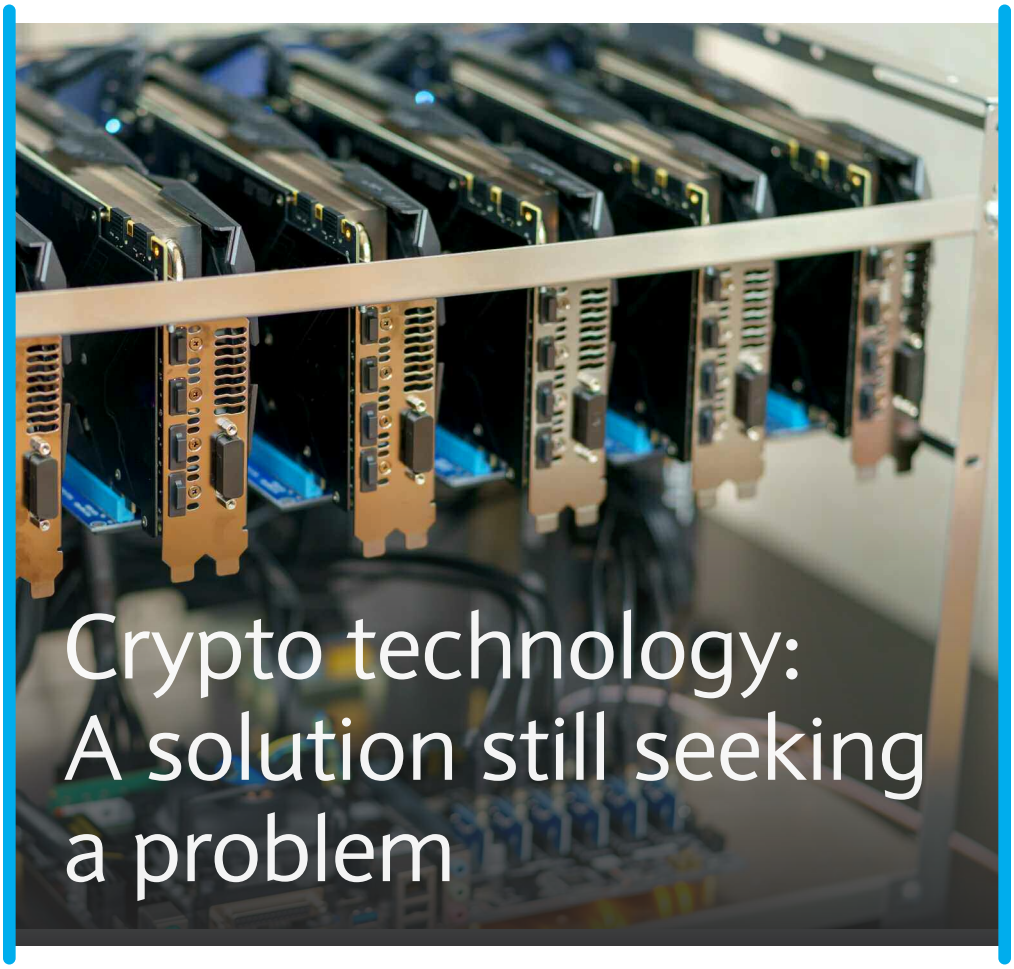
BARCLAYS

10 April 2018



Crypto technology: A solution still seeking a problem

#emergingpayments

#futurebanking

Joseph Abate
+1 212 412 7459
joseph.abate@barclays.com
BCI, US

Marvin Barth
+44 20 3134 3355
marvin.barth@barclays.com
Barclays, UK

Zoso Davies
+44 20 7773 5815
zoso.davies@barclays.com
Barclays, UK

Tomasz Wieladek
+44 20 3555 2336
tomasz.wieladek@barclays.com
Barclays, UK

This is an extract from the Equity Gilt Study 2018

Completed: 10-Apr-18, 00:19 GMT Released: 10-Apr-18, 04:10 GMT

Crypto technology: A solution still seeking a problem

Joseph Abate
+1 212 412 7459
joseph.abate@barclays.com
BCI, US

Marvin Barth
+44 20 3134 3355
marvin.barth@barclays.com
Barclays, UK

Zoso Davies
+44 20 7773 5815
zoso.davies@barclays.com
Barclays, UK

Tomasz Wieladek
+44 20 3555 2336
tomasz.wieladek@barclays.com
Barclays, UK

Despite tremendous hype over the potential for crypto technologies in money and finance – specifically, blockchain and distributed ledger technology – we see little likelihood of widespread adoption in any area in the near future. Crypto currencies may have a home in low-trust corners of the global economy, but broader adoption of crypto technologies faces critical challenges and strong incumbents.

Our primary findings

- **Adoption of crypto technologies faces four critical challenges:** 1) acceptance/trust; 2) sovereignty/regulation; 3) privacy; and 4) irreversibility. At present, existing technologies appear to be sufficiently good, or even better, to deter broad crypto technology adoption in money and finance.
- **Adoption of crypto currencies – a specific use case of crypto technologies – provides a case study in the four critical challenges to adoption:**
  - In wealthy societies, adoption appears primarily speculative and thus likely temporary.
  - More durable potential long-run demand likely will come from low trust and opportunity economies and criminal enterprise, based on crypto currencies' ability to facilitate trust in transactions without legal enforcement that may outweigh privacy and irreversibility costs.
  - But sovereign power likely will restrict usage to only weaker states and the criminal shadows of the global economy.
- **Incorporating those lessons, we examine five areas of money and finance where crypto technologies may hold promise: 1) fiat money substitutes; 2) smart contracts; 3) asset custody; 4) settlements; and 5) payments.**
  - In each area, we find that incumbent technologies retain significant advantages over crypto technologies at their current stage of development, and the four critical challenges we identify still represent significant hurdles to crypto technology adoption.
  - Finally, history suggests that the ultimate beneficiaries of crypto technology adoption likely will be incumbent financial institutions, rather than disruptors.

Blockchains and distributed ledgers, collectively crypto technologies, continue to generate extensive excitement about their potential. In *Fintech primer vol. 3 – Blockchain* (9 March 2016), our equity colleagues laid the foundation for some scepticism regarding effective uses of these technologies that we largely still hold. Since its publication, there have been significant developments in crypto technology in general and the uptake of crypto currencies in specific. We reflect upon those to update our conclusions regarding crypto currencies and potential uses of crypto technologies.

In the first section, we introduce four critical challenges that we see to crypto technology adoption. We then examine the specific application of crypto technologies in non-sovereign currencies as a case study in the factors that lead to adoption and the role of the critical challenges we identify. We then reconsider applications of crypto technologies in six potentially promising areas of money and finance. Finally, we consider who might be the long-run winners of eventual adoption of crypto currencies.

Critical challenges for crypto technology adoption

Crypto technology must address four challenges

One of our key points is that there is nothing new under the sun as regards the application of crypto technologies in money and finance. Most of the problems crypto currencies propose to solve already have incumbent solutions that may be difficult to dislodge, particularly if they are Pareto superior to – that is, more desirable than – *current* crypto technologies. To dislodge incumbents, crypto technologies will have to overcome four critical issues that reoccur across the proposed uses we consider:

- **Acceptance/trust:** The willingness of a critical mass of others to trust and accept a new platform or vehicle for transactions. All new monetary and financial technologies face issues of trust and acceptance. Crypto technologies offer new means to facilitate trust in multi-party transactions, but must gain acceptance (generally) without sovereign support amid widely used and trusted incumbent technologies.

- **Sovereignty/regulation:** Nearly all sovereigns have the ability to dictate the type and form of transactions allowable within their borders and, in some cases, beyond. This imposes a requirement that new monetary and financial technologies adhere to sovereign prerogatives. A widely touted advantage of crypto technologies is that they enable transaction trust without a legal structure or sovereign interference, but this puts them in direct conflict with sovereign priorities, including seigniorage, tax collection and regulation of finance and commerce.

- **Privacy:** For many if not most transactions, participants desire at least a degree of privacy that shields their transactions from others, while at the same time, sovereigns desire the ability to monitor transactions for legality. A potential short-coming of crypto technologies is their (current) lack of privacy; distributed ledgers make public all transactions contained on blockchains and experiments have shown that the public keys in the blockchain record can be traced to individuals, unmasking any privacy. While newer crypto offerings attempt to address this, successful efforts likely will meet with government suppression.

- **Irreversibility:** Another desired attribute of transactions is reversibility: the ability to unwind the transaction if it was in error or if one or more parties to the transaction fail to deliver on the expected terms. Blockchain and distributed ledgers provide means of contract or transaction enforceability without a supporting legal structure, but lack recourse or reversibility in the cases of errors or fraud.

Box 1: Blockchain in 18th Century France[1]

Blockchain is an extension of much older value transfer technology, dating to the era of metallic money and horses.

Consider the problem facing Le Nicolais and Company in August 1763. How do you transfer a large amount of money from Laval, a textile manufacturing town located 190 miles west of Paris, to the capital – and through the crime-ridden Bois de Boulogne? LeFebvre estimates that on average, the mail and news travelled at 10-12km/hour between major cities. Special fast couriers travelling at full gallop might travel faster, at over 14km/hour.[2] Three thousand livres was equivalent to 125 louis d'or, the standard gold coin in France at the time. Each golden louis bore the king's (Louis XV's) likeness and weighed 6.75g (Figure 1). Thus, 3000 livres is just under 30 ounces (1.86lbs) of coins.

Le Nicolais and Company solved their problem like many of their contemporaries – and, indeed, many of their predecessors in prior centuries. They wrote a bill of exchange: a negotiable instrument authorizing payment of a certain sum to a particular individual (Figure 1, right). The note was 'accepted', or verified in blockchain parlance, by the bank or merchant on whom the note was drawn. Once accepted, the payee could pass the note along to another person or hold it to maturity. Passing the note or transferring it to another owner before maturity meant exchanging it for less than its face value. In our example, M. Morange, a Paris merchant, accepted the note.

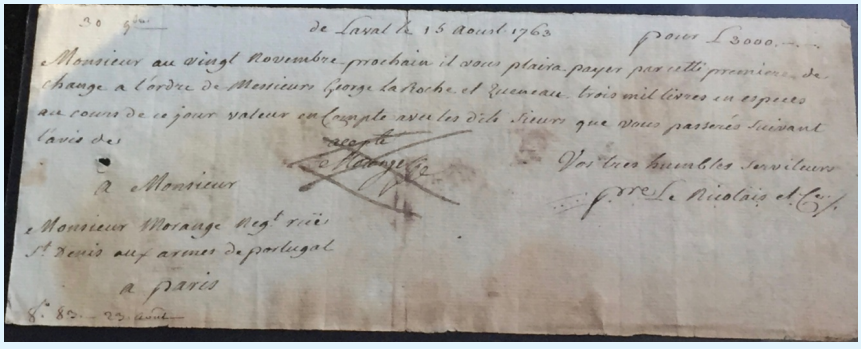
In an era of chronic illiquidity and inelastic credit with no central bank, discounted bills of exchange freely circulated, much like paper money today. Markets existed in all major cities in which merchants regularly accepted and discounted these bills of exchange. Each step in the value transfer chain requires trust – although in an era before instant communication, credit reporting bureaus, and deposit insurance – this was largely a matter of personal networks. M. Morange was vouching for the creditworthiness of Le Nicolais and Company – not just to the payee (La Roche and Queneau), but to every other person in the subsequent value chain. He likely was personally known to the community of Paris merchants and bankers who at some point handled this note. Significantly, each trusted that M. Morange himself was creditworthy. Blockchain replaces the personal network with digitized verification – or proof of work in an unpermissioned distributed ledger – in order to transfer value.

Our 18th century blockchain was kicked off almost immediately after the note was written and reached Paris. Indeed, the reverse of this note is a kind of public access blockchain or recorded history of the note's existence: La Roche and Queneau paid it over M. Vallienne on August 19, 1763. He, in turn, passed it to Mr. Granger, four days later. As far as we can tell, M. Granger was the final recipient: he received his 3000 livres (in coin) on November 20, 1763 from M. Morange. He canceled the note by crossing out his signature.

Finally, this note was not recorded or taxed by the royal authorities. In later years, bills of exchange were regularly taxed. Often taxes were applied to the underlying paper, which might have a special watermark or be stamped with a royal cipher or seal. This paper could only be purchased at official stationers.

FIGURE 1

French bill of exchange, 1763



French, Louis d'or, 1726

Source: Abate collection

[1] All the notes and coins in this piece are from J. Abate's collection.
[2] *The Great Fear of 1789*, G. Lefebvre, Pantheon Books, 1973. Translated from the French by Joan While.

