of a government or central bank and potentially offers greater anonymity than conventional payment systems. Multiple cryptocurrencies exist, as newer digital coins like Monero and Zcash focus more on privacy and build on lessons from Bitcoin. These cryptocurrencies may have different underlying technologies or even be built on a cryptocurrency platform like Ethereum, described below.

1 Satoshi Nakamoto, "A Peer-to-Peer Electronic Payment System," p. 1. Accessed January 30, 2018. https://bitcoin.org/bitcoin.pdf

2 Bank for International Settlements. Committee on Payments and Market Infrastructure. "Digital Currencies," November 2015. https://www.bis.org/cpmi/publ/d137.htm; Bank of International Settlements. Central Bank Cryptocurrencies. BIS Quarterly Review, September 2017. https://www.bis.org/publ/qtrpdf/r_qt1709f.pdf

- **Payment infrastructure tokens** (such as Ripple, Particl and, Utility Settlement Coin): Support a payment system for one or more conventional currencies at lower cost, higher speed, or with greater reliability. For example, Ripple has been designed to enable near-instant, bilateral transactions across currencies. Conventional currencies are traded for Ripple tokens in the execution of a payment transaction, and the token enables the protocol for the transaction to be executed efficiently. Another example is Utility Settlement Coin, currently in development by a consortium of banks to improve institutional payments.
- **Securities tokens** (such as RMG and Maecenas): Support peer-to-peer trading activity by creating a token that represents a unit of something of value, such as an ownership stake in a physical asset or fund. For example, Royal Mint Gold (RMG coin) represents ownership of a gram of gold, held by The London Bullion Market Association. Maecenas, for its part, plans on creating a tradable token that represents a stake in an art piece.
- **Utility tokens** (such as Filecoin, Golem and 0x): Support peer-to-peer trading to secure access to a specific good or service. For example, Filecoin plans to allow purchasing and selling of data storage while Golem plans on doing the same for computing power.
- **General platform tokens** (such as Ether and NEO): Support an underlying platform or protocol that can underpin the creation of new "apps" that take the principles of electronic decentralized peer-to-peer transactions and flex them beyond currency transactions. An example "app" could execute a transaction automatically, such as paying an insurance claim, if certain conditions are met and parties have signed a "smart contract." Apps can also include other cryptocurrencies. Ethereum is an example platform that allows developers to build their own decentralized applications. Ether, Ethereum's token, is both a tradeable cryptocurrency and used to value how much developers pay for running their applications on Ethereum.

For some of these categories, the designers could choose either to have the token circulate only within a limited group, such as the direct users, or could allow it to circulate in the public domain as conventional currencies do. For the purposes of this primer, we will only focus on those that allow wider circulation.

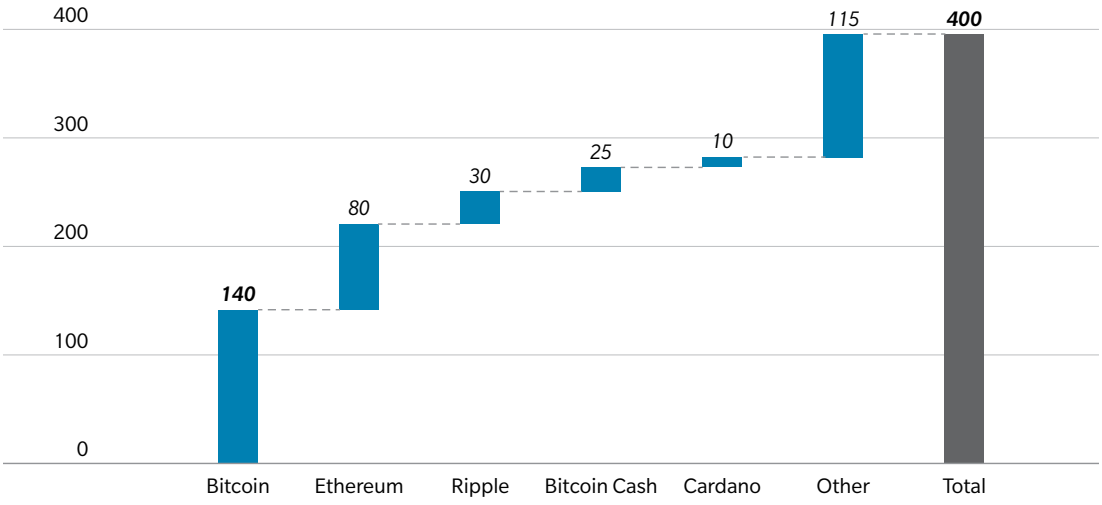
As this is an evolving space, the design goals of any given cryptocurrency may not exactly align with how people end up using cryptocurrencies.

How big is the cryptocurrency market?

It is difficult to know how big the cryptocurrency market is, as a result of the large number of such currencies, their very rapid growth, their extreme price volatility, market illiquidity, wide scope of market exchanges spread across the globe, and, sometimes, as a result of their privacy protection features.

The estimated cryptocurrency market capitalization during January 2018 varied between approximately $400 billion and $800 billion, with Bitcoin responsible for approximately 35% of market capitalization, followed by Ether with 20%, followed by more than a thousand other cryptocurrencies. In terms of transaction volumes, Bitcoin alone had more than 200,000 average daily transactions.[3]

EXHIBIT 1: MARKET CAP BY CRYPTOCURRENCY ($ BILLION, AS OF FEBRUARY 8, 2018)[4]



3 Accessed February 8, 2018, https://coinmarketcap.com/

4 Oliver Wyman analysis. Accessed February 8, 2018. https://coinmarketcap.com/

Why should policymakers care about cryptocurrencies?

Cryptocurrencies overlap with key parts of the global monetary and financial system. The rapid growth of cryptocurrencies demands that policymakers and regulators consider whether or how to fit them into their existing systems or revise those systems for the new world. Key questions for policymakers include the following, which are addressed in more detail in their own sections:

How could cryptocurrencies affect economic efficiency and growth?

Many cryptocurrencies are set up at least in part to make payments or other processes faster and more efficient. To what extent would these advantages improve the economy? Are there other effects that would increase the benefits or offset them? Are there alternative technologies that offer the same improvements with lower risks? The answers vary significantly with the specifics of the cryptocurrencies and their design and use.

What would be the potential impacts on financial stability if cryptocurrencies were adopted widely?

Cryptocurrencies could impact financial stability either directly, as payments and investments denominated in Bitcoin or other virtual currencies become sizable, or indirectly by changing the size, profitability, and stability of existing financial institutions and markets.

How might monetary policy be affected by cryptocurrencies?

Monetary policy primarily operates by affecting the amount of a nation's money and the interest rates charged in the economy for using that money. At the extreme, the more people use cryptocurrencies for their monetary needs, the less important a country's own money becomes, except for any secondary effects on cryptocurrencies. How much substitution will occur for conventional currencies? Would central banks be able to find alternative approaches to achieve their monetary policy objectives? How much would it matter if their monetary policy tools become less useful?

How could fiscal policy be affected by cryptocurrencies?

There are two first-order effects on fiscal policy. First, by decreasing a government's benefits from creating money instead of borrowing to make payments. Second, cryptocurrency transactions can generate tax revenue, which may be higher or lower than equivalent conventional transactions would produce. Looking beyond the tax rules themselves, some fear that cryptocurrencies could aid in tax evasion, reducing government revenues.

What are the options for taxing cryptocurrencies?

Depending on whether cryptocurrencies are viewed as currencies, investment assets, fixed assets, or something else, there are a variety of different potential tax treatments. The distributed nature of cryptocurrencies, without a central home, also challenges traditional frameworks that treat money earned domestically differently from foreign earnings.

To what extent may cryptocurrencies facilitate illicit activities?

Law enforcement officials are concerned that cryptocurrencies, with their greater anonymity, could encourage money laundering and abet a wide range of illegal activities.

What could be the effects of cryptocurrencies on privacy protection?

