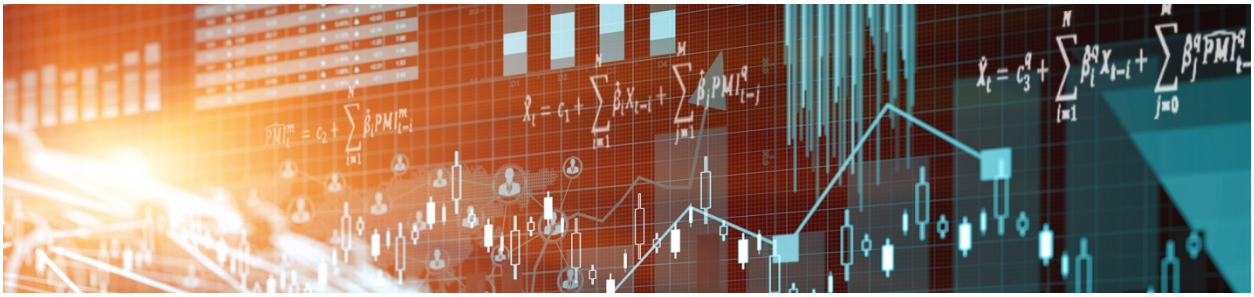
BANK OF CANADA
BANQUE DU CANADA

Staff Discussion Paper/Document d'analyse du personnel 2019-1

Crypto "Money": Perspective of a Couple of Canadian Central Bankers



by James Chapman and Carolyn A. Wilkins

www.bank-banque-canada.ca

Bank of Canada Staff Discussion Paper 2019-1

February 2019

Crypto "Money": Perspective of a Couple of Canadian Central Bankers

by

James Chapman[1] and Carolyn A. Wilkins[2]

[1] Funds Management and Banking Department
[2] Senior Deputy Governor
Bank of Canada
Ottawa, Ontario, Canada K1A 0G9
jchapman@bankofcanada.ca
cwilkins@bankofcanada.ca

ISSN 1914-0568

Acknowledgements

Many thanks, without implication, to Adam Epp for excellent research assistance, and Rod Garratt, Scott Hendry, Tim Lane, Stephen Murchison and others for discussion and comments. This paper is based on a lecture Senior Deputy Governor Wilkins gave at Princeton