Crypto currencies as a case study in adoption

Much of the focus of crypto technologies has been on crypto currencies as a sovereign-free alternative to 'fiat' currencies. Because crypto currencies are the most well developed and widely used crypto technologies at this point, they make a useful case study for understanding some of the advantages, disadvantages and potential uses of crypto technology in other areas. Crypto currency is a specific use of blockchain and distributed ledger technology. It is a unit of account encoded on a blockchain that is used to transfer value, much like electronic cash. Crypto currency is a form of non-sovereign money, that is, a means of exchange that is not backed by laws and the tax collecting authority of a government. Thus, while it may be accepted as a medium of exchange, unlike sovereign 'fiat' currencies, it is not legal tender required for tax payments and whose acceptance in private transactions usually is legally mandated. Crypto enthusiasts might be surprised to learn that similar instruments have been around in some form for centuries and that the near-complete absence of private money in advanced economies is probably as much a testament to its checkered past as it is to confidence in fiat money.

Crypto currencies also well illustrate all four of the critical challenges that all crypto technologies face. All non-sovereign monies have had to deal with the problems of trust and acceptance in the absence of support from a sovereign balance sheet and legal authority. Similarly, they have, at some point, confronted sovereign prerogatives related to seigniorage – the interest governments earn from issuing money – tax collection, and regulation of finance and commerce. The related concern of privacy, which runs afoul of government attempts to regulate and tax commerce, also has affected all non-sovereign monies, but crypto currencies face additional privacy concerns related to blockchain records of all transactions stored on publicly viewable distributed ledgers. Furthermore, crypto currencies face the issue of irreversibility in the event that acceptance fails: there is no recourse against issuers in the event no one accepts it.

Necessary traits of money: Trust and acceptance

Any money must possess three key traits: act as a unit of account; be a store of value; and be accepted by others as a medium of exchange. All three traits, but particularly the last two, require trust and, under the right circumstances, can be fulfilled by both sovereign and non-sovereign monies. However, sovereignty can convey a distinct advantage in the second and third traits. The taxing authority of a sovereign gives its liabilities, including its fiat money, value. While that value is intimately tied to the fiscal strength of the sovereign's balance sheet and tax base – a concern raised by many crypto currency advocates – in most countries, at most times, the faith and credit of a sovereign bestows some level of value to its currency. More importantly, the sovereign's power to insist that taxes be paid in its currency or to require that all other transactions within its sovereign domain accept settlement in its legal tender ensures that others will accept it as a means of exchange. Guaranteed acceptance as a means of exchange conveys value.

But sovereign money has not always existed, or existed in sufficient quantities, to meet the needs of commerce, or, on occasion, been trusted. These periods in history gave rise to non-sovereign monies.

Box 2: A brief history of private money[3]

As private money, crypto currency is not new. While several general themes behind the issuance of private money, we consider the two identified below as most relevant to crypto currency: sovereign acceptance and special purpose money.[4]

Sovereign permission

A creditworthy issuer's private money is of little value if the sovereign forbids the existence of any money other than its own. At its most basic level, private money challenges the sovereign's ability to collect taxes, earn seigniorage and regulate financial markets and commerce. This makes crypto – much like its paper money ancestors – vulnerable to regulation and outright bans.

Indeed, consider the 'free banking' period in the US (1816-63) and in Scotland (1716-1845). In both countries, banks were able to issue their own paper. In the US, circulating non-metallic money was mostly privately issued paper by state-chartered banks (Figure 2). These were able to issue convertible notes (that is, into government-issued silver and gold coins) subject to state requirements on reserves, interest rates, and capital. Banks generally were weakly capitalized and had short lifespans, given their tendency to make speculative and illiquid investments in land and railroads. Note issuance, rather than deposits, was often their principal source of financing. Notes regularly traded at a discount to their stated face value in coin, often in relation to the distance to the bank's office (where it could be redeemed for coin).

FIGURE 2

State chartered bank issues, 1850s

Source: Abate collection

The wide distribution of notes and the slowness of information meant that those issued by banks that had already failed might continue to circulate far from the original town of issue. The Federal government stopped this activity during the Civil War, when it imposed a 10% tax on the issuance of notes by state-chartered banks. This not only put an end to the inadequately backed state paper but eliminated any competition for its own, non-convertible notes. Bank-issued paper made a comeback with the National Banking Acts of 1863 and 1864, but from nationally chartered banks that had to back their scrip with US Treasury debt, effectively providing a sovereign backstop.

Most developed countries haven't moved to ban crypto currencies outright. But the ability to move large values outside the view of tax authorities is unlikely to win many fans at the treasuries of developed economies. Crypto currencies – like gold – are treated as an asset subject to capital gains taxes. It is not hard to imagine that some versions of crypto currency with features designed to make it more untraceable will eventually be banned, or at least subjected to intense regulatory scrutiny.

[3] We limit our discussion to paper money whose value is based on trust.
[4] The other two – safekeeping and a lack of trust in the sovereign – we consider in Appendix C.

Special purpose money

The ability to design crypto currency with various features designed for specific activities is also not unique. Instead, special purpose money – some of it even sanctioned by sovereign authorities – also has a long history. Mintage of silver and gold coins was erratic, and throughout the 18th century, there was a persistent shortage of low value copper coins. This led to the creation of low value notes that, once the accumulated value reached a certain level, could be exchanged for coins.[5] In most instances, this paper was not legal tender – only the coins were. Special purpose money was usually local and frequently did not circulate outside a particular town or, in some cases, outside of a prisoner-of-war camp. Issuing local-use currency in prisons was also a security measure in that prisoners would not be able to bribe guards or have the financial resources for escaping. An extreme version of limited purpose money was issued by authorities in towns under military siege (Figure 3.).

FIGURE 3

French, Siege of Lyons, August 9 – October 9, 1793

Source: Abate collection

Acceptance and trust

Non-sovereign money is not legal tender…

Non-sovereign currencies are at a distinct disadvantage, as their value and their acceptance by others cannot be guaranteed. Bills of exchange and 'free banking' notes derived their initial value from trust in the solvency of the issuer and belief that others would accept them in future transactions. As acceptance of these non-sovereign monies grew, both their use as media of exchange and the value of their acceptance increased. But non-sovereign monies' value proved fragile: without taxation authority and sovereign enforcement of acceptance, privately issued currencies were subject to perceptions (and the reality) of issuer solvency. Loss of confidence could lead to instantaneous collapse in acceptability as a medium of exchange and impossibility of redemption if the issuer was insolvent, a likely consequence of a run on the issuer (eg, the run on the South Sea Company at the heart of the South Sea bubble).[6]

…and trust that it will be accepted by others is a key hurdle

Trust that a crypto currency will be accepted by others is the key hurdle for adoption and its sole source of value. As with all non-sovereign currencies, acceptance is a fragile equilibrium without a sovereign guarantee. Indeed, sovereigns are competitors with the potential to suppress acceptance of challengers to their own fiat issues. But crypto currencies face acceptance challenges that other non-sovereign monies have not. Previous non-sovereign currencies had either intrinsic value (commodity money) or the backing of an assumed solvent entity that guaranteed repayment in the event others failed to accept its scrip. Additionally, paper non-sovereign monies guaranteed anonymity, whereas the public distributed ledgers of crypto currencies broadcast the history of all transactions recorded in the blockchain.

Crypto currencies are backed by no one, and there is no recourse if acceptance by others does not take hold. A finite supply of tokens is infinitely too much if no one accepts them. If a crypto currency is accepted by others as a medium of exchange, its value will be dictated by its

[5] See, *Stuff and Money in the Time of the French Revolution*, R. Spang, Harvard University Press, 2015
[6] See Appendix C.

supply and pool of users' transactions. Yet, just like past examples of sovereign money, this is a fragile equilibrium. Endemic frauds[7] or robberies via hacking may undermine confidence in a crypto currency as a store of value, and its acceptance by others. But unlike previous sovereign monies, there is no recourse in the event that acceptance evaporates. With commodity monies, the intrinsic value of the money is a backstop to its value. In prior cases of non-sovereign paper money, the recovery value of its issuers' assets (if any) was a backstop to value. Crypto currencies' value comes only from acceptance by others.

Crypto currency is vulnerable to sovereign suppression…

Crypto currency acceptance also is at acute threat from sovereign suppression. Sovereigns earn seigniorage from issuance of their own currencies, and the sums can be substantial: at the peak of its balance sheet expansion, the Federal Reserve remitted nearly $100bn to the US Treasury in 2015.[8] But crypto currencies' potential for anonymity is an even greater threat to sovereigns by better facilitating commerce the government forbids (eg, narcotics, arms) and hiding commerce the government taxes (eg, income, payments). While identification of individuals' public keys in the blockchain is feasible, unmasking privacy in crypto currencies, it is resource intensive and may be beyond the abilities of many less developed countries. Further, new crypto technologies are emerging that claim to obscure transaction identities completely. As a result of these threats, several governments have moved to partially or fully ban use of crypto currencies in their countries, including Bangladesh, Bolivia, China, Ecuador, Iceland, India, Nigeria, and Venezuela.[9]

Crypto currencies as a threat to themselves

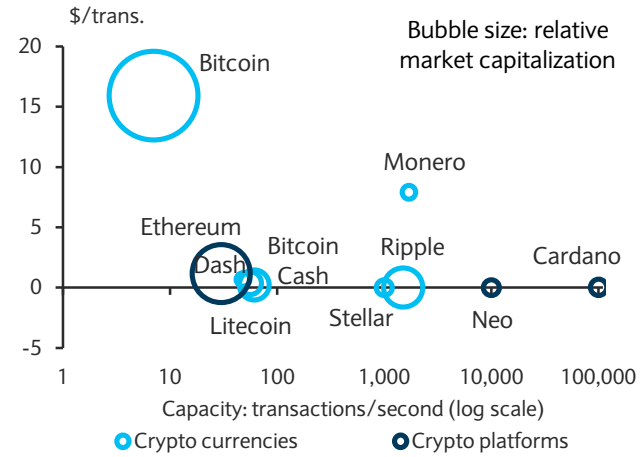
…and competition from other crypto versions

Furthermore, like most species, crypto currencies face the greatest danger from their own kind: while any individual crypto currency may have a fixed supply, the potential supply of new, faster-transacting, lower-cost, more secure competitors is infinite. If a rival with superior transactional characteristics attracts sufficient acceptance, a tipping point reaction may lead to a collapse in use (and value) of an incumbent crypto currency.

2017 was a pivotal year for crypto currencies and technologies that illustrates well the tradeoffs between incumbency and innovation in the battle for acceptance. Figure 4 plots for ten crypto currencies with the largest market capitalizations – denoted by bubble size and used here as a proxy for degree of acceptance – their respective estimated peak transaction capacity versus transaction costs. For reference, the VISA interchange network processes 2,000 transactions per second at a cost of 0.05-1.9% of the transaction, depending on the merchant type and jurisdiction, and claims a peak capacity of 56,000 per second. While Bitcoin benefits from incumbency and name recognition, its transaction capacity and cost make it a far inferior medium of exchange relative to newer entrants. Bitcoin's slow speed and high costs led it last year to create Bitcoin Cash, which is on par with early rival efforts to address Bitcoin's speed and cost issues, Dash and Litecoin. But those three lag far behind Ripple and Stellar, which were developed specifically to be cheaper, high-volume international payment systems. Ethereum, the second largest crypto currency, presented a different alternative: rather than focus on speed and capacity – issues its developers are working to address – it offers a fully integrated crypto platform that allows for 'smart contracts', decentralized applications and organizations, and the potential for a user-defined 'smart economy'. This value proposition led to rapid uptake of its underlying currency, ether. Neo and Cardano have followed Ethereum's lead as crypto platforms, but each with its own twist: Neo aims to be regulatory compliant by enforcing digital identities, while Cardano boasts a peer-reviewed process that attempts to learn from the shortcomings of previous crypto technology iterations.

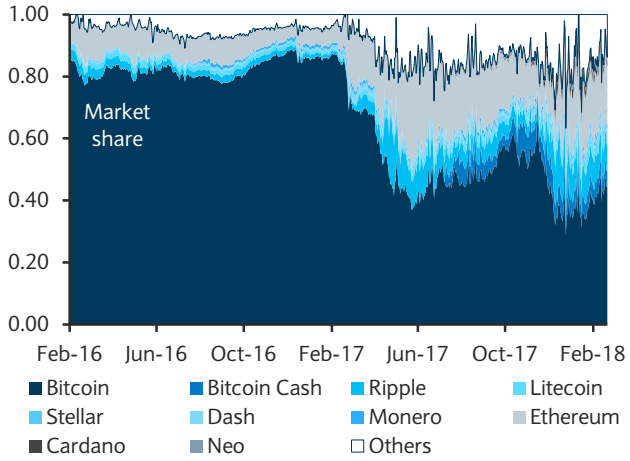
[7] "A company for carrying out an undertaking of great advantage, but nobody to know what it is", unknown pamphleteer in reference to a (likely fraudulent) venture at the time South Seas Company shares were inflating, 1720.
[8] 'Fed 2017 profit payments to Treasury fall to $80.2 billion,' *Reuters*, 10 January 2018.
[9] 'Crypto currencies by country,' *Dividend Magazine*, ThompsonReuters, October 2017.