Many advocates of cryptocurrencies believe that their use protects personal privacy more than existing systems and institutions do. For example, Bitcoin transactions are tied to account "addresses", not directly to names. This does not provide absolute protection, however, as linkages can be established between addresses and personal identities, with varying degrees of difficulty.

What consumer/investor protections may be needed in regard to cryptocurrencies?

As with many other innovations, cryptocurrencies can be used in fraudulent transactions or suffer from market manipulation. Beyond outright fraud, there is a risk that consumers or investors may act without sufficient information or understanding.

What tools do policymakers have at their disposal?

As governments weigh the pros and cons of cryptocurrencies, they often reach different conclusions. Policymakers are in the early stages of determining how best to interact with cryptocurrencies, with current responses ranging from declaring them illegal all the way to actively fostering their development. There are a wide range of tools at the disposal of the authorities, but also some unconventional constraints created by the distributed, somewhat anonymized and global nature of cryptocurrencies. Given the decentralized nature of most cryptocurrencies, there would be benefits from global coordination of legal and regulatory treatment, but there is clearly not a global consensus among policymakers.

BOX A: BRIEF TECHNICAL INTERLUDE

What is "blockchain" and how does it relate to cryptocurrencies?

Blockchain is the underlying technology behind most cryptocurrencies. In brief, a blockchain is a continuously growing list of electronic data records (blocks) that are sequentially linked using cryptography. This list, or "ledger," is stored and maintained by a network of users (nodes) that collectively validates each new block and keeps synchronized replicas of the entire ledger – therefore eliminating the need for a central, trusted counterparty. This concept is known as "distributed ledger technology" (DLT), of which blockchain is one form of implementation.

The two terms are so closely identified in some people's minds that they assume all cryptocurrencies use blockchain and all blockchains are related to cryptocurrencies. This, however, is a misconception. Blockchain technology is used for many different purposes (for example, smart contracts) and, on the flip side, some cryptocurrencies do not make use of the technology at all (such as IOTA).

Each blockchain-based cryptocurrency has its own unique distributed ledger and nodes. Each block will typically contain: transactions data (for example, amount, payee, payer), a timestamp and a hash pointer (the link to the previous block). At a high level, a transaction works as follows:

EXHIBIT 2: HOW A BLOCKCHAIN TRANSACTION WORKS

1 REQUEST
Someone requests a transaction (for example, User A wants to send a given number of "cryptocurrency units" to user B)

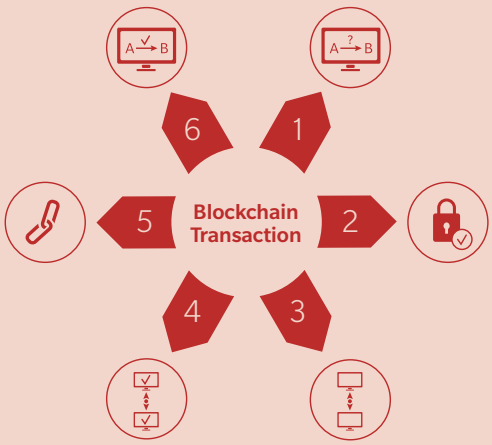
2 ENCRYPT
The transaction data is encrypted with a digital security code and represented electronically as a "block"

3 BROADCAST
The block is broadcast to every node in the network (i.e. computers)

4 VALIDATE
The nodes validate the transaction by solving a cryptographic puzzle associated with the data in the block. The first solver "gets paid" in brand new cryptocurrency

5 APPEND
The block is then added to the front of the chain (list), which provides a permanent and immutable record of the transaction

6 DISTRIBUTE
The transaction is complete (for example, cryptocurrency units move from user A to user B)



As there is no central entity responsible for maintaining the ledger, in order to add a new "broadcasted" block, the nodes need to reach consensus on its validity. To do so, the nodes compete to be the first to successfully solve a cryptographic puzzle – this puzzle is such that it is hard to solve, but easy to check if someone has a solution. Once a solution is found, whichever node solved it offers a "proof of work" that is validated by other nodes; consensus is achieved when more than 50% of the active nodes confirm that the "proof of work" is correct. At the end of this process the new block is added irrevocably to the ledger, creating an auditable transaction log that is designed to be immutable. It is worth noting that any public blockchain depends on the integrity of the consensus system. If some malicious entity gained control of over 50% of active nodes, it is possible they could gain control of the ledger and introduce fraudulent transactions.

These nodes are called "miners," because their proof of work is rewarded with newly created units of whatever cryptocurrency they are mining for (in an analogy with "mining for gold"). Transaction costs are largely driven by the computational power (and as a consequence, energy usage) invested by the solvers in providing the "proof of work."

Cryptocurrency communities are exploring ways to improve multiple technical aspects of the blockchain. For example, some communities are considering ways to validate transactions through distributed consensus different than the "proof of work" described above.[5]

How do cryptocurrencies vary in their implementation?

Since the launch of Bitcoin, over a thousand other cryptocurrencies have been developed. Although most of them are based on blockchain technology, they may differ on key technology aspects – which can make them more suited to specific purposes.

One key distinction is whether a cryptocurrency is public or permissioned. Public (or permissionless) cryptocurrencies allow anyone to own copies of their ledger and add to valid transactions. Conversely, permissioned cryptocurrencies have their ledgers maintained by a known network of authorized stakeholders. For instance, the proposed Utility Settlement Coin would be maintained by financial institutions.

Many cryptocurrencies, even permissioned ones, are accessible to anyone who wants to own and trade them on exchanges. This feature means that any such cryptocurrency, independent of its design rationale, could in theory be treated as a currency.

Another difference in cryptocurrencies' implementation is the level of "privacy" that it allows – that is, to what extent a transaction history can be traced back to individual users. Cryptocurrencies in general provide some level of anonymity, as users use pseudonyms instead of real-life identification. However, some cryptocurrencies are specifically designed to provide greater privacy by using more advanced cryptographic techniques and making it harder to see transaction details. Examples include Monero and Particl.

Other differentiating aspects may include, for example, the techniques used to encrypt information in the blockchain and the type of data and size of each block. As these factors drive the computational power required to expand the ledger, they can give some cryptocurrencies much lower transaction costs than others. Cryptocurrencies can also vary in the amount of coins or tokens they make available, a topic explored in the next Box: "Supply and Demand."

5 Another approach is "proof of stake," where validation is provided by nodes with large ownership in the cryptocurrency.

BOX B: SUPPLY AND DEMAND

Who are the different types of market participants and what drives their behavior?

The key cryptocurrency market participants are:

- **Users**: comprise the broad range of holders of cryptocurrencies for use for purchases, as a store of value, or for investment or speculative purposes. See the later discussion of the sources of demand for cryptocurrencies.
- **Developers**: cryptocurrency communities many times rely on developers focused on the continuous improvement and maintenance of the underlying technology, as well as participating in the cryptocurrency's governance. These developers may be compensated by being invested in the cryptocurrency or by being miners. In many cases, the developers that founded the cryptocurrency continue to be heavily involved in the cryptocurrency's technical development.
- **Validators/Miners (i.e. nodes)**: are the computers that validate and record new transactions in the blockchain in exchange for transaction fees and newly minted units of cryptocurrencies for their owners/users. As the mining process is computationally intensive, typically these machines are designed for this specific purpose by specialized manufacturers (for example, Bitmain and Bitfury). These nodes can also be "grouped" via cloud platforms. In a survey conducted by the University of Cambridge, as of early 2017, publicly known mining facilities are geographically dispersed, but a significant concentration can be observed in certain Chinese provinces.[6] However, this is an evolving landscape and may be impacted by the Chinese ban on Initial Coin Offerings and trading.
- **Crypto-wallets**: are software platforms that enable users to make cryptocurrency transactions through user-friendly interfaces. These wallets also enable users to store their private cryptographic key (basically a fairly long number), which is necessary to execute transactions. Alternatively, users may prefer to simply write down this number on paper and keep it somewhere physically safe. Wallet providers are said to offer "cold storage," if they maintain user passwords mostly in offline hardware devices (that connect to the internet only when needed), typically at a fee. Otherwise, wallet providers are said to offer "hot storage."[7] Examples: Trezor, Ledger, Exodus, Jazz.