FIGURE 4
Crypto currencies: market capitalization, peak transaction capacity and average transaction cost



Notes: Average transaction cost is based on most recent 90-day average, except Cardano, Dash, Neo, and Stellar, for which it is based on algorithm pricing terms.
Source: BitInfoCharts.com, Cardanodocs.com, Dash.org, docs.neo.org, Hackernoon, TheMotleyFool, and www.stellar.org.

FIGURE 5
Peak daily transactions and costs, various crypto currencies



Source: Coinmarketcap.com

Monero, a crypto currency, has gone in the opposite direction: it is specifically designed to have untraceable users and transactions, addressing the potential anonymity gaps of other crypto technologies, but potentially attracting greater sovereign suppression.

Each of these innovations – crypto platforms, modes of regulatory compliance, increased privacy, greater transaction capacities, and lower costs – shows the potential of crypto currencies to adapt to meet market place needs, but ultimately each still faces the hurdles presented by the four critical challenges and incumbency of existing technologies.

Crypto currencies are evolving into specific use money…

Indeed, the past year illustrates why we think it will be difficult for any single crypto currency to become the dominant medium of exchange. It is relatively easy to create a new crypto currency that is designed to meet a specific requirement or need. Historically, special purpose money typically has a short lifespan. Instead, as anachronistic as paper money is, its ability to multi-task means that it meets most of the various needs that crypto currencies purport to solve. Paper is private; transactions are anonymous; and, to some extent, regulations exist to enable officials to keep track (somewhat) of at least large values. But crypto currency appears to be evolving in the opposite direction. The proliferation of specific purpose crypto currency is the electronic equivalent of using euros to make online purchases, sterling to buy securities and dollars for in-person transactions. Initial coin offerings are an extreme illustration of this: they are the functional equivalent to store-issued coupons. Maintaining an accounting framework to keep track of multiple single-function currencies is highly inefficient. For a dominant crypto currency to emerge – for either legitimate or illicit activities – its functional use must be broad enough to challenge paper, specifically, large denomination bills such as the $100 and EUR500. Instead, our sense of recent developments is that crypto currencies are moving in the opposite direction; this fracturing based on use makes it unlikely one unit will come to dominate.

…and competing to establish acceptance

Figure 5 illustrates simultaneously the power of first-mover advantage in terms of acceptance and the threat to incumbency from innovation.[10] Bitcoin began 2017 with nearly a 90% share of

[10] One caveat to consider in interpreting these data is that it is difficult to separate out transactions that are "investments" from those where the crypto is used as a medium of exchange. Perhaps a better measure – assuming one could be created – would be to look at purchases of goods and services made with crypto. An example is the Federal Reserve Bank of Boston's *Survey of Consumer Payment Choice*.

the total crypto currency universe market capitalization, but by early 2018 that share had dipped (briefly) below 30% before recovering more recently to about 45%. Smaller incumbents such as Ethereum and Ripple, or Bitcoin fork Bitcoin Cash, with better technologies have taken the most market share over the last year (with respective gains of 14pt, 8pt and 5pt), but new entrants such as Neo and Cardano have come from nowhere in mid-2017 to market capitalization shares of 1.5-2.0% based on their technological offerings.[11] But while these start-ups show how innovation threatens incumbency, the decline in market share of other, smaller rivals from nearly a quarter of the total universe to less than 10% of total market capitalization illustrates that acceptance by others ultimately is the source of value for any crypto currency.

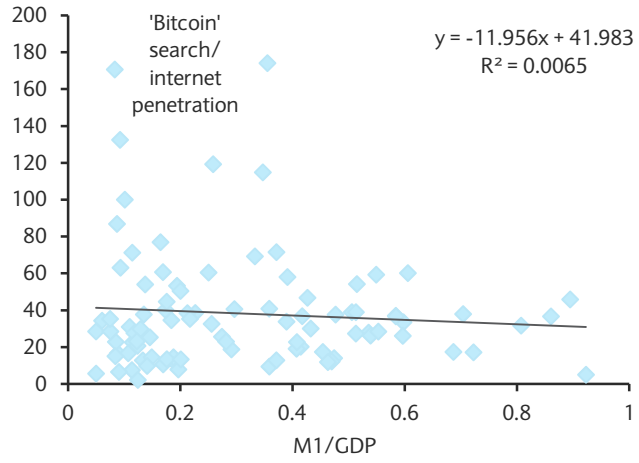
A cross-country study of factors behind adoption

A cross-country study of Bitcoin uptake offers insights into the motives and challenges to adoption of crypto technologies – not just currencies – and the likely pool of end-users that may define crypto currencies' potential value. We find that adoption as a currency is more likely in environments with low levels of trust and development; where crypto currencies may be more trustworthy than incumbent money or offer asset diversification not feasible in local markets; where sovereigns may have less ability to enforce regulation; and where the cost of irreversibility is outweighed by gains in trust, diversification or privacy. These findings suggest that crypto currencies are unlikely to gain widespread acceptance outside of underdeveloped economies. In contrast, we find that the price of crypto currencies appears to be driven by speculative behaviour in developed economies that is dependent on the flow of new entrants who show signs of running out.

While we do not have data on Bitcoin use by country, we can use Google Trends' search intensity of 'Bitcoin' as a proxy for interest in and potential use by country.[12] Figure 6 charts the dispersed but exponentially increasing relationship between internet penetration and Bitcoin interest by country. The relationship testifies to the effect of network externalities: the more connected people are, the faster and easier information and interest spreads. But the dispersion illustrates that other factors clearly play a role in Bitcoin interest. To account for the non-linear network effects, we use search interest inversely weighted by (divided by) internet penetration as a proxy for Bitcoin interest by country in exploring the other factors.

FIGURE 6

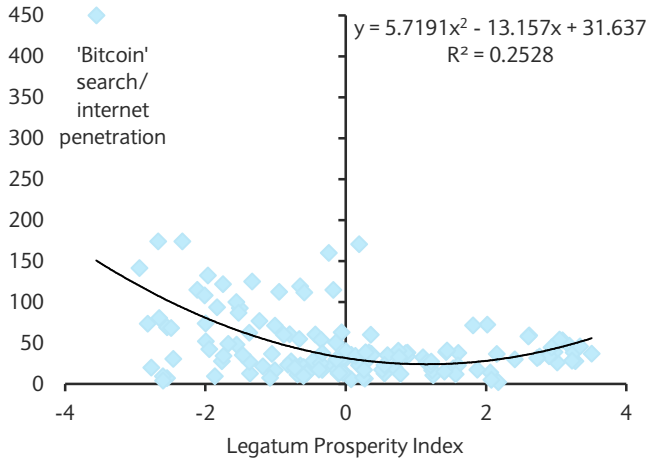
Weighted Bitcoin interest vs. intensity of money use, by country



Source: Google Trends, IMF, ITC Facts and Figures 2017, International Telecommunications Union

FIGURE 7

Weighted Bitcoin interest vs. societal welfare, by country



Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union, Legatum Institute

[11] Cardano and Neo existed before 2017, but the former did not begin to trade actively until 2017, and the latter underwent a rebranding and re-introduction with new technologies in 2017.

[12] A Bank of Canada study suggests a reasonable degree of correlation between Bitcoin-related Google searches and actual transactions; see Christopher S. Henry & Kim P. Huynh & Gradon Nicholls, *Bitcoin Awareness and Usage in Canada*, Staff Working Papers 17-56, Bank of Canada, November 12, 2017.

Is a fixed supply important?

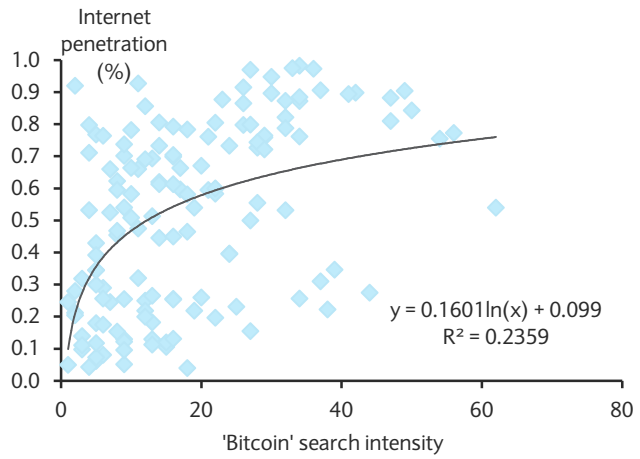
Crypto currency advocates often point to their fixed supply (or fixed growth rate) as a key attraction, as it removes the ability of governments to undermine their value through inflation. But there appears to be little relationship between Bitcoin interest across countries and their respective rates of inflation (Figure 7). Nor is there a clear relationship across countries between interest in Bitcoin and the volatility of inflation (not shown). But that does not mean that there is no relationship between Bitcoin interest and the local money supply. Figure 8 shows the weak but negative relationship between M1/GDP – the monetary intensity of economic activity – and interest in Bitcoin. While inflation may not be the cause, countries with low usage of the local currency relative to economic activity appear more likely to have higher interest in Bitcoin.

Interest in Bitcoin is highest in both high and low welfare societies …

A much stronger, but nonlinear, relationship exists between Bitcoin interest and of societal welfare. Figure 7 plots weighted interest in Bitcoin versus the Legatum Prosperity Index, a broad measure of societal welfare that spans the economy, governance, opportunity, education, health, personal freedoms, safety, and social capital.[13] Bitcoin interest is highest at both ends of the spectrum: the highest and lowest welfare societies, but lowest on average in medium welfare countries. The dispersion is highest in countries with below-average welfare.

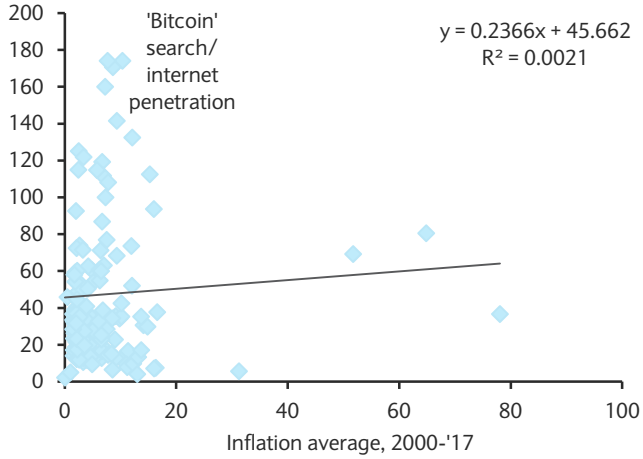
Looking into the subcomponents of societal welfare yields surprising insights into the sources of the two tails of interest. Personal freedoms, a measure of government intervention in people's lives, often touted as a benefit of crypto technologies in general and crypto currencies in specific, appears wholly unrelated to interest in Bitcoin across countries (Figure 10). Economic strength and governance (not shown) turn out to be weak predictors of interest, as well. But institutional development does appear important, at least for the lower tail of prosperous countries. The strongest relationship to interest in Bitcoin – by tightness of fit – is with country health scores, a measure that often proxies for institutional development and robustness (Figure 11). The closeness of fit appears driven by the lower tail of the distribution; ie, below a certain threshold the lower health outcomes, the greater the interest in Bitcoin, but above that threshold there is little difference in interest. Development issues likely also help to explain the relatively tight relationship with the entrepreneurship and opportunity subindex (Figure 12). In countries with few opportunities for or means of investment, crypto currencies may be one of the few ways to diversify

FIGURE 8
'Bitcoin' searches vs. internet penetration, by country



Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union

FIGURE 9
Weighted Bitcoin interest vs. inflation, by country

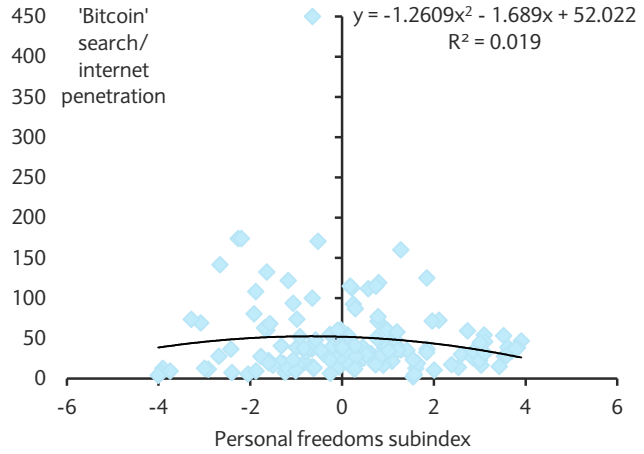


Source: Google Trends, IMF, ITC Facts and Figures 2017, International Telecommunications Union

[13] The Legatum Prosperity Index is a measure of country-level social welfare produced by the Legatum Institute. It measures welfare based on 110 questions divided into eight categories (subindices): Economy, Entrepreneurship and Opportunity, Governance, Education, Health, Safety and Security, Personal Freedoms, and Social Capital, the last being a measure of the 'glue' of society, particularly trust in fellow citizens and institutions.

FIGURE 10

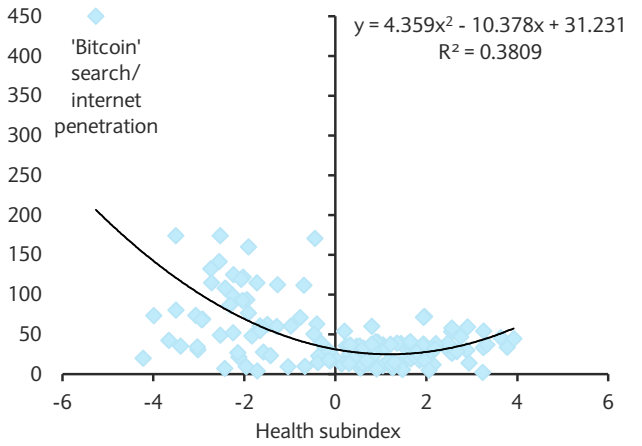
Weighted Bitcoin interest vs. personal freedom, by country



Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union, Legatum Institute

FIGURE 11

Weighted Bitcoin interest vs. health, by country



Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union, Legatum Institute

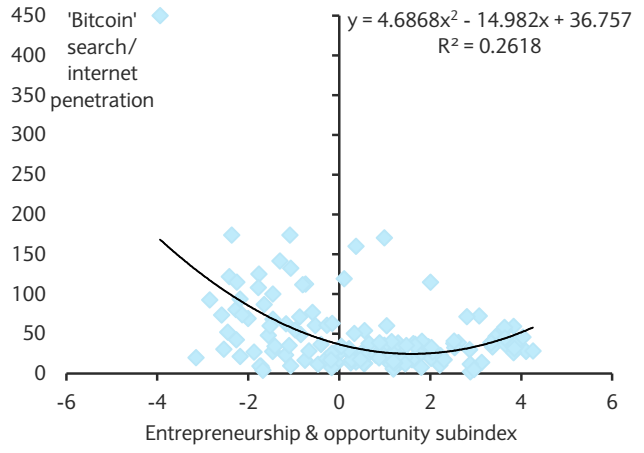
savings out of domestic assets. The somewhat higher level of interest in the highest entrepreneurship and opportunity societies – which also are the richest – suggests high-risk tolerance speculation may play a role, as does the high concentration of holdings in most crypto currencies.[14]

…and is related to issues of trust and safety

Beyond institutional development and opportunities, Bitcoin interest across countries is most related to issues of trust and safety, again particularly in the lower end of the development spectrum. Figure 13 plots the relationship of weighted Bitcoin interest with the Legatum safety and security subindex, and Figure 14 shows the relationship to social capital, a measure of trust within a society. While the relationship between Bitcoin interest and safety or trust is relatively flat for above average countries, it is increasingly negative for countries with below-average safety and trust.

FIGURE 12

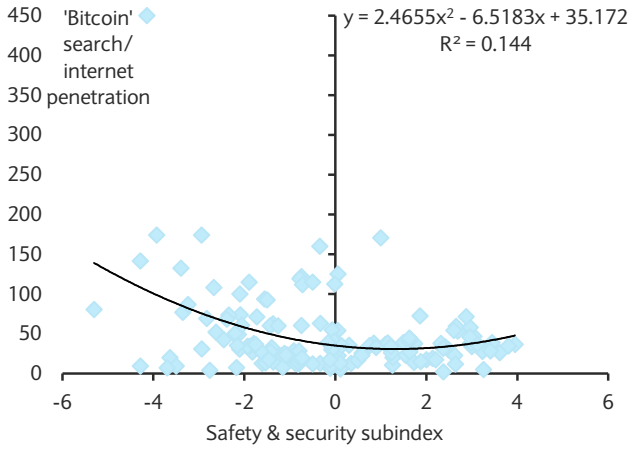
Weighted Bitcoin interest vs. entrepreneurship and opportunity, by country



Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union, Legatum Institute

FIGURE 13

Weighted Bitcoin interest vs. safety and security, by country

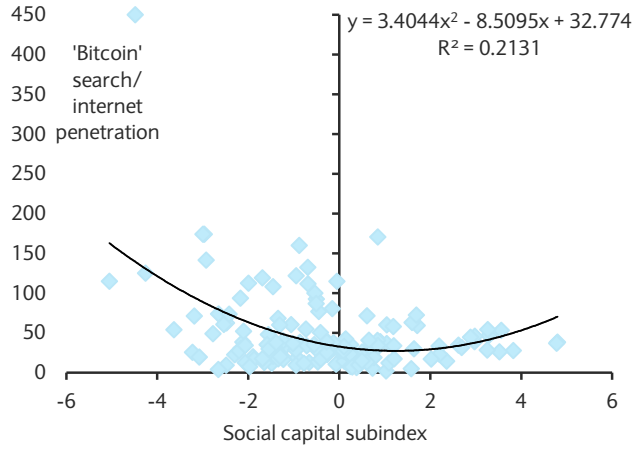


Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union, Legatum Institute

[14] Under constant relative risk aversion, risk tolerance rises with wealth. According to Bitinfocharts.com, the top 100 holders of Bitcoin hold 18.6% of its market capitalization; the same figures for Bitcoin Cash and Litecoin are 24.5% and 45.2%, respectively.

FIGURE 14

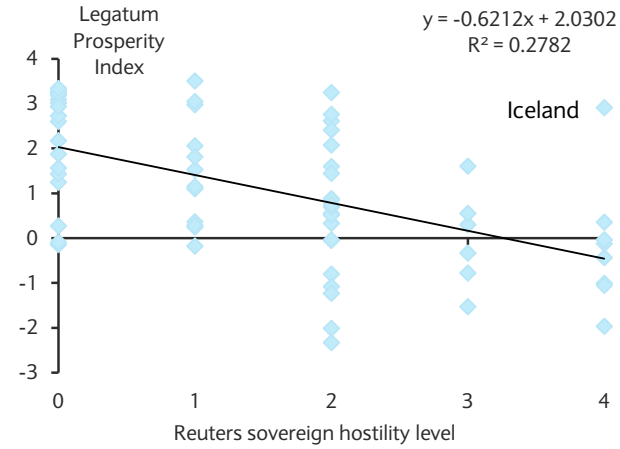
Weighted Bitcoin interest vs. social capital, by country



Source: Google Trends, ITC Facts and Figures 2017, International Telecommunications Union, Legatum Institute

FIGURE 15

Societal welfare vs. state hostility to crypto currencies, by country



Source: Legatum Institute, ThompsonReuters

The most likely uses for crypto currency are in low-trust, low-security environments

These analyses suggest that the most likely uses for crypto currencies – and crypto technologies such as smart contracts – are in low-trust, low-security environments with little institutional development and opportunity for alternatives. These likely are failed or weak states, or criminal enterprises, where trust, security and alternatives are in short supply. Without adoption by major central banks, demand for crypto currencies in well-functioning societies with strong institutions, rule of law and systems for adjudication is likely to remain either evangelical or speculative.

Yet governments in countries with low trust are unlikely to accept rejection of their currencies by their citizens without a fight. Figure 15 plots countries' Legatum Prosperity score versus a ThompsonReuters categorization of governments' legal stances towards crypto currencies from complete acceptance (0) to banning (4).[15] Nearly all the countries that ban crypto currencies are in the bottom half of the Legatum index, with Iceland – the only OECD country with capital controls – a notable exception. In contrast, sovereigns with strong institutions and payment and legal systems – thus little threatened by crypto currency adoption – are open to them.

Beyond crypto: Prospective applications

How might blockchain and distributed ledger technology be applied outside of currencies?

Blockchain and distributed ledger technologies have a large number of potential applications. Although using crypto currencies as a substitute for fiat money is the use case that has received the most attention, others include smart contracts, asset custody, and payments. In each use case, there are inefficiencies in the status quo that are theoretically addressable using these technologies. However, in none of these cases is the technology ready for application now. There are significant hurdles that would need to be surmounted, such as improvements in speed and process or the development of new trade protocols. In some cases, the potential gain likely justifies the required investment, although in most of the financial market use cases, the *status quo* appears to be efficient enough that we do not expect any medium-term deployment of these technologies.

Fiat money substitutes

- Recent trends in crypto currencies suggest a move towards 'specialty' transactions vehicles like those on 'smart economy' platforms that may speed up international

[15] 'Crypto currencies by country,' *Dividend Magazine*, ThompsonReuters, October 2017.

payments, or privacy-enhancing electronic currencies that may be more appealing for illicit activities.

- Crypto currency is ideally suited for use in low trust environments. It is useful to move large values unobtrusively and as a means of tax and regulatory evasion.
- But by directly challenging the authorities' monopoly on money creation, crypto fiat substitutes are vulnerable to regulation and outright bans.

Recent developments in crypto currency technology suggest that trend adoption may come from specialty transactions demand. Broad adoption of crypto currency as a means for making fast international payments may develop on "smart economy" platforms such as Ethereum, Neo or Cardano, or as an international payment mechanism such as Ripple and Stellar. Ethereum, however, was specifically created as an institution-free platform for commerce and communication, hence likely would come into direct conflict with regulators. So, too is the strategy of newer crypto currency entrants Monero and Zcash, both of whom provided enhanced transaction privacy, masking participants and amounts transacted. Neo and, to a lesser extent, Cardano, in contrast, are designed to be compliant with regulators from the start. Neo's connections to and backing by the titans of China's economy have led some to speculate that it is positioning itself for adoption by the Chinese state.[16] But adoption of a crypto platform need not imply adoption of its underlying currency over the sovereign's own fiat currency.

We do not believe any crypto currency is likely to become legal tender in a developed economy

More importantly, we struggle to see how any government would willingly seek to undermine its sovereign authority by allowing an alternative unit of account to become a substitute for its issuance, threatening its seignorage and tax collection. As such, we believe that no crypto currency is ever likely to become legal tender in a developed economy.

Instead, we suspect that crypto's appeal is higher in the underground economy, which has always been cash-reliant, given the un-traceability of currency. But moving currency has become increasingly difficult. The US stopped printing large denomination notes (of $500 and $1000) by the late 1960s in an effort to reduce tax evasion and crime. For similar reasons, the ECB recently stopped printing the EUR500 note. As the supply of large denomination notes disappears, other means of transporting high values have increased. But even diamonds have become harder to smuggle, as recent rules marking stones were introduced in the last decade. Unsurprisingly, this has created demand for an alternative to paper currency that is discreet and hidden from the view of authorities.

Indeed, although criminal activities tend to be cash-intensive businesses at the retail level, the practical limitations on currency seem to be reducing the attachment to paper at the wholesale level, where cash mixes undetected with legitimate money and transactions. This might explain why the Drug Enforcement Agency's seizures of bulk cash have declined nearly 60% since 2010. For what's estimated to be a $64bn (illegal) drug economy that, at least at the retail end of the business, is very cash intensive, the amount of currency seized is surprisingly small. Only $337mn in bulk cash – or 0.5% of US drug "GDP" – was seized by the DEA in 2016.[17] The DEA notes that low bulk cash confiscation rates are partially tied to the fact that at the wholesale level, cash has been pushed aside in favour of other ways for hiding and laundering illicit money.

[16] 'Neo versus Ethereum: Why NEO might be 2018's strongest cryptocurrency,' Noam Levenson, Hackernoon, 6 December 2017.
[17] See "Drug Enforcement Agency: 2017 National Drug Threat Assessment Report".

Box 3: Frictionless money laundering

A cottage industry has developed that allows owners of "dirty" Bitcoins to convert them into legitimate, "clean" crypto currency. Laundering Bitcoins generally takes two forms – although we suspect that there are other, more sophisticated methods. In one, the Bitcoin proceeds from illegal activity are mixed with clean ones from other investors on an exchange though an intermediary. The intermediary "swaps" coins across different owners, so that the clean ones are returned to the owner of the dirty coins, which are then distributed throughout the exchange ("tumbling"). Alternatively, dirty coins are spent on low value transactions, and the change from the transaction is returned to another address (a process known as "peeling"). This new address repeats the same transaction, with the change returned successively to different addresses.