6 "Global Cryptocurrency Benchmarking Study," University of Cambridge, Bitcoin.com, April 17, 2017. https://news.bitcoin.com/cambridge-university-global-cryptocurrency-benchmarking-study/

7 Princeton University Coursera class on Bitcoin and Cryptocurrency Technologies, accessed February 8, 2018. https://www.coursera.org/learn/cryptocurrency/lecture/BABeP/hot-and-cold-storage

- **Cryptocurrency Exchanges**: provide digital platforms for the public to buy and sell cryptocurrencies using conventional currencies and/or other cryptocurrencies. These transactions are on a "spot" basis meaning they are agreed upon immediately at today's prices. Interestingly, several smaller exchanges only allow trading between cryptocurrencies. Exchanges earn money by charging conversion fees or dynamic maker/traker fees per transaction. Providers vary in sophistication and variety of services – such as offering their own crypto wallets, enabling peer-to-peer deal negotiation and multiple cryptocurrency support. **Examples: Coinbase, BitX, BTX**
- **Cryptocurrency Derivatives Exchanges**: provide an infrastructure for market participants to take positions on the future price of cryptocurrencies by trading a financial instrument or contract, rather than the cryptocurrency itself. Market participants may choose to transact in derivatives instead of spot markets either with the expectation of gain or to hedge against price volatility. This is the most recent market element discussed in this section; the first US Bitcoin swaps and options were traded on LedgerX in October 2017[8] and the first US Bitcoin futures contract was traded at the Chicago Board Options Exchange (CBOE) in December 2017.[9] **Examples: CME, CBOE, LedgerX**
- **Crypto-payment processors**: provide the infrastructure network and platforms that enable merchants to accept cryptocurrency as a mean of payment – typically by converting it immediately into conventional currencies and charging fees. Price volatility is currently managed through guaranteed exchange rates; in the future they could use derivatives to manage the risk. **Examples: Bitpay, Coinkite, GoCoin**

What drives demand for cryptocurrencies?

There are five fundamental sources of demand for cryptocurrencies, generally analogous to the sources for currency and commodity demand:

- **Use as an alternative currency**: Some owners of cryptocurrencies do so for the same fundamental reasons they own dollars or pounds or yen: because they use it to purchase goods and services or to hold it as a stable store of value that will allow for purchases of goods and services in the future. In many cases, cryptocurrencies are preferred by some over conventional currencies based on greater perceived anonymity or lack of trust in governments and central banks. This source of demand is presumably increasing as more vendors have begun accepting payments in cryptocurrencies, in addition to other factors increasing interest in this medium of exchange.
- **Technological uses**: Many cryptocurrencies are created to help facilitate specific tasks, usually in the realm of payments. The cryptocurrencies can act directly or indirectly as tokens that support a protocol for getting the specific task done. Demand for these is similar to the demand for gold for use in electronics, which is independent of other reasons for its use. Future demand for cryptocurrencies for these uses is also likely to increase, given the surge in applications built around them.

8 "Whoah, That was Fast," LedgerX, October 20, 2017. https://ledgerx.com/whoah-that-was-fast/

9 CNBC, accessed February 8, 2018. https://www.cnbc.com/2017/12/17/worlds-largest-futures-exchange-set-to-launch-bitcoin-futures-sunday-night.html

- **Investment**: Just as some investors believe gold or other commodities are likely to increase in value over time or provide protection against risks of conventional currencies, some buy cryptocurrencies as long-term investments. It is difficult to predict future demand from this source.
- **Market making**: As cryptocurrencies are traded across a multitude of platforms, many times at different prices, some may own cryptocurrencies to make markets and take advantage of arbitrage opportunities. These investors will own a positive inventory to facilitate market making.
- **Speculation**: Others are convinced that one or more cryptocurrencies will increase in price in the short run, regardless of long term prospects. Some speculators may be treating all cryptocurrencies as essentially equal, investing in the asset class without picking winners, while others may make more targeted bets. As with investors, it is difficult to predict future demand from speculators.

What determines the supply of a cryptocurrency?

Supply varies for each individual cryptocurrency. Some increase supply at a more of less predictable pace. Bitcoin, for instance, rewards a miner roughly every 10 minutes with new bitcoins. That reward level is halved roughly every four years, placing a bound on the total bitcoin supply that will ever be available. The algorithms used by other systems can be more variable as additional factors are taken into account. Some cryptocurrencies, such as Ripple, are referred to as "pre-mined" because their supply of coins is predetermined and assigned at the offset.

Placing bounds such as these on the ultimate total supply of a cryptocurrency is intended to avoid devaluing the currency by over-issuance, as has been the fate of many conventional currencies in the past. However, there are ways in which these limits could be circumvented to some extent, even in cases where supply for a specific cryptocurrency is limited:

- Supply rules are often subject to change. For instance, Bitcoin also allows users to decide by consensus to change the supply algorithm. In some cases, this leads to new currencies (further elaborated below).
- New cryptocurrencies could be used for money creation. In other words, deposits or even a new cryptocurrency that are backed by holdings of existing cryptocurrencies could be created on less than a one-to-one basis, much as modern banks lend more than their capital base. If users are willing to treat these deposits or new currency as of roughly equal value to the underlying cryptocurrency, then there will be an expansion of the effective money supply.
- To the extent that holders treat cryptocurrencies as one relatively interchangeable asset class, the creation of new cryptocurrencies expands the effective money supply.

How do new cryptocurrencies come into existence?

Any entrepreneur can create a new cryptocurrency if they can convince users of the value of the proposition. Many new cryptocurrencies are initially funded through an "Initial Coin Offering" (ICO), where the developers of a new cryptocurrency sell off some portion of the currency in exchange for a more established currency (conventional or crypto), to help fund the development of the cryptocurrency's infrastructure. Currently, many developers of a new cryptocurrency attract investors and users by publishing a white paper explaining how the cryptocurrency will work, its design goals and the underlying technology.[10]

Additionally, new cryptocurrencies can be also created through what is known as a "fork" from a previously established cryptocurrency. A fork occurs when there is demand to introduce a new rule or feature to the cryptocurrency. A "soft fork" is analogous to a software update, where a new feature is introduced (for example, improved transaction capacity) without creating incompatibility issues. In contrast, a "hard fork" is a more substantial upgrade, leading to a new cryptocurrency that inherits the ledger from its predecessor. In some cases, the hard fork leads to the new cryptocurrency completely replacing the old one. In other cases, the new cryptocurrency co-exists with its predecessor. For example, Bitcoin Cash was created from a fork from Bitcoin, as some members of the community wanted to lower transaction costs by increasing block size.

10 The white paper for Bitcoin is available through: Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Payment System," accessed January 30, 2018, p.1. https://bitcoin.org/bitcoin.pdf

MACROECONOMIC CONSIDERATIONS

How could cryptocurrencies affect economic efficiency and growth?

There are a number of ways that cryptocurrencies might be able to improve economic efficiency and foster higher growth. Please note that there are large debates among experts as to these potential benefits and as to whether they could be better obtained in other ways. This section will lay out the potential benefits without attempting to do justice to those wider debates.

Cryptocurrencies have the potential to improve payments and payment-like processes, enabling lower costs and increased speed, transparency, reliability, and immediacy in availability of funds. Many payment infrastructure systems were built decades ago based on what was possible with the technology of the past and have a number of high cost intermediaries. For example, cross-border payments often pass through a series of correspondent banks. A cryptocurrency can skip those intermediaries and allow direct peer-to-peer transactions, increasing efficiency with the same or higher reliability than existing approaches. For example, a blockchain ensures that the data in any given block, once recorded, cannot be altered retroactively without the alteration of all subsequent blocks in the chain.