Smart contracts

- Blockchain and smart contracts can significantly reduce record keeping and verification burdens by shifting the recordkeeping from the counterparties in a transaction to the asset itself. The associated efficiencies are potentially meaningful where transaction volume is extremely high, such as tri-party repo.
- Replicating the flexibility built into the current system is an important hurdle to adoption. While true for even the simplest tri-party repo, more advanced use cases such as ABS transactions require even more judgement.

Built into most financial transactions is a multi-step verification process, which establishes who owns the asset, whether the owner has permission to sell it, where the asset is located or stored, along with instructions on its transfer. In most cases, this requires multiple ledger entries across different counterparties in an asset transfer, including the buyer, seller and custodian. These records need to be cross- and double-checked before and after the asset's transfer can be completed.

But ownership and transfer details can be encoded into the asset's 'DNA' via a permissioned blockchain. The public ledger programmed into the asset's DNA eliminates the need for cross-checking records across multiple corporate ledgers. Smart contracts can be designed to execute automatically, linking cash and trading accounts. Significantly, as the blockchain establishes a publicly visible record of ownership, the asset record does not have to sit in an account at a custodian bank for safekeeping. This fundamentally changes the nature of custodial relationships, as securities lending – for *any* blockchained asset – can now occur outside of a custody bank that traditionally has provided safekeeping and ownership records. Automatically executing contracts can be designed to perform a variety of functions that traditionally have been done by custody banks or exchanges: from calculating and collecting variation margin to asset transfers and securities lending. Blockchain and smart contracts mean that recordkeeping moves from the counterparties and the custody agent to the asset itself.

Tri-party repo

Can tri-party repo be blockchained?

Consider the specific case of tri-party repurchase agreements (repo). Repo is a collateralized loan where cash is exchanged for securities (such as Treasuries) and then reversed the following day. In a tri-party transaction, the cash and collateral move within an account or 'box' maintained on the balance sheet of the clearing bank. This is considerably more efficient than the alternative of delivery-versus-payment, where the counterparties have to make their own transfer arrangements.

After both counterparties agree to an exchange, their back offices contact the clearing bank to move the respective assets. But before the actual movement of cash and collateral, the

lender, borrower, and the clearing bank each have to confirm the location of the cash and collateral, initiating a double-checking process that spans three separately maintained ledgers. Although three-way trade confirmation is automated, it still requires some effort to prevent mistakes.

Now imagine each Treasury CUSIP existed on a blockchain. The blockchain would be updated with the owner's details, including bank information. The agreement to exchange cash and the CUSIP would represent a new block on the issue's blockchain. And since the cash and collateral both reside in a box at the clearing bank, it should be a relatively simple matter linking both sides of the transaction via the blockchain. A smart contract could be designed to unwind (reverse) the trade after exactly 24 hours.

The self-executing contract means that trade might be programmed to unwind at different times throughout the day. This frees cash and collateral to move throughout the day, rather than one specific time in the afternoon. This is important to some institutions: US Federal Home Loan Banks have an aversion to repo because their unwinding cash is not returned until late in the following afternoon, although their own cash needs are highest early in the morning. The free movement of cash and collateral throughout the day suggests that, at least in theory, it might be possible for an intra-day repo market to develop.

One hurdle to adoption is that there is flexibility built into the current system that would be important to maintain. In the *status quo*, there is the ability to modify the collateral pledged – for example, substituting one CUSIP for another – before the cash and securities are exchanged at the end of the day. Dealers and the clearing bank have developed sophisticated programs that can automatically do these substitutions based on an optimization algorithm. Significant investment would be required to convert existing collateral substitution programs into smart contracts, particularly given the importance of repo markets to market participants and regulators.

Smart contracts may struggle to handle collateral substitution...

At the moment, there is only one tri-party clearing bank and the prospects for new entrants are very low given the high cost of entry. We suspect the burden of converting tri-party to blockchain would initially fall to the clearing bank. But as this bank has no competitors, it would be easy for it to recoup its conversion costs. Most likely this would be accomplished via a widening in bid-ask spreads in the tri-party market.

ABS

A portfolio of assets – for example, credit cards – is assembled and financed through the issuance of asset backed debt. The portfolio is over-collateralized; that is, it holds more loans than the amount of debt issued. This is not the only type of securitization, of course. Other structures use subordinated debt in combination with a reserve (cash account) and excess spread. Asset-backed securities (ABS) typically are purchased by a variety of investors including money managers, banks, insurance companies, and, when funded with CP, money market funds. We consider some of the operational roles and plumbing details in a simple credit card (master trust) asset-backed program.

A servicer's role is to manage the credit card portfolio, as well as its associated cash flows. It processes the collection of the loan payments and remits them to a trustee, which then pays bondholders. In a credit card master trust, the servicer also determines the level of excess collateral the portfolio will maintain against its outstanding debt. The master trust servicer also can remove non-performing loans, replacing them with other, performing loans by requesting the borrower to post more collateral or retire debt. And the borrower also can post additional collateral, for example, to issue more ABS debt or to replace loans that are paid off.

So, where might blockchain fit in?

It is possible to put all credit card loans onto a blockchain. Each loan might have an embedded code identifying the originator and the note holder. These details could be used

to design a smart contract that automatically directs the loan payments to the asset-backed debt holders' accounts. In practice, we suspect that loan payments would be directed to a central, distribution account that itself would be governed by its own smart contract linked to a blockchain embedded into the asset-backed debt. It would be relatively simple to design a smart contract to distribute payments automatically to the asset-backed debt holders according to some pre-determined calendar schedule, much like automatic bill-pay. In theory, this removes the need for a servicer to process loan payments.

...Or collect on delinquent receivables in a credit card trust

But it may be difficult for blockchain to address some of the credit card master trust servicers' other functions. Designing smart contracts that automatically replace collateral as it pays down or is removed from the trust without some amount of judgment is considerably more challenging. And while blockchain and smart contracts could efficiently distribute incoming debt payments to ABS holders, it is unclear how the technology could be structured to collect on delinquent receivables or sell charged-off receivables. Separately, a blockchain would not remove the need for a trustee whose responsibility it is to represent noteholders in cases where there is a breach of trust disagreement such as the default of the servicer.

Asset custody

- Blockchain can be used to establish the provenance of an asset and prevent its transfer. This could reduce theft and reduce transaction costs associated with verifying ownership, such as title insurance.
- The key hurdle is converting asset holdings into blockchained digital registries, although the costs vary by asset, as some aggregated databases already exist, such as for real estate. In those cases, we see potential for nearer-term adoption.

Blockchain can establish asset provenance

Beyond simple recordkeeping, blockchain can be used to establish the provenance of an asset and prevent or authorize its transfer. In the case of an asset that doesn't change hands frequently, like a home, it is easy to develop a digital contract between the buyer and seller than updates the asset's blockchain. This could be linked directly with a bank whose mortgage financing would also be encoded into the home's blockchain. Similarly, mortgage payments encoded on the same blockchain could be processed directly into the servicer's accounts. Moreover, the property's chain would contain all tax data including liens and deed restrictions. In this example, there theoretically would be little need to pay someone to do a title search or buy title insurance.

New York City real estate

What role does title insurance play in a world with blockchained deeds?

The New York City Department of Finance maintains an online registry of real estate transactions dating back to 1966. The Automated City Register Information System (ACRIS) provides information on real estate transactions that, in addition to the names of the buyer and seller, includes data on the mortgage (amount and noteholder), as well as information about transfer taxes paid on the sale. The data also include the sales price of the unit and if the mortgage has been paid off. This database is searchable by name, location, and type of form (mortgage payoff data, for example, are recorded on the UCC financing statement. In theory, as these data are all readily accessible, there is little need to hire someone to do a title search or for the buyer to purchase title insurance.

As the information is already effectively in a centralized ledger, the next step of converting these records into a blockchain is relatively easy. Of course, not all localities have detailed, searchable real estate records, so the initial hurdle of converting paper records maintained at the town hall is likely to be expensive. But once this occurs, we expect the next step of blockhaining title transfers, school taxes, and mortgage payments quickly to follow.

But just as the blockchain be can used to record and authorize asset transfers, it can also prevent the movement or resale of assets. On the simplest level, the asset's digital DNA

could be encoded in such a way so that it cannot be resold or transferred outside a small list of authorized individuals. Jewellery or artwork could be registered in such a manner. This might not prevent the asset from being stolen and fenced or resold. But it would make transferring these ill-gotten assets to legitimate buyers much harder. Assets whose provenance is well verified and whose ownership is unequivocally established via the blockchain are theoretically easier to insure, as it would be difficult to bring an offline asset that was previously registered back into a legitimate chain of transactions.

Returning to our Treasury CUSIP blockchain, consider how a "do not transfer code" could be inserted that automatically prevents the sale of the security to buyers whose phone number has a specific area code. Unlike currency, which is transportable over borders, crypto assets might be programmed to become invalid if an attempt is made to use or transfer them improperly or in a sanctioned country.

Settlements

- Blockchain and distributed ledger technology could allow for immediate settlement, eliminating one form of operational risk. In addition, they could eliminate settlement failure or incomplete deliveries.
- However, this might not be desirable. Money laundering and customer identification requirements may require some timing gap in settlement, as does correcting mistakes. Overcoming these hurdles may require new trade protocols, such as different approaches to trusted or known counterparties.

In theory, blockchain and distributed ledger could allow for immediate settlement…

Discussions of Bitcoin and cross-border payments frequently highlight the potential for blockchains and distributed ledgers to eliminate delays in settlement. They point out how long it takes to send a payment from a US bank in dollars to an overseas institution in another currency – and the associated expense. We think that with smart contracts that execute automatically and blockchains linking payments to ownership transfer, immediate settlements are possible.

Immediate settlement eliminates one form of operational risk – settlement risk. This exists when there is a delay between the transaction agreement and the ultimate exchange of cash. Since the 1970s, banks have adopted real-time gross payment settlements in their processing of check and wire payments. While this reduces settlement risk, it is less efficient from the perspective of processing, as it requires significant amounts of intra-day credit.

Settlement failure

Despite significant technological improvements with respect to electronic payments, settlement failures are surprisingly common in some large markets such as Treasuries. Indeed, over the past several years, the volume of failed Treasury deliveries has increased, rising to approximately 4% of average daily trading activity.[18] Based on the distribution and type of incomplete deliveries, our sense is that this increase is tied to a pick-up in delivery instruction errors. Beyond the obvious question of why delivery instruction errors have increased, there is the issue of why technology is not able to solve this. After all, failing to deliver a Treasury as promised incurs a pretty hefty charge, not to mention the client's dissatisfaction. The increasing cost of fails should, in theory, motivate firms to spend more on technology to eliminate these settlement gaps.

Although the precise cause of the increase in incomplete deliveries is not well understood, our sense is that blockchain technology might help reduce their incidence. Smart contracts could, theoretically, eliminate settlement fails by authorizing the immediate release of cash

[18] See *Spontaneous failure*, January 17, 2018.

and Treasuries once certain pre-conditions had been satisfied (for example, upon receipt of a confirmation message).

…but legal and regulatory requirements mean that immediate settlement may not be desirable

That said, even in a post-blockchain world, immediate settlement might not be as optimal as faster settlement, for two reasons. First, because it is difficult to correct mistakes on a blockchain, it might be wise to have a longer "curing" period for settlements. Trades could be reviewed during a brief pre-settlement period to ensure the details are correct before the confirmation codes are sent.

Second, even if there were no risk of mistakes and transactions could be reversed easily, it might still not be possible or desirable for transactions to settle immediately. In many markets, investors are required to check whether the transaction satisfies anti-money laundering (AML) and know your customer (KYC) rules. Of course, it is possible for technology to solve this issue, as well. Firms could establish trusted counterparties whose trades settle immediately, while others go through a more thorough regulatory review process and settle later.

Payments

- Faster payments are possible with blockchain technology, and aspects of the existing payments infrastructure are arcane and impose delays on payments processing.
- But even in the simplest proofs of concept, such as a study at the Bank of Canada over a closed system of inter-bank payments, the current blockchain and DL technology was not much of an improvement over the existing model. More complicated applications, with more meaningful potential gains, would require substantial improvements in technology.

Faster and cheaper payment processing has attracted the most attention from blockchain enthusiasts. Recently, the Bank of Canada studied a proof-of-concept test – Project Jasper – that applied distributed ledger technology to interbank wholesale payments.[19] The BoC was interested in learning if its large value transfer system (LVTS) could eventually shift to a distributed ledger. On average, the BoC processes roughly C$175bn/day in these payments, via roughly 10 transactions every second. These are fairly simple transfers between the reserve accounts of member banks, all within a closed system on the BoC's balance sheet.

Transactions are mostly settled on a real-time gross settlement basis, that is, immediately as they come in. But this requires enormous amounts of liquidity, given the volume of transactions and a natural tendency to delay outflows while accelerating inflows. In the absence of intraday credit, no one would send out payments until they had first received their cash due. At the extreme, this creates a traffic jam: no one is willing to move first, so everyone's payments are held back. Central banks attempt to mitigate these effects by liberally providing intra-day credit – for a cost. That is meant to encourage banks to develop their own strategies that conserve the aggregate amount of liquidity the system needs to process payments. Liquidity savings mechanisms (LSMs) are designed to net down offsetting payments on a multilateral basis at different times throughout the day. But to be able to net down potentially offsetting payments, banks need to delay some outflows long enough to establish a backlog that can be netted against incoming flows. This requires them to determine which payments need to be cleared immediately, ie, on a real-time gross settlement basis, and which can be delayed long enough to build a pool of "net-able" transactions.

The challenge for the designers was first to create a settlement asset, a digital drawing right (DDR) on the BoC. The DDR was equivalent to a transferable reserve account balance, that is, a claim on a deposit at the BoC. The designers used Ethereum. DDRs would be exchanged on a real-time gross settlement basis using simulated data. In addition, the programmers built in LSM algorithms consistent with what banks already use.

[19] See *Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?* J. Chapman, R. Garratt, S. Hendry, A. McCormack, and W. McMahon, Bank of Canada, Financial System Review, June 2017.

Program designers found that they could process about 14 transactions per second using an Ethereum-based DDR. Chapman *et al.* argue that this is probably sufficient to handle average daily processing requirements, but it could become insufficient and might already be so for peak payment flow days. The designers did note that it was possible to overcome the scalability issue by switching to a more centralized ledger that did not rely on consensus based verification. Instead, a distributed ledger that used a trusted 'notary' might eliminate the scalability problem. Designing a LSM for the DDRs using simulated data turned out to be significantly more challenging. As of mid-2017, program designers were still testing the algorithms.

Real-time gross settlement results were somewhat lackluster

Overall, the results from Project Jasper were somewhat lacklustre. Chapman *et al*. note, 'Current versions of distributed ledger technology do not provide an overall net benefit relative to current centralized systems.' Indeed, the results suggest that – at least for interbank payments – the most efficient distributed ledger seems to be one that is fairly narrow in scope and, instead of a broad consensus-based verification mechanism (such as is used in Bitcoin), relies on a single notary that updates a centralized DDR ledger.

FIGURE 16
Prospective applications of blockchain and distributed ledger technology

	Acceptance/Trust	Security/Regulation	Privacy	Irreversibility
Fiat money substitute				
Crypto currency	Acceptance outside low trust activity is likely to be low. Multiple specific-use currency may diffuse demand for crypto, reducing broader acceptance.	Major sovereigns are unlikely ever to grant legal tender status. Some cryptos are designed to be untraceable, which makes outright bans likelier.	Mixed. Newer crypto technologies claim absolute privacy, while first generation crypto technologies are traceable; full privacy may invite sovereign conflict.	In theory, this is no different than for paper currency. But it might be hard to enforce legally, depending on the nature of the transaction.
Smart contracts				
Tri-party repo	Trust unlikely to be an issue, but acceptance will require securities to be converted from book entry to blockchain, meaning acceptance requires overcoming.	All the transactions go through the "box" of one bank and are viewable. In theory, there would be no change over the existing framework.	How anonymous should counterparties be to each other? More fundamentally, how visible should a Treasury CUSIP's blockchain be? Should "write" access be through primary dealers only?	Settlement failure is somewhat frequent, likely reflecting human error. A reversibility process likely would be required, calling into question the value of blockchain efficiency gains.
ABS (credit cards)	No obvious trust issues, but agreement on blockchain format, structure and permissioning may be a hurdle.	Requires putting the credit card loans onto a blockchain. Write access would be controlled by originator and the note holder. But designing a contract that would collect or sell off delinquent receivables might be difficult.	We do not see any obvious issues: individual loans making up the collateral would be anonymous.	Misdirected payments encoded into the blockchain would be hard to correct without an additional offsetting transaction.
Asset custody				
Real estate	High. Records are already moving to electronic registries, so banks and noteholders may have little issue with trust.	Real estate transactions are largely in the public record. But digitization makes it less costly to search records or establish provenance.	We do not see any obvious issues.	Misdirected payments encoded into the blockchain would be hard to correct without an additional offsetting transaction.
Settlements				
Financial assets	High. Much of the delay in settlements results from double- and cross-checking ledgers maintained by the buyer and seller.	In theory, it would be possible to reduce operational risk by eliminating the time delay in settlement.	How anonymous should counterparties be to each other? Likewise, who should have "write" access to the asset's blockchain?	Misdirected payments encoded into the blockchain would be hard to correct without an additional offsetting transaction. This is problematic, given the frequency of delivery instruction errors in some markets. Is it desirable to have a "cure" period,

	Acceptance/Trust	Security/Regulation	Privacy	Irreversibility
				a brief delay in settlement to allow buyers and sellers to correct mistakes before the trade is finalized?
Payments				
Project Jasper	High. Large interbank transfers are limited to central bank deposits among counterparties that presumably share an identifiable encryption code.	High, given the limitation on the ability to transfer money outside the network.	High. As these are interbank payments on a closed system, privacy might not be an issue.	Misdirected payments encoded into the blockchain would be hard to correct without an additional offsetting transaction.

Source: Barclays Research

Potential exists

We think blockchain and distributed ledger technologies hold potential. In our quick survey of potential efficiency gains, we see two general impediments to widespread adoption.

First, what might be technologically possible may not be legally so. Much of the verification and double-checking that now occurs in financial transactions are driven by regulation. Banks and non-bank financial service providers are subject to KYC rules, as well as AML reporting requirements. We have no doubt that technology can greatly simplify these requirements; for example, much like border controls, it is possible to establish trusted counterparties whose transactions and activities are subject to less monitoring and verification. Similarly, as we describe above, it is possible to encode KYC and AML restrictions into the blockchain of the asset, much like a tax lien on a land title.

Second, we suspect that some improvements may be slow to take hold because the existing technology is good enough. As described above, real-time gross settlements for bank payments may be difficult to shift over to blockchain and – at least currently – have little net benefit over the existing technology. And the cost of transitioning may be high relative to the potential savings.

It is not entirely clear what kind of blockchain access should exist for financial assets

Finally, it is not entirely clear what kind of blockchain access should exist for financial assets. In our earlier examples, we assumed that buyers and sellers would enter a matching encrypted code on a permissioned distributed ledger that turns a switch on the asset's blockchained CUSIP. In theory, all investors with write access to the ledger would be able to update the CUSIP chain directly. However, we assume regulators would wish to establish some minimum standards on investors with write access to blockchains. But if the blockchain is publicly viewable, how could it be structured simultaneously to preserve ownership anonymity while allowing the Treasury and other financial market regulators the ability to identify owners and transactions?

Who benefits from the efficiency gains?

Most of the studies of the potential gains from distributed ledger have a similar theme: technology lowers intermediation costs; therefore, consumers benefit. A Bitcoin-based international payments platform eliminates the need for middlemen and correspondent banks while promising (near) immediate settlement. More extreme versions with widespread distributed ledger adoption and smart contracts imagine a completely de-centralized financial marketplace where intermediation costs have been reduced nearly to 0. But this is probably an oversimplification.

Consider the US payment system, which has been the focal point of much of the heated commentary about de-centralization and intermediation costs. Even if US payments become safer and faster through the application of distributed ledger and blockchain, it is unclear

how much the cost of sending and receiving payments will decline. Instead, this would depend on how the organizational structure of the payments system evolves alongside new technology.[20] Three potential market structures could emerge: a dominant operator, a multi-operator or a completely de-centralized platform. These depend on the fixed expense of the new technology and whether, in an industry such as payments, there are economies of scale and network efficiencies.

Will the financial services industry de-concentrate?

It is unclear to what extent the financial services industry will de-centralize, despite stories about the end of traditional banking and the expansion of peer-to-peer lending. While distributed ledger and blockchain may make it easier for smaller firms with cutting-edge technology to become significant financial market disruptors, banking, market-making and other forms of financial intermediation are heavily regulated, so that entry is expensive. Importantly, financial intermediation exhibits significant returns to scale and network efficiency.

New financial technology such as blockchain, distributed ledgers, and smart contracts, have historical parallels. Indeed, advances in computers and telecommunications since the 1970s have tended to favour more centralization in financial services. This has certainly been the case for automatic consumer electronic payments such as direct deposits, mortgages, and other consumer bills. Where once there were several regional platforms processing payments on the Automated Clearing House (ACH) platform, there are now only two left: The Clearing House (TCH) and the Federal Reserve. But electronic payment processing is only one example. Originally, there were several banks that cleared repo transactions, but higher capital and other requirements eventually reduced this number to just one by mid-2016.[21] Our reading of this history suggests that some of the optimism about 'cost-less' cross border payments outside the traditional banking sector may be overstated.

Separately, the application of distributed ledger technology shares some features with 'dematerialization', *ie*, the removal of paper stock and bond certificates. By the late 1960s, increasing financial market activity created an avalanche of circulating paper certificates shuttling between banks and depositories. Not only did this create security risk (no pun intended), but the amount of time it took to move certificates required the New York Stock Exchange to shorten trading hours and close on Wednesday, even with T+5 settlement.[22]

Initially, banks attempted to reduce the volume of circulating paper by immobilizing certificates at a central repository. Ownership changes could be reflected in a book entry ledger without the certificates ever leaving the repository, a pre-computer version of a blockchain without a publicly viewable ledger. Initially, the book entry only modestly reduced the paper avalanche, as the program was voluntary. It was only in 1983 that the NYSE required members to settle securities in book entry form. At about the same time, the Treasury moved its issuance to book entry. That said, even as late as 2012, there were still 1.2m stock and bond certificates sitting in the DTCC's vaults, although down 94% since 2000. Our sense is that removing or reducing the back office costs associated with double-checking ledgers, bookkeeping, and trade verification will be similar to the cost savings associated with dematerialization.

New technology tends either to create a new dominant presence or is quickly co-opted by incumbents

Curiously, despite the technological advances described above, a recent examination of financial intermediation costs reveals surprising stability.[23] Philippon estimates that the unit cost of financial intermediation has been steady at about 2% for 130 years. He suggests there might be three reasons for the stickiness in intermediation costs: barriers to entry, increasing returns to scale, and inefficient regulation (in the form of 'too big to fail', which

[20] See *Faster Payments: Market Structure and Policy Considerations*, A. Rosenbaum, G. Baughman, M. Manuszak, K. Stewart, F. Hayashi, and J. Stavins, Federal Reserve Bank of Boston, September 2017.
[21] Even the Fed's daily reverse repo transactions settle on this platform.
[22] See *A Proposal to Fully De-materialize Physical Securities: Eliminating the Costs and Risks They Incur*, DTCC White Paper, July 2012.
[23] See *The FinTech Opportunity*, T. Philippon, Bank for International Settlements working paper, August 2017.

could act as a *de facto* proxy for counterparty trust). Our sense is that new technology tends either to create a new dominant presence or is quickly co-opted by incumbents.

But if Philippon's numbers are correct, the outlook for lower transaction costs from blockchain and distributed ledger technology is a bit disappointing. After all, if dematerialization, electronic payments, and telecommunication advances such as the phone and Bloomberg have failed to reduce the cost of financial intermediation, what's to say that these new technologies will have any more success?

Of course, it may be the case that crypto adoption is *currently* limited to low-trust environments. But as the technology develops and the sophistication of smart contracts advances, we cannot reject that adoption could spread to developed economies with strong legal frameworks.

Appendix A: A brief lexicon

For a more detailed discussion, please refer to *Fintech primer vol. 3 – Blockchain*, 9 March 2016.

Blockchain: A specific type of ledger in which transactions are recorded in groups or 'blocks' that have been encrypted and linked together. The encryption of new block in the chain uses an identifier uniquely generated from the previous block as an input; in this way, the blocks are 'chained' together. As this is done in a near-unique manner, altering past transactions is extremely difficult and costly.[24]

Distributed ledger: An electronic ledger that is kept in multiple places simultaneously. Because there are multiple copies, a distributed ledger requires a mechanism for keeping all copies of the ledger synchronised and for resolving disputes when copies of the ledger differ from one another.

Public ledgers: The extent to which anyone can read the information recorded in a copy of the distributed ledger. Public ledgers are more resilient because with enough copies in existence, it becomes almost impossible to shut down or permanently lose the ledger. Every transaction is public. To the extent that activity can be linked or tagged to specific owner, this means that ownership is also (potentially) viewable.