However, these potential improvements to payment are still being tested. For example, it was once believed that Bitcoin transactions costs would be low enough to enable micropayments. However, Bitcoin transaction fees are not only high currently, but also volatile. At the end of 2017 fees spiked above traditional payment systems, driven by the high computational costs, and associated high electricity usage, required to mine bitcoins and accommodate the high volume of transactions[11]. Final settlement also takes longer than traditional systems, both on average and in extreme cases, where it can take as much as two weeks[12]. Alternative coins have tried to address these challenges and many have achieved lower transaction costs by experimenting with different validation methods or using permissioned ledgers.

If transaction costs are lowered and cryptocurrency values stabilize, economic efficiency can potentially be increased by an expansion of payment services. If cryptocurrencies enable lowered transaction costs, they may be useful for people seeking to provide remittances abroad. Similarly, if cryptocurrencies become more stable and provide more reliable consumer protections, they could be used to expand financial inclusion, as they may provide easier access than setting up an account with a formal financial institution[13]. In addition to helping to fight inequality, financial inclusion also increases efficiency and fuels economic growth.

11 BitInfoCharts for average transaction fees in USD. https://bitinfocharts.com/

12 Financial Times, "The currency of the future has a settlement problem," May 2017.

13 Brett Scott, "How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?" 2016, UNRISD Working Paper, No. 2016-1.

Cryptocurrencies and their enabling technologies have the potential to add efficiencies and innovation outside the payments space. As a reflection of the trust in the reliability and security of blockchain technology, many have proposed the use of blockchain for other record management activities, such as voting, government services[14], identity management[15], agricultural trading[16], and even food traceability[17]. These activities could issue their own cryptocurrencies or power their distributed ledger through a non-publicly traded token. For example, the World Food Programme, a United Nation agency, has been testing a private version of Ethereum to provide food assistance, including an ongoing pilot at a Syrian refugee camp. Members of the camp are able to transact at a particular retailer and have their transactions recorded on a blockchain with greater privacy and increased accountability at lower costs.[18]

The possibilities of cryptocurrencies are still being explored and it remains to be seen whether use cases that offer greater benefits and lower risks than existing or future technologies will be developed. While the development of Bitcoin led to the development of blockchain and distributed ledger technologies, it is also possible that these technologies find wider adoption while cryptocurrencies do not. On the other hand, new applications may be developed to use cryptocurrencies that are completely novel and unexpected. It is difficult to draw firm conclusions at this point on the size and nature of the economic benefits that will be brought by cryptocurrencies.

What would be the potential impacts on financial stability if cryptocurrencies were adopted widely?

If cryptocurrencies continue to grow rapidly, they could affect financial stability, usually defined as the ability of the financial system to continue to provide credit and other financial services to the wider economy in the face of shocks. Cryptocurrencies might also provide new tools for managing financial stability. As the technology is still nascent, this may depend on how cryptocurrency adoption evolves and how interlinked it becomes with existing systems. Agustín Carstens, the new head of the BIS, recently cautioned "if authorities do not act preemptively, cryptocurrencies could become more interconnected with the main financial system and become a threat to financial stability."[19]

Among the risks to financial stability, volatile cryptocurrency prices and weak consumer and investor protections could produce losses that affect important financial institutions or markets. The relative opacity of cryptocurrencies, and weak understanding of them by the public, and even many in the financial sector, could exacerbate any resulting loss of confidence or drying up of liquidity and credit.

14 KSI Blockchain — e-Estonia, accessed February 8, 2018. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

15 "Swiss "Crypto Valley" to Create Digital Identities for Its Citizens on the Ethereum Blockchain," Bitcoin Magazine, accessed February 8, 2018. https://bitcoinmagazine.com/articles/swiss-crypto-valley-create-digital-identities-its-citizens-ethereum- blockchain/

16 "U.S. soy cargo to China traded using blockchain," Reuters, January 22, 2018. https://www.reuters.com/article/grains-blockchain/u-s-soy-cargo-to-china-traded-using-blockchain-idUSL8N1PG0VJ

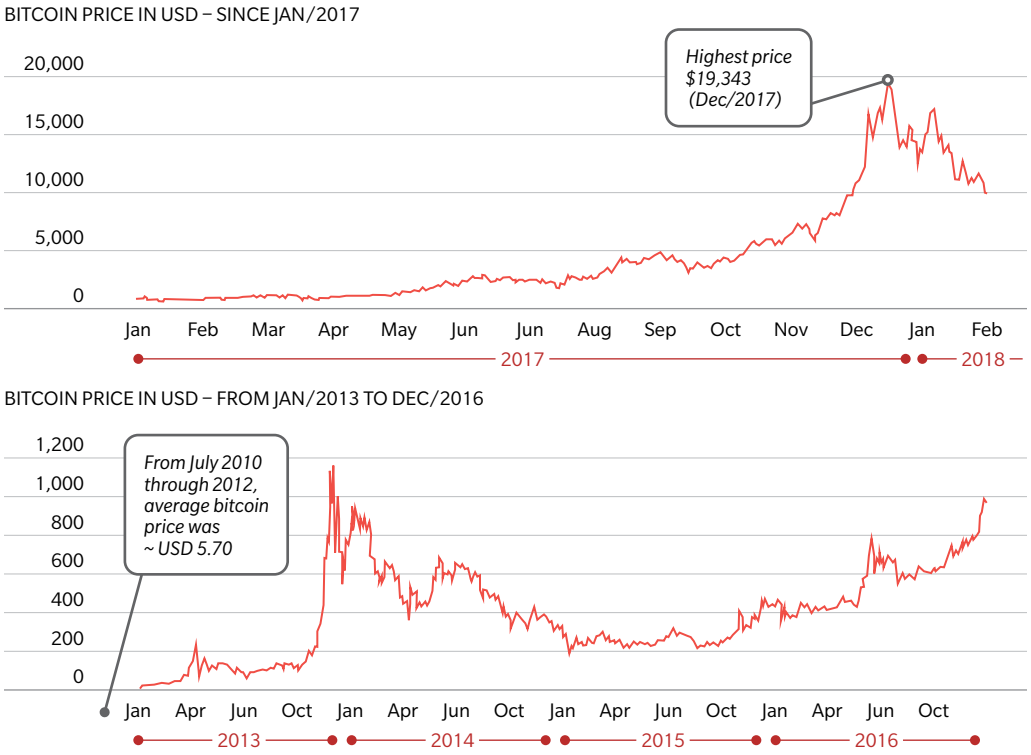
17 "Blockchain Unleashed: IBM Blockchain Blog," IBM, accessed February 18, 2018. https://www.ibm.com/blogs/blockchain/category/blockchain-in-food-safety/

18 World Food Programme (WFP.org), http://innovation.wfp.org/project/building-blocks

19 "Money in the digital age: what role for central banks?" February 6, 2018. Lecture by Mr. Agustín Carstens, General Manager of the BIS, at the House of Finance, Goethe University, Frankfurt. https://www.bis.org/speeches/sp180206.htm

Cryptocurrency prices have been extremely volatile. Bitcoin rose by over 15 times in 2017, and fell by more than 25% in the first month of 2018 (See exhibit 3).[20] Cryptocurrency volatility may likely continue, as many cryptocurrencies limit their monetary supply. When supply is limited, prices will swing with changes in demand. As Bitcoin has shown, demand for cryptocurrencies can be highly variable leading to extreme price volatility.