Permissioned access: A distributed ledger that only allows specific users to add transactions to the ledger – that is, "write access". By contrast, unpermissioned ledgers allow anyone to add transactions to the record, subject to pre-set rules. Competition between processors to earn a reward for updating the ledger should in theory encourage faster processing at lower cost.

Consensus mechanism: A design feature of unpermissioned distributed ledgers governing the ability to write new information to the ledger. As everyone has the ability to update their copy of the ledger, there needs to be an agreed-upon mechanism to establish a hierarchy for determining the most current version. Consensus mechanisms establish this hierarchy by requiring updaters to solve complicated algorithms: 'proof of work'. Other mechanisms, however, require updaters to establish a 'proof of stake'.

Appendix B: Money: a history

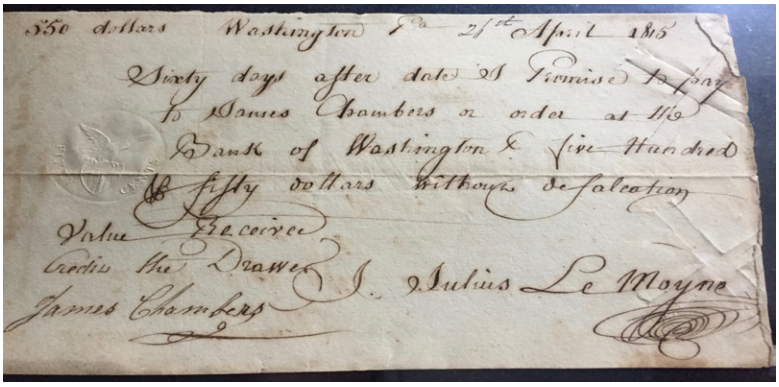
Initially, paper money developed as a receipt from a goldsmith for the deposit of valuables held for safekeeping. People quickly discovered that these paper receipts were much easier for transferring value than moving physical assets in out of the goldsmith's safe. Goldsmiths – and other merchants – quickly discovered that they could issue certificates for more than the value of the metal sitting in their safes; thus, fractional reserve banking was born.

[24] For first generation BC/DLT, which use 'proof-of-work' algorithms, the generation of the nonce is extremely computationally expensive, due to competition to solve increasingly difficult mathematical problems, but newer generations of BC/DLT use 'proof-of-stake' algorithms for verification that reduce the computational (and time) drag, yet, with a distributed ledger, maintain the security of proof-of-work methods.

Individuals began writing their own personal 'notes of hand' (effectively circulating IOUs) as an early form of credit (Figure 17).

Unsurprisingly, this created an environment ripe for forgeries and fraud – the "passing of bad notes". There was no central database of names or signatures of people with a history of passing bad notes. Nor was there a central agency that would vouch for the credit quality and general trustworthiness of the issuer or the solvency of the goldsmith. Henry Fielding's work, like many of his contemporaries, contains numerous references to the circulation of bad paper and the bankruptcies of goldsmith-bankers.

FIGURE 17
Promissory note, 1815



Note: the impressed seal at the left indicates the note was taxed. Source: Abate collection

In Europe, banks with varying levels of government sponsorship began issuing their own convertible paper in the 18th century. Paper notes were exchangeable for a fixed value in specie at the state bank. Over-issuance led to spectacular bubbles and busts in the 1720s, including the Mississippi and South Sea bubbles.

These quasi-private issuers frequently suspended their notes' convertibility. For example, during the Napoleonic Wars, the Bank of England suspended the convertibility of its notes to preserve its holdings of gold. The 'Restriction Period', which began in 1797, only ended in 1821. During this period, a scarcity of silver pushed the Bank of England to issue its own tokens as well as re-coin Spanish pieces (Figure 18).[25] Spanish coins circulated as crowns (5*s*), but their silver content was considerably below that in an English crown.[26]

[25] Minting coins was a sovereign's right, so the Bank of England could only issue 'tokens' in denominations other than those making up royal coinage. See *The Coinage of the British Empire*, H. N. Humphreys, London, 1868
[26] The coins had King of Spain's portrait counterstamped with the King of England's; hence "two crowns not worth a crown". See Figure 18.

FIGURE 18

English 5s countermarked Spanish 8 real coin, 1792

Source: Abate collection

Many crypto enthusiasts are 'hard money' advocates at heart. They note that since the supply of Bitcoin, for example, is fixed, it is not subject to central bank devaluation from over-issuance. However, private money as a substitute for sovereign money is not unique to crypto.

Following its defeat in World War I and its reparation payment requirements under the Versailles Treaty, Germany entered a period of severe hyperinflation. In January 1920, the minimum weekly cost of subsistence for a family of four living in Berlin was 220 Reichsmarks; by mid-November 1923, it was more than RM20 trillion.[27] There are plenty of anecdotes of how families coped with the hyperinflation but one curiosity of corporate behaviour during this period was the issuance of private money to pay employees and suppliers. Railroads[28], banks, coalmines, and even shoe manufacturing companies paid their employees with company script that in some cases could be used in commissaries maintained by the company. Not only could these companies negotiate to buy staples at a discount, but it also meant that workers would not have to cut short their working day in order to spend hours in line at stores and shops to purchase basic necessities (Figure 19).

FIGURE 19

Germany, private issue, notgeld, 1923

Source: Abate collection

[27] See Table 8, *The German Inflation 1914-1923*, C.L. Holtfrerich, deGruyter, 1986.
[28] See "*Das Papiergeld der deutschen Eisenbahnen und der Reichpost*, M. Muller, A. Geiger, Verlag A. Geiger.

'Workmen are given their pay twice a day now – in the morning and in the afternoon, with a recess of a half hour each time so they can rush out and buy things – for if they waited a few hours the value of their money would drop so far that their children would not get half enough food to feel satisfied. Satisfied – not nourished. Satisfied with anything that can be stuffed into their stomachs, not with what the body needs.'[29]

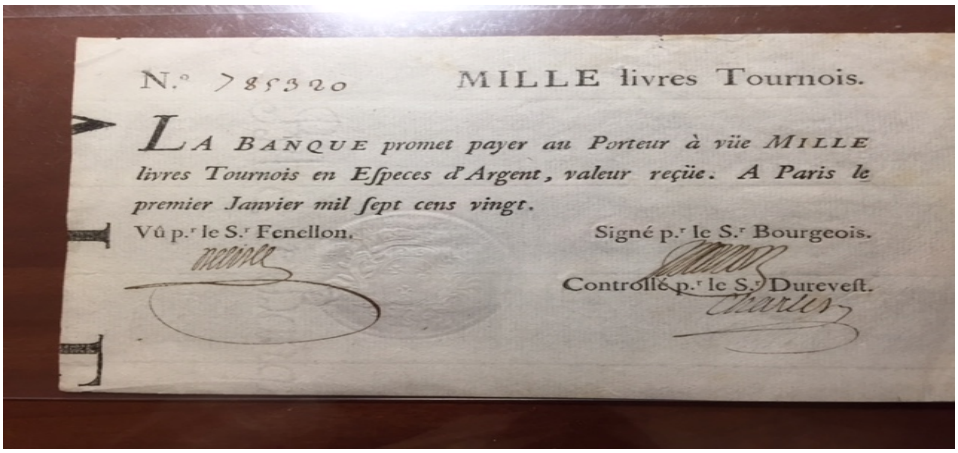
Once the German government established a credibly independent central bank, its currency stabilized,[30] and all this 'worthless paper muck'[31] disappeared in a reverse of Gresham's Law: good (stable value money) drove out the bad. The immediate acceptance of the new *Reichsmark* was supported by its status as legal tender.

Appendix C: Early bubbles

South Seas Company: a public/private monopoly set up in England to trade with South America in 1711. Like the Bank of England at the time, it also traded in government debt. Its directors were involved in insider trading, bribing Parliament, and promising rich returns to shareholders on the potential value of trade with South America. Share prices rapidly inflated, and then collapsed in 1720.

Mississippi Company: a public/private monopoly set up in France to trade with its North American (Mississippi) colonies in 1716. The company gained the right to issue paper currency in return for gold and silver, although these notes were never legal tender. The popularity and excited prospects of profits from North American trade enabled the company (renamed the Compagnie des Indes) to collect indirect taxes, mint coins and eventually restructure French government debt. Over-issuance of paper money and an inability to meet customer's demand for specie led to a run and a swift plunge in its share price.

FIGURE 20
Mississippi bubble note



Source: Abate collection

[29] See *The Black Obelisk*, Erich Maria Remarque, 1957
[30] 'The Ends of Four Big Inflations,' Thomas J. Sargent, *Inflation: Causes and Effects* (NBER 1982), Robert E. Hall, editor (p. 41 - 98).
[31] See *Wolf among Wolves*, Hans Fallada, 1937.

Analyst Certification
We, Joseph Abate, Marvin Barth, Zoso Davies and Tomasz Wieladek, hereby certify (1) that the views expressed in this research report accurately reflect our personal views about any or all of the subject securities or issuers referred to in this research report and (2) no part of our compensation was, is or will be directly or indirectly related to the specific recommendations or views expressed in this research report.

Important Disclosures:
Barclays Research is produced by the Investment Bank of Barclays Bank PLC and its affiliates (collectively and each individually, "Barclays")
All authors contributing to this research report are Research Analysts unless otherwise indicated. The publication date at the top of the report reflects the local time where the report was produced and may differ from the release date provided in GMT.

Availability of Disclosures:
For current important disclosures regarding any issuers which are the subject of this research report please refer to https://publicresearch.barclays.com or alternatively send a written request to: Barclays Research Compliance, 745 Seventh Avenue, 13th Floor, New York, NY 10019 or call +1-212-526-1072.

Barclays Capital Inc. and/or one of its affiliates does and seeks to do business with companies covered in its research reports. As a result, investors should be aware that Barclays may have a conflict of interest that could affect the objectivity of this report. Barclays Capital Inc. and/or one of its affiliates regularly trades, generally deals as principal and generally provides liquidity (as market maker or otherwise) in the debt securities that are the subject of this research report (and related derivatives thereof). Barclays trading desks may have either a long and / or short position in such securities, other financial instruments and / or derivatives, which may pose a conflict with the interests of investing customers. Where permitted and subject to appropriate information barrier restrictions, Barclays fixed income research analysts regularly interact with its trading desk personnel regarding current market conditions and prices. Barclays fixed income research analysts receive compensation based on various factors including, but not limited to, the quality of their work, the overall performance of the firm (including the profitability of the Investment Banking Department), the profitability and revenues of the Markets business and the potential interest of the firm's investing clients in research with respect to the asset class covered by the analyst. To the extent that any historical pricing information was obtained from Barclays trading desks, the firm makes no representation that it is accurate or complete. All levels, prices and spreads are historical and do not represent current market levels, prices or spreads, some or all of which may have changed since the publication of this document. Barclays Research Department produces various types of research including, but not limited to, fundamental analysis, equity-linked analysis, quantitative analysis, and trade ideas. Recommendations and trade ideas contained in one type of Barclays Research may differ from those contained in other types of Barclays Research, whether as a result of differing time horizons, methodologies, or otherwise.
The Barclays Research Department operates independently from the Absa Research Department. Absa Research is produced by Absa Bank Limited acting through its Corporate and Investment Bank division, which is a part of Barclays Africa Group Limited and affiliated with the Investment Bank of Barclays Bank PLC. Eligible clients may receive research reports from both research departments, which may reach different conclusions and may contain different and conflicting forecasts, recommendations, or trade ideas. In order to access Barclays Statement regarding Research Dissemination Policies and Procedures, please refer to *https://publicresearch.barcap.com/S/RD.htm*. In order to access Barclays Research Conflict Management Policy Statement, please refer to: *https://publicresearch.barcap.com/S/CM.htm*.

Other Material Conflicts

One of the authors of this report has a financial interest in Bitcoin, Ethereum and Litecoin.

All pricing information is indicative only. Prices are sourced from Thomson Reuters as of the last available closing price at the time of production of the research report, unless another time and source is indicated.

Explanation of other types of investment recommendations produced by Barclays FICC Research:
Trade ideas contained herein that have been produced by the Credit teams within Barclays Research are valid at current market conditions and may not be otherwise relied upon.
Trade ideas contained herein that have been produced by other research teams within Barclays FICC Research shall remain open until they are subsequently amended or closed in a future research report.

Disclosure of previous investment recommendations produced by Barclays FICC Research:
Barclays FICC Research may have published other investment recommendations in respect of the same securities/instruments recommended in this research report during the preceding 12 months. To view previous investment recommendations published by Barclays FICC Research in the preceding 12 months please refer to *https://live.barcap.com/go/research/Recommendations*.