EXHIBIT 3: BITCOIN PRICE IN US DOLLARS



Leverage has the potential to increase the impact of price volatility on financial stability as the greater the leveraged exposures the greater the impact of a price crash. Cryptocurrency leverage becomes even more problematic if financial institutions become more exposed to this risk, due to their centrality to the financial system and the wider economy. The decentralized and global nature of cryptocurrencies could make it harder for policy makers to monitor how this aspect of the overall financial market evolves. Leverage is already present in the system to some extent. For example, Bitcoin futures offer a mechanism for private investors to gain leveraged exposure to the value of a cryptocurrency. So far, this market is still very limited and many large banks have not offered clients access to these markets[21]. The CBOE, for instance, reported only a bit over one billion dollars of total trades during the first month after the launch of its Bitcoin futures (compared to current Bitcoin average *daily* transaction volume of approximately $15 Billion).[22]

20 "JPMorgan: Blockchain Tech is an 'Opportunity' for Asset Managers," Coindesk, July 13, 2016. Oliver Wyman analysis. https://www.coindesk.com/jpmorgan-blockchain-tech-opportunity-asset-managers/

21 As of January 2018, Morgan Stanley and Goldman Sachs are the only major banks to offer Bitcoin futures trading clearing. "Morgan Stanley Joins Goldman Sachs in Clearing Bitcoin Futures," Bloomberg, January 18, 2018. https://www.bloomberg.com/news/articles/2018-01-18/morgan-stanley-joins-goldman-sachs-in-clearing-bitcoin-futures

22 "Here are all the theories explaining the crypto market crash," Business Insider, January 17, 2018. http://markets.businessinsider.com/currencies/news/bitcoin-cryptocurrency-market-crash-explained-causes-2018-1-1013158074

Participation in cryptocurrency markets from institutional investors is still very limited, as they are leery of exposure to counterparty risk from nascent and lightly regulated spot exchanges, exposure to security risk for the custody of cryptocurrencies and concern about operational connectivity across multiple exchanges to create a unified market.[23] Increased regulation and investor protections could increase confidence in cryptocurrency markets, potentially driving significantly more trading activity. Linkages between cryptocurrencies and financial institutions could increase, if demand from institutional investors grows and financial institutions seek to accommodate that demand.

It is unclear at this point how cryptocurrencies will impact financial institutions. On the one hand, cryptocurrencies may divert substantial business from traditional financial institutions, particularly in payments. This could weaken incumbents, which might injure financial stability. There is also the risk that an environment of fierce competition fuels less desirable types of financial innovation, where new exotic instruments with poorly priced risk are pushed onto the market. On the other hand, cryptocurrencies could make financial institutions stronger and more profitable. Incumbents have begun using and testing blockchain to obtain similar gains in their execution processes and it is possible they could use cryptocurrencies directly as well, if they are useful. It is also possible that new financial institutions that take advantage of these innovations will gain market share and also prove to be more financially stable. Thus, there is a wide range of potential indirect effects on financial stability.

Further, there is the potential for cryptocurrencies to reduce systemic risks in the financial system, especially in the payments sector. If transactions were executed, and funds exchanged, almost instantaneously, a number of credit risks in our existing system would disappear. Of course, other techniques than blockchain and cryptocurrencies may turn out to be more efficient or effective in achieving these same risk reductions.

In a highly interconnected global financial system, cyber security presents its own risks to financial stability. It is too early to tell how cryptocurrencies and distributed ledger technology impact cyber risks. The cryptography algorithms underpinning cryptocurrencies are currently very secure, however, vulnerabilities may emerge based on how other market participants store and manage data. Others see risks emerging from many cryptocurrencies' governance mechanisms, that could cause the network to come to a halt. Please see the recent Oliver Wyman report on the security of cryptocurrencies[24] for more information.

Risks associated with the need for improved consumer and investor protection are discussed later. In essence, problems in these areas can reduce financial stability by either creating very large losses or by damaging consumer and investor confidence in institutions and markets.

23 "BTC for institutions: more hurdles to clear," Goldman Sachs, Top of Mind. http://www.goldmansachs.com/our-thinking/index.html

24 "Cryptocurrency Unmasked, Part 1: Are Cryptocurrencies Secure?" Oliver Wyman, February 2018. http://www.oliverwyman.com/our-expertise/insights/2018/feb/cryptocurrency-unmasked-part-1.html

How might monetary policy be affected by cryptocurrencies?

Theoretically there could ultimately be very large impacts on monetary policy if cryptocurrencies became a far bigger substitute for conventional currencies than is currently true. However, existing levels of cryptocurrencies are dwarfed by the volume of major conventional currencies. The total estimated global value of cryptocurrencies peaked in early January 2018 at over $800 Billion (before tumbling to less than $500 billion only a couple of weeks later).[25] In contrast the world's coins and banknotes alone amount to $7.6 trillion. Including checking accounts brings the figure to nearly $37 trillion, while adding in money market and savings accounts brings it to over $90 trillion.[26] The difference in scale becomes even bigger if cryptocurrency holdings used for non-monetary purposes are taken out.

Therefore, in the immediate term, the biggest monetary policy challenges from cryptocurrencies would likely be for countries with exchange and capital controls. This is because market participants could potentially bypass the need to purchase foreign currency through traditional payment systems, by using cryptocurrencies instead for capital transfers and foreign exchange transactions. This depends, of course, on whether, and how effectively, a government limits the ability to buy or redeem cryptocurrencies with their national currency.

The more cryptocurrencies are treated as currency and the larger they grow, the more they challenge monetary policy. A major barrier to their treatment by holders as a true currency is the extreme price volatility they have experienced thus far. Central Banks, and their national governments, may also take further actions to limit adoption of cryptocurrencies, if they become large enough to threaten the dominance of conventional currencies.

If they become a much bigger factor on the world stage, cryptocurrencies have the potential to create long-term challenges to monetary policy similar to some already experienced using conventional currencies. For example, economies that switch heavily from the use of their national currency to cryptocurrencies, either through government choice or households and businesses fleeing their unstable currency, would face issues similar to "dollarization." Such economies would find price levels and interest rates to be determined more by external factors than by national fiscal and monetary policies.

Similarly, if society loses faith in conventional money throughout the world, countries might face a situation similar to the gold standard era when the value of national currencies were fixed to gold. This would also be analogous to a global monetary union, with all their pluses and minuses, in addition to any purely cryptocurrency related issues. For instance, monetary policy could be simultaneously too loose for some countries and too tight for others, with a single policy having different effects in different nations.

It is possible that central banks could choose to develop their own cryptocurrencies,[27] and some have considered it. This cryptocurrency could be limited to financial institutions or it could be made widely available to the public. If limited to financial institutions, this would be similar to bank

25 Coinmarketcap. https://coinmarketcap.com/

26 Jeff Desjardins, "All the World's Money and Markets in One Visualization." The Money Project, Visual Capitalist, October 26, 2017. http://money.visualcapitalist.com/worlds-money-markets-one-visualization-2017/

27 For the sake of simplification, per the discussion in the BIS Central Bank Cryptocurrencies paper, we also refer to these as "cryptocurrencies" although a central bank issued cryptocurrency would be a liability of the government, different than the definition put forth from the BIS CPMI cited at the beginning of this paper. See the BIS Central Bank cryptocurrency paper for a more detailed discussion on this topic.

reserves, which are already electronic, but the underlying technology could enable peer-to-peer payment transactions and immediate settlement between banks. Both the Bank of Canada and Singapore Monetary Authority have run pilot projects but concluded the technology is still too early to adopt.

Instead of limiting their own cryptocurrency to financial institutions, a central bank may choose to develop a universally accessible cryptocurrency with one-for-one convertibility with cash and reserves. This could provide new advantages to monetary policy, for example, greater visibility into monetary demand and the possibility of interest payments on the cryptocurrency (potentially including negative interest rates). However, many open questions remain, including whether it would be adopted (as some may express concerns around anonymity) and whether this would be too disruptive to the financial sector (as people may prefer to hold the central bank currency instead of holding bank deposits).[28]

How could fiscal policy be affected by cryptocurrencies?

When a government, or its central bank, creates money, it is essentially able to buy things for little or no cost. This has an immediate fiscal benefit by reducing the need to borrow or tax to buy the same goods or services. In the simplest case, issuing 20 dollars worth of paper money that costs pennies to print is a real bargain for a government, although there are indirect costs to issuance when done in bulk, such as fueling inflation or lowering the currency's value in the foreign exchange markets. Economists refer to the gain to the government as "seigniorage". There are at least three sources of seigniorage: minting coins, printing paper money, and creating electronic money, such as when the Federal Reserve or another central bank buys bonds. The last is currently by far the largest factor, although that is partially due to the massive monetary easing of recent years.