Legal entities involved in producing Barclays Research:
Barclays Bank PLC (Barclays, UK)
Barclays Capital Inc. (BCI, US)
Barclays Securities Japan Limited (BSJL, Japan)
Barclays Bank PLC, Hong Kong branch (Barclays Bank, Hong Kong)
Barclays Capital Canada Inc. (BCCI, Canada)
Barclays Bank Mexico, S.A. (BBMX, Mexico)
Barclays Securities (India) Private Limited (BSIPL, India)
Barclays Bank PLC, India branch (Barclays Bank, India)
Barclays Bank PLC, Singapore branch (Barclays Bank, Singapore)

Disclaimer:

This publication has been produced by Barclays Research Department in the Investment Bank of Barclays Bank PLC and/or one or more of its affiliates (collectively and each individually, "Barclays"). It has been distributed by one or more Barclays affiliated legal entities listed below. It is provided to our clients for information purposes only, and Barclays makes no express or implied warranties, and expressly disclaims all warranties of merchantability or fitness for a particular purpose or use with respect to any data included in this publication. To the extent that this publication states on the front page that it is intended for institutional investors and is not subject to all of the independence and disclosure standards applicable to debt research reports prepared for retail investors under U.S. FINRA Rule 2242, it is an "institutional debt research report" and distribution to retail investors is strictly prohibited. Barclays also distributes such institutional debt research reports to various issuers, regulatory and academic organisations for informational purposes and not for the purpose of making investment decisions regarding any debt securities. Any such recipients that do not want to continue receiving Barclays institutional debt research reports should contact debtresearch@barclays.com. Barclays will not treat unauthorized recipients of this report as its clients and accepts no liability for use by them of the contents which may not be suitable for their personal use. Prices shown are indicative and Barclays is not offering to buy or sell or soliciting offers to buy or sell any financial instrument.

Without limiting any of the foregoing and to the extent permitted by law, in no event shall Barclays, nor any affiliate, nor any of their respective officers, directors, partners, or employees have any liability for (a) any special, punitive, indirect, or consequential damages; or (b) any lost profits, lost revenue, loss of anticipated savings or loss of opportunity or other financial loss, even if notified of the possibility of such damages, arising from any use of this publication or its contents.

Other than disclosures relating to Barclays, the information contained in this publication has been obtained from sources that Barclays Research believes to be reliable, but Barclays does not represent or warrant that it is accurate or complete. Barclays is not responsible for, and makes no warranties whatsoever as to, the information or opinions contained in any written, electronic, audio or video presentations of third parties that are accessible via a direct hyperlink in this publication or via a hyperlink to a third-party web site ('Third-Party Content'). Any such Third-Party Content has not been adopted or endorsed by Barclays, does not represent the views or opinions of Barclays, and is not incorporated by reference into this publication. Third-Party Content is provided for information purposes only and Barclays has not independently verified its accuracy or completeness.

The views in this publication are solely and exclusively those of the authoring analyst(s) and are subject to change, and Barclays Research has no obligation to update its opinions or the information in this publication. Unless otherwise disclosed herein, the analysts who authored this report have not received any compensation from the subject companies in the past 12 months. If this publication contains recommendations, they are general recommendations that were prepared independently of any other interests, including those of Barclays and/or its affiliates, and/or the subject companies. This publication does not contain personal investment recommendations or investment advice or take into account the individual financial circumstances or investment objectives of the clients who receive it. The securities and other investments discussed herein may not be suitable for all investors. Barclays is not a fiduciary to any recipient of this publication. Investors must independently evaluate the merits and risks of the investments discussed herein, consult any independent advisors they believe necessary, and exercise independent judgment with regard to any investment decision. The value of and income from any investment may fluctuate from day to day as a result of changes in relevant economic markets (including changes in market liquidity). The information herein is not intended to predict actual results, which may differ substantially from those reflected. Past performance is not necessarily indicative of future results.

This document is being distributed (1) only by or with the approval of an authorised person (Barclays Bank PLC) or (2) to, and is directed at (a) persons in the United Kingdom having professional experience in matters relating to investments and who fall within the definition of "investment professionals" in Article 19(5) of the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 (the "Order"); or (b) high net worth companies, unincorporated associations and partnerships and trustees of high value trusts as described in Article 49(2) of the Order; or (c) other persons to whom it may otherwise lawfully be communicated (all such persons being "Relevant Persons"). Any investment or investment activity to which this communication relates is only available to and will only be engaged in with Relevant Persons. Any other persons who receive this communication should not rely on or act upon it. Barclays Bank PLC is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority and is a member of the London Stock Exchange.

The Investment Bank of Barclays Bank PLC undertakes U.S. securities business in the name of its wholly owned subsidiary Barclays Capital Inc., a FINRA and SIPC member. Barclays Capital Inc., a U.S. registered broker/dealer, is distributing this material in the United States and, in connection therewith accepts responsibility for its contents. Any U.S. person wishing to effect a transaction in any security discussed herein should do so only by contacting a representative of Barclays Capital Inc. in the U.S. at 745 Seventh Avenue, New York, New York 10019.

Non-U.S. persons should contact and execute transactions through a Barclays Bank PLC branch or affiliate in their home jurisdiction unless local regulations permit otherwise.

Barclays Bank PLC, Paris Branch (registered in France under Paris RCS number 381 066 281) is regulated by the Autorité des marchés financiers and the Autorité de contrôle prudentiel. Registered office 34/36 Avenue de Friedland 75008 Paris.

This material is distributed in Canada by Barclays Capital Canada Inc., a registered investment dealer, a Dealer Member of IIROC (www.iiroc.ca), and a Member of the Canadian Investor Protection Fund (CIPF).

Subject to the conditions of this publication as set out above, Absa Bank Limited, acting through its Corporate and Investment Bank division, which is a part of Barclays Africa Group Limited and affiliated with the Investment Bank of Barclays Bank PLC, an authorised financial services provider (Registration No.: 1986/004794/06. Registered Credit Provider Reg No NCRCP7), is distributing this material in South Africa. Absa Bank Limited is regulated by the South African Reserve Bank. This publication is not, nor is it intended to be, advice as defined and/or contemplated in the (South African) Financial Advisory and Intermediary Services Act, 37 of 2002, or any other financial, investment, trading, tax, legal, accounting, retirement, actuarial or other professional advice or service whatsoever. Any South African person or entity wishing to effect a transaction in any security discussed herein should do so only by contacting a representative of Absa Bank Limited acting through its Corporate and Investment Bank division in South Africa, 7th Floor, Barclays Towers West, 15 Troye Street, Johannesburg. Absa Bank Limited is an affiliate of the Barclays group.

All Barclays research reports are distributed to institutional investors in Japan by Barclays Securities Japan Limited. Barclays Securities Japan Limited is a joint-stock company incorporated in Japan with registered office of 6-10-1 Roppongi, Minato-ku, Tokyo 106-6131, Japan. It is a subsidiary of Barclays Bank PLC and a registered financial instruments firm regulated by the Financial Services Agency of Japan. Registered Number: Kanto Zaimukyokucho (kinsho) No. 143.

Barclays Bank PLC, Hong Kong Branch is distributing this material in Hong Kong as an authorised institution regulated by the Hong Kong Monetary Authority. Registered Office: 41/F, Cheung Kong Center, 2 Queen's Road Central, Hong Kong.

All Indian securities-related research and other equity research produced by Barclays' Investment Bank are distributed in India by Barclays Securities

(India) Private Limited (BSIPL). BSIPL is a company incorporated under the Companies Act, 1956 having CIN U67120MH2006PTC161063. BSIPL is registered and regulated by the Securities and Exchange Board of India (SEBI) as a Research Analyst: INH000001519; Portfolio Manager INP000002585; Stock Broker/Trading and Clearing Member: National Stock Exchange of India Limited (NSE) Capital Market INB231292732, NSE Futures & Options INF231292732, NSE Currency derivatives INE231450334, Bombay Stock Exchange Limited (BSE) Capital Market INB011292738, BSE Futures & Options INF011292738; Depository Participant (DP) with the National Securities & Depositories Limited (NSDL): DP ID: IN-DP-NSDL-299-2008; Investment Adviser: INA000000391. The registered office of BSIPL is at 208, Ceejay House, Shivsagar Estate, Dr. A. Besant Road, Worli, Mumbai – 400 018, India. Telephone No: +91 2267196000. Fax number: +91 22 67196100. Any other reports produced by Barclays' Investment Bank are distributed in India by Barclays Bank PLC, India Branch, an associate of BSIPL in India that is registered with Reserve Bank of India (RBI) as a Banking Company under the provisions of The Banking Regulation Act, 1949 (Regn No BOM43) and registered with SEBI as Merchant Banker (Regn No INM000002129) and also as Banker to the Issue (Regn No INBI00000950). Barclays Investments and Loans (India) Limited, registered with RBI as Non Banking Financial Company (Regn No RBI CoR-07-00258), and Barclays Wealth Trustees (India) Private Limited, registered with Registrar of Companies (CIN U93000MH2008PTC188438), are associates of BSIPL in India that are not authorised to distribute any reports produced by Barclays' Investment Bank.

Barclays Bank PLC Frankfurt Branch distributes this material in Germany under the supervision of Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin).

This material is distributed in Mexico by Barclays Bank Mexico, S.A.

Nothing herein should be considered investment advice as defined in the Israeli Regulation of Investment Advisory, Investment Marketing and Portfolio Management Law, 1995 ("Advisory Law"). This document is being made to eligible clients (as defined under the Advisory Law) only. Barclays Israeli branch previously held an investment marketing license with the Israel Securities Authority but it cancelled such license on 30/11/2014 as it solely provides its services to eligible clients pursuant to available exemptions under the Advisory Law, therefore a license with the Israel Securities Authority is not required. Accordingly, Barclays does not maintain an insurance coverage pursuant to the Advisory Law.

Barclays Bank PLC in the Dubai International Financial Centre (Registered No. 0060) is regulated by the Dubai Financial Services Authority (DFSA). Principal place of business in the Dubai International Financial Centre: The Gate Village, Building 4, Level 4, PO Box 506504, Dubai, United Arab Emirates. Barclays Bank PLC-DIFC Branch, may only undertake the financial services activities that fall within the scope of its existing DFSA licence. Related financial products or services are only available to Professional Clients, as defined by the Dubai Financial Services Authority.

Barclays Bank PLC in the UAE is regulated by the Central Bank of the UAE and is licensed to conduct business activities as a branch of a commercial bank incorporated outside the UAE in Dubai (Licence No.: 13/1844/2008, Registered Office: Building No. 6, Burj Dubai Business Hub, Sheikh Zayed Road, Dubai City) and Abu Dhabi (Licence No.: 13/952/2008, Registered Office: Al Jazira Towers, Hamdan Street, PO Box 2734, Abu Dhabi).

Barclays Bank PLC in the Qatar Financial Centre (Registered No. 00018) is authorised by the Qatar Financial Centre Regulatory Authority (QFCRA). Barclays Bank PLC-QFC Branch may only undertake the regulated activities that fall within the scope of its existing QFCRA licence. Principal place of business in Qatar: Qatar Financial Centre, Office 1002, 10th Floor, QFC Tower, Diplomatic Area, West Bay, PO Box 15891, Doha, Qatar. Related financial products or services are only available to Business Customers as defined by the Qatar Financial Centre Regulatory Authority.

This material is distributed in the UAE (including the Dubai International Financial Centre) and Qatar by Barclays Bank PLC.

This material is not intended for investors who are not Qualified Investors according to the laws of the Russian Federation as it might contain information about or description of the features of financial instruments not admitted for public offering and/or circulation in the Russian Federation and thus not eligible for non-Qualified Investors. If you are not a Qualified Investor according to the laws of the Russian Federation, please dispose of any copy of this material in your possession.

This material is distributed in Singapore by the Singapore branch of Barclays Bank PLC, a bank licensed in Singapore by the Monetary Authority of Singapore. For matters in connection with this report, recipients in Singapore may contact the Singapore branch of Barclays Bank PLC, whose registered address is 10 Marina Boulevard, #23-01 Marina Bay Financial Centre Tower 2, Singapore 018983.

This material is distributed to persons in Australia by either Barclays Bank plc, Barclays Capital Inc., Barclays Capital Securities Limited or Barclays Capital Asia Limited. None of Barclays Bank plc, nor any of the other referenced Barclays group entities, hold an Australian financial services licence and instead they each rely on an exemption from the requirement to hold such a licence. This material is intended to only be distributed to "wholesale clients" as defined by the Australian Corporations Act 2001.

IRS Circular 230 Prepared Materials Disclaimer: Barclays does not provide tax advice and nothing contained herein should be construed to be tax advice. Please be advised that any discussion of U.S. tax matters contained herein (including any attachments) (i) is not intended or written to be used, and cannot be used, by you for the purpose of avoiding U.S. tax-related penalties; and (ii) was written to support the promotion or marketing of the transactions or other matters addressed herein. Accordingly, you should seek advice based on your particular circumstances from an independent tax advisor.