Estimates of the annual value of seigniorage in the US range from about $30 billion to $90 billion,[29] equivalent to about one or two percent of the federal budget.[30] This benefit would be at least partially at risk if cryptocurrencies come to substitute for national currency in the future.

In the most immediate term, cryptocurrencies could have an impact on tax receipts as they may allow for easier tax evasion – this point is elaborated separately below.

What are the options for taxing cryptocurrencies?

Taxation is a policy area where countries have been particularly active, as they have chosen to define cryptocurrency as a currency or an asset.

As cryptocurrency market capitalizations have increased to hundreds of billions of dollars, tax authorities globally have sought to determine a view on the classification of cryptocurrencies.

28 Tony Yates, "The consequences of allowing a cryptocurrency takeover, or trying to head one off," Financial Times, Alphaville, June 7, 2017. https://ftalphaville.ft.com/2017/06/07/2189849/guest-post-the-consequences-of-allowing-a-cryptocurrency-takeover-or-trying-to-head-one-off/ Izabella Kaminska, "Crypto fiat coin confusion," Financial Times, Alphaville, January 12, 2018. https://ftalphaville.ft.com/2018/01/12/2197556/crypto-fiat-coin-confusion/

29 Based on the fact that there are over $1.5 trillion of notes in circulation issued by the Federal Reserve in the US, the calculation could be the amount by which the currency in circulation increases in a year (about $90 billion recently), it could also be the amount you would have had to pay to borrow the outstanding stock of paper and electronic money, minus anything you do pay for creating the money (about $75 billion recently), or it could be the inflation rate times outstanding stock (about $30 billion recently). Estimates based on a) comparison between currency in circulation at the end of year 2016 vs. 2017; b) average borrowing cost times monetary base; and c) inflation times currency in circulation. FRED Economic Data. As of January 31, 2018. And "Interest Expense on the Debt Outstanding," Treasury Direct.

30 "Budget." Congressional Budget Office, December 7, 2017. www.cbo.gov/topics/budget.

Cryptocurrencies are versatile and they share characteristics with other traditional financial products: they can be earned for a service (via processes like transaction validation), used to purchase goods and services (like currency) and/or held for longer-term investment (like a commodity or security). Countries have typically applied different tax treatments each for currencies, investment assets and fixed assets, often taking the form of varying sales taxes, transaction taxes, or capital gains taxes.

A patchwork quilt of tax policy has sprung up globally. Most tax authorities recognize cryptocurrencies like Bitcoin as a capital asset, being subject to a capital gains tax whenever a cryptocurrency is bought or sold. In the US, the IRS notably made such a ruling in 2014. Despite the apparent simplicity, cryptocurrency tax reporting requirements remain murky, as cryptocurrency is in many ways different from traditional securities that receive similar treatment. For example, the current US cryptocurrency tax policy creates some ambiguity as to whether sales are ultimately taxable when they occur at a foreign-domiciled exchange, similar to questions raised about foreign-based brokerage accounts denominated in a foreign currency.

Regardless of tax classification, effectively taxing cryptocurrencies is difficult given the anonymization underlying blockchain technology, as well as the large number and decentralized nature of cryptocurrencies and exchanges. Taxation of public cryptocurrencies, like Bitcoin, is more challenging than taxation of permissioned cryptocurrencies. The latter only requires regulating and overseeing the set of known permissioned entities. On the other hand, regulating public cryptocurrencies requires setting standards and enforcing them across a decentralized anonymous network spread across the world. Existing controls could be applied in some cases as cryptocurrencies are converted to conventional currencies, however, these controls could be evaded in cases where value is maintained in cryptocurrencies.

The complexity also adds challenges for taxpayers. Those with complex trading activity have to collect information to pay their taxes from a wide variety of sources. Some exchanges have started to provide this information to customers. For example, Coinbase provides tax forms with gross proceeds from crypto-trading to US-based customers,[31] but this is not a standard or a requirement.

In the effort to enforce taxation policies, tax authorities have recently been seeking to gain stronger insight into transaction volumes for Bitcoin and other cryptocurrencies, but it is difficult to comprehensively ascertain ownership across the cryptocurrency market. Additionally, the geographic location of the taxable event may also be difficult to trace. These efforts may require added compliance and record-keeping costs, as well as coordination and information sharing among policymakers around the world.

31 Coinbase. https://support.coinbase.com/customer/portal/articles/2721660

CONSUMER AND INVESTOR CONSIDERATIONS

To what extent may cryptocurrencies facilitate illicit activities?

In the traditional financial system, there are a series of regulations in place to limit illicit activities. These are known as know-your-customer (KYC) and anti-money laundering (AML) regulations and they require banks to perform due diligence on customers and monitor and report suspicious activity. Cryptocurrencies, as they enable anonymous (or at least pseudo-anonymous) transactions that do not rely on a third party like a bank, can circumvent these regulations. While different types of consumers may value the added anonymity that cryptocurrencies provide for different reasons, it does also make cryptocurrencies well-suited for a number of illegal activities – such as tax evasion, black market transactions, financing terrorism, avoiding sanctions and enabling ransomware payments and money laundering schemes. It should be noted that cash has the same characteristics of anonymity and relative ease of use, which is why governments attempt to track large scale movements of cash.

The greater level of anonymity is an intentional design feature for many cryptocurrencies. Their electronic transactions omit surface-level real-life identifiers and are not processed centrally prior to being executed. Though many cryptocurrencies indeed are recorded via a public distributed ledger of transaction data (making them more transparent even than cash), market participants are known only by their "address(es)," which limits traceability to any real-world identity. Therefore, little to no personally identifiable information about the payer or the payee is transmitted in a transaction itself.

For Bitcoin, it is however possible that a user may be tracked and possibly identified through different matching techniques and blockchain analysis combined with transaction "metadata" from Bitcoin address reuse and IP address monitoring. A sufficiently motivated user could get around this however, by making use of what are known as "mixers" which swap your bitcoins for ones with a different transaction history[32] – effectively laundering them. Additionally, new cryptocurrencies have been designed to avoid this and provide more anonymity.

Historical patterns of "dark web" activity – effectively online black markets often dealing in illegal commodities and services, and commonly taken as a proxy for less obvious illicit cryptocurrency activities – seem to support the notion that increasing anonymity (such that a counterparty is fully obscured), though not necessarily encouraging illicit activity, does facilitate it. Over the past decade these activities have shifted away from popular and more-oft scrutinized cryptocurrencies, like Bitcoin, to alternatives that offer more secure privacy.

32 Mauro Conti, "A Survey on Security and Privacy Issues of Bitcoin," IEEE.

In the mainstream financial system, institutions, as the trusted third parties intermediating transactions, are the natural place for regulatory enforcement given their access and control of information. They continue to play a role in ensuring AML/KYC regulation, at the point of conversion from cryptocurrencies to conventional currencies. For example, some UK lenders have declined mortgages to people whose downpayment could not be traced because the money was made selling cryptocurrencies.[33]

Cryptocurrencies do not have an exact equivalent of financial institutions when compared to traditional currencies. In the case of permissioned cryptocurrencies though, enforcement could happen at the level of the fixed, known entities responsible for validating transactions.

On the other hand, public cryptocurrencies are more challenging to regulate. Enforcement could happen at the level of exchanges or digital wallets. This has been so far the preferred method for AML/KYC compliance; for example, South Korea recently has begun requiring exchanges to track personal information such as real names[34]. These AML/KYC mechanisms implemented at some exchanges provide information about the moment of initial client registration and when conventional currency is converted into cryptocurrencies or vice versa. The individual transactions of cryptocurrencies between existing users may not effectively be monitored for potential AML risks.

However, a sufficiently motivated user could avoid the well-known and regulated exchanges and cryptocurrencies and conduct their activity through a network of decentralized entities spread throughout the globe. Further adding complexity, responsibility for AML compliance and supervision/enforcement across jurisdictions may be unclear and may require global coordination.

Fully anonymous and decentralized cryptocurrencies may not only enable criminals to remain anonymous but often can make the execution of some illegal activities actually easier than in the past. As a practical example, when both India and Venezuela banned their highest denomination bank-notes to make it more difficult to pay bribes and to render any accumulated black money useless, the demand for and use of less traceable cryptocurrencies surged. Of course, some of this would have been a reasonable response by honest individuals who feared expropriation in the future.

What could be the effects of cryptocurrencies on privacy protection?

While AML/KYC regulations help governments manage illicit activities, these regulations require financial institutions to collect a certain amount of information about their customers. But, people may want to limit the information they disclose, as privacy and anonymity reduces risk of theft, surveillance, unwanted solicitations, and excessive government intrusion or interference.

Generally, cryptocurrencies (especially newer currencies) offer a higher level of protection to individuals' privacy compared to most means of payment, which in theory could make it an important "tool" to minimize the risk of violation of consumer privacy. This increased sense of

33 Kate Beioly, James Pickford. "Bitcoin investors struggle to cash out new fortunes," Financial Times, January 12, 2018, accessed February 4, 2018. https://www.ft.com/content/40c64992-f606-11e7-88f7-5465a6ce1a00

34 Kyungji Cho and Shinhye Kang, "S. Korea to Decide on Crypto Trading Only After Government Talks," accessed February 8, 2018. https://www.bloomberg.com/news/articles/2018-01-15/s-korea-to-decide-on-crypto-trading-only-after-government-talks

privacy and anonymity may be a key driver of interest in cryptocurrencies, and many niche online communities have already started to adopt cryptocurrencies as the de facto medium of payment. For example, the Wikileaks organization requests its users to donate using Bitcoins, presumably to deter government notice of any individual's financial support for the organization's interests.

However, as with any technology in its early stages of maturity, data security is not guaranteed. As discussed previously, personal information may still be traceable for Bitcoin, the most popular cryptocurrency. Additionally, many users prefer to manage their cryptocurrency through a digital wallet or exchange. As AML/KYC regulations evolve, so might the privacy commitments made by these service providers. For example, Coinbase (a popular wallet) retains the right to disclose any information as necessary to satisfy any applicable law, regulation, sanctions program, legal process, or governmental request.[35]

Privacy may also be reduced indirectly from AML/KYC regulations. If wallets and exchange become required to store and track personal information, privacy could be further compromised if these service providers do not also take sufficient precautions to protect this information. Privacy or security breaches at digital wallets and exchanges then also creates risks even for those not directly using them. When someone is identified, and their full transaction history is on a public ledger, then everyone they have transacted with can also be more easily identified. Maintaining effective anonymity thus depends on the data security of every single entity one transacts with.

What happens when privacy is breached is another important impact to consumers. Once consumer privacy is violated (for example, when payment and personal information becomes public), it is difficult – if not impossible – to reestablish it. In traditional banking, consumers might previously have had recourse (for example, insurance) for loss of identity information at the fault of a trusted third-party such as a bank. In turn, the decentralized system behind cryptocurrencies provides limited protections in case of violation of privacy due to the lack of a central counterparty responsible for the underlying transaction.

All these concerns have raised the question of whether the anonymity and privacy built into and associated with cryptocurrencies should be encouraged or controlled, since increased privacy protections could also enable increased illicit activities. Some countries have already made these decisions, for example South Korea with the previously mentioned decision to increase control over it.

Therefore, despite hypothetically offering a similar level of privacy protection as cash, it is not clear whether cryptocurrencies will ultimately offer better privacy protections than existing institutional systems.

35 Coinbase, Privacy Policy, accessed on January 31, 2018. https://www.coinbase.com/

What consumer/investor protections may be needed in regard to cryptocurrencies?

Policymakers across many countries have a responsibility to ensure confidence and trust in financial markets through consumer and investor protections. As cryptocurrency markets are thin and volatile, the risks of price manipulation, fraud, market manipulation and anti-competitive behavior are higher. There are few regulations currently in place to set market standards across individual and group conduct, information disclosure, and exchange mechanisms.

Standards of conduct may be needed to protect against fraud. Reflecting higher valuations, cryptocurrencies have been particularly rife with fraudulent activity seeking to take advantage of less savvy investors in an environment of limited ramifications for fraudulent behavior. For example, investment schemes involving unlicensed individuals or unregistered firms "guaranteeing" high investment returns have emerged.

Consumers and retail investors may assume that standards of conduct that exist in other regulated markets (such as equity markets) may apply to cryptocurrency markets. For example, an estimated $4 billion was raised in 2017 through ICOs,[36] many being made openly accessible to any investor. The apparent light level of regulation was doubtless one incentive for most issuers to use this route, as opposed, for instance, to doing an initial public offering of equity or selling other conventional securities. However, it is not clear in all cases what level of regulation currently applies, much less what the optimal approach would be. In the US, the SEC has warned that many ICOs are securities offerings and must follow those rules, but it is not clear this has always been done in practice. Further, some ICOs appear potentially fraudulent, promising big returns in exchange for tokens or cryptocurrencies that may result in total loss to investors. While the private market has begun to take actions against risks (for example, Facebook has prohibited ICO and cryptocurrency advertisements[37]) existing regulation may not provide the legal recourse to recover losses in the case of misconduct.

Further, thin markets are particularly sensitive to price manipulation. Many people trust cryptocurrencies due to their self-governance mechanisms. However, these mechanisms may not be themselves sufficient to avoid collusion completely, especially when the market is concentrated in a small subset of individuals. For example, as has happened in the past, groups of traders may organize over instant messaging groups and forums to orchestrate "pump and dump" schemes on cryptocurrency markets with few ramifications, if any. As this type of market manipulation is illegal in equity markets, some are exploring this regulatory gap.

Lack of clear guidance against self-dealing also exposes investors to price manipulation. Ascertaining self-dealing is particularly challenging given levels of anonymity. It may be that exchanges are the best placed market participants to address this risk, however, they are also a potential place where this risk originates. As a notable example, a recent study suggests that the trading activity between two self-dealing bots at then-popular exchange Mt. Gox may have been

36 "ICOs In 2017: From Two Geeks And A Whitepaper To Professional Fundraising Machines," Forbes, accessed February 8, 2018. https://www.forbes.com/sites/outofasia/2017/12/18/icos-in-2017-from-two-geeks-and-a-whitepaper-to-professional-fundraising-machines/#45fb5137139e

37 "New Ads Policy: Improving Integrity and Security of Financial Product and Services Ads," Facebook Business. January 30, 2018. https://www.facebook.com/business/news/new-ads-policy-improving-integrity-and-security-of-financial-product-and-services-ads

responsible for an increase in Bitcoin prices in 2013. These bots may have even been originated from Mt. Gox itself.[38]

Consumers may also seek recourse when they are harmed outside of conduct-related issues. Lost passwords, lack of backup recovery methods, death of the account holder, etc. all provide little to no recourse to reclaim funds. (This is analogous in some ways to situations where large amounts of cash have been misplaced.) Consumers are also increasingly exposed to risk of cyber attacks. Emboldened by high valuations, hackers have launched increasingly frequent attacks with some success. Consumers may perceive cryptocurrencies to be safe because of the sophisticated way cryptography is used, however, personal keys can still be breached by malicious hackers targeting exchanges, wallets, or even individuals, who may not take the necessary precautions to secure user passwords. Policy makers have started to make moves in this area: Japanese authorities recently ordering Coincheck, a wallet and exchange service, to refund their clients after hackers stole $500 million worth of cryptocurrencies.[39]

Disclosure and transparency standards could help investors make better informed decisions about what exchanges they use and what type of information to expect. For example,[40] the owner of the CoinMarketCap exchange decided to delete South Korean bids and offers embedded in its listing, causing prices to fall as much as 24% in 2018. The exchange's owner made the change to improve pricing quality, as he observed the South Korean bids and offers were higher than elsewhere and suspected their reliability. However, the deletion came without any transparency around the move and confounded traders.

38 N, Gandal, et al, "Price manipulation in the Bitcoin ecosystem," Journal of Monetary Economics, 2018, ISSN 0304-3932.

39 "Japan raps Coincheck, orders broader checks after $530 million cryptocurrency theft," Reuters. January 28, 2018. https://www.reuters.com/article/us-japan-cryptocurrency/japan-raps-coincheck-orders-broader-checks-after-530-million-cryptocurrency-theft-idUSKBN1FI06S

40 "The Programmer at the Center of a $100 Billion Crypto Storm," Wall Street Journal, January 23, 2018. https://www.wsj.com/articles/the-programmer-at-the-center-of-a-100-billion-crypto-storm-1516708800

REGULATORY OPTIONS

What tools do policymakers have at their disposal?

As discussed throughout this primer, there are a wide range of areas policymakers may choose to focus on, whether to build trust and legitimacy in cryptocurrency markets, limit their growth and activity, protect financial stability or serve other goals. Broadly speaking, financial regulation may span the following areas:

- **Market integrity and efficiency and investor protection**: Market regulators may act to improve fairness, efficiency, price discovery and liquidity. Examples of policy tools include delineating conduct rules for market participants and defining and penalizing price manipulation, setting trading rules, setting standards for participating investors and information disclosure for ICOs, as well as post-ICO, ongoing disclosure requirements. Policymakers could also require registration or licensing for different market participants.
- **Consumer protection**: Policy tools available for consumer protection include setting minimum standards for service providers, as regards privacy protection, information sharing and safeguards against cyber risks. Policies could also include limiting access to certain types of products for retail customers and taking enforcement action as a deterrent to fraud and misconduct. Price regulation is also an available tool, such as limiting the transaction fees or spreads that can be charged by services that convert cryptocurrencies into conventional currencies.
- **Financial stability and prudential regulation**: Many central banks and other financial regulators look to ensure the stability and soundness of the financial system as a whole, as well as financial institutions individually through prudential regulation. Policy tools may include setting limits or standards to activities undertaken, for example, limiting the amount of leveraged exposure. Policymakers may also look to collect data to monitor the growth of a new market activity and its linkages to the financial system. In the extreme, regulators could forbid any linkages between the financial institutions they regulate and the cryptocurrency ecosystem.
- **Limiting illicit activities**: policymakers may look to curb the illicit uses of a new market. Policy tools include implementing AML/KYC regulations and increasing the level of monitoring and tracking. Policymakers may also choose to take enforcement actions against various parties, including criminal penalties. Finally, they could ban or shut down certain market participants if they are found to be aiding illicit activities.

Policymaking involves trade-offs. Increasing market integrity by setting conduct standards, increasing disclosure requirements, and establishing custody and safeguard requirements, for example, could all help build trust with various types of investors and bring in more trading volume to the market as a whole. However, they may also make it more costly for individual cryptocurrency initiatives or market participants and may hinder innovation. Many may be attracted to cryptocurrency for the anonymity from the government. However, to the extent that anonymity is used for illicit activities, the ensuing externalities may justify limiting anonymity through AML/KYC regulations.

Depending on how cryptocurrencies are treated (for example, as a currency or even as a security) and the availability of existing regulation in any given country, existing regulation may be adapted to appropriately cover cryptocurrencies. In other cases, entirely new regulation may need to be drafted.

Countries currently have a range of approaches with respect to cryptocurrencies. So far, countries differ both in terms of the level of formality of their policies (ranging from public statement to formal policies) and the level of favorability with which they view cryptocurrencies.

At one extreme, some countries have chosen to completely ban cryptocurrencies. For example, China, after enacting regulation that prohibits ICOs and cryptocurrency trading in specialized exchanges, has also made moves to block access to any websites related to ICOs and cryptocurrency trading[41]. On the other end of the spectrum, Australia and Japan have both recognized cryptocurrencies as a formal means of payment and a type of financial asset.

Most governments are still in the process of enacting codified legislation or specifying how cryptocurrencies will be treated in existing regulatory frameworks. Many have warned consumers and the investor community about the risks of investing in cryptocurrencies; indicated informally that they have intentions to enact relatively favorable regulation; or simply adopted a "wait and see" approach, observing cautiously the evolution of the technology and its effects in the system.

Thus, there is clearly not a consensus on the "right" legal and regulatory approach. As policymakers and industry participants pursue the answers to the above (and other) questions there could be a push for increased global coordination in policy, with the potential of increasing convergence. But is still too early to make any bet as to which direction they will follow.

41 "China to stamp out cryptocurrency trading completely with ban on foreign platforms," February 5, 2018. South China Morning Post. http://www.scmp.com/business/banking-finance/article/2132009/china-stamp-out-cryptocurrency-trading-completely-ban

CONCLUSION

Cryptocurrencies, while they have been around for the past decade, are a relatively new, evolving, and largely ill understood phenomenon. Given their growing size and importance, it will be crucial for policymakers and regulators to better understand them and to make the appropriate public policy choices. The current level of consumer hype appears to be considerably overdone. At the same time, cryptocurrencies, broadly defined, are unlikely to vanish again. Indeed, it is more likely that they grow in importance and evolve in their approaches, requiring policies to deal with them.

BIBLIOGRAPHY

- European Banking Authority (2014) Opinion on "Virtual Currencies."
- Financial Conduct Authority (April 2017) Discussion Paper on distributed ledger technology and (Dec 2017) Feedback Statement on Discussion Paper.
- Bank of England Quarterly Bulletin (Q3 2014) "Innovations in payment technologies and the emergence of digital currencies" and "The economics of digital currencies."
- Bank for International Settlements (BIS) Quarterly Review (September 2017) "Central bank cryptocurrencies."
- Bordo and Levin (2017), "Central Bank Digital Currency and the Future of Monetary Policy," Hoover Institutions Economics Working Papers.
- Barrdear and Kumhof (2016) "The Macroeconomics of Central Bank Issued Digital Currencies."
- He et al (2017), "Fintech and Financial Services: Initial Considerations," International Monetary Fund Staff Discussion.
- Pinsent Masons (2017) Bitcoin, Blockchain & Initial Coin Offerings: A Global Review.
- Credit Suisse – "Blockchain 2.0 – Cryptocurrencies are only the beginning", January 2018.
- Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) joint statement on Cryptocurrencies, February 2018.
- George Mason University (2016) Bitcoin: A Primer for Policymakers.
- Coinhills – Statistics on Bitcoin Market Activity.
- University of Cambridge (2017) Global Cryptocurrency Benchmarking Study.
- Kevin Tu and Michael Meredith "Rethinking Virtual Currency Regulation in the Bitcoin Age."
- Matthew Kien-Meng Ly. Coining bitcoin's "legal-bits": examining the regulatory framework for bitcoin and virtual currencies. Harvard Journal of Law & Technology. Volume 27, Number 2 Spring 2014.
- J.P.Morgan Cazenove – "Blockchain – A revolutionary technology too important to ignore," May 2016.
- Goldman Sachs – "Top of Mind – Is Bitcoin a (Bursting) Bubble?" February 2018.
- UK Government Office for Science – "Distributed Ledger Technology: beyond block chain," 2016.
- Boucher, Philip – European Parliament Research Service – "How blockchain technology could change our lives," February 2017.
- Oliver Wyman – "Blockchain in Capital Markets," January 2016.
- Oliver Wyman – "Unlocking Economic Advantage with Blockchain," July 2016.
- Oliver Wyman – "The Blockchain Revolution For Loyalty Programs," 2017.
- Oliver Wyman – "Cryptocurrency Unmasked, Part 1: Are Cryptocurrencies Secure?" February 2018.

ABOUT THE AUTHORS

Douglas J. Elliott
Partner in the Finance & Risk and Public Policy and Corporate & Institutional Banking Practices
Phone: +1 646 364 8444
Email: douglas.elliott@oliverwyman.com

Larissa de Lima
Engagement Manager in the Corporate & Institutional Banking Practice
Email: larissa.delima@oliverwyman.com

Ryan Singel
Associate
Email: ryan.singel@oliverwyman.com

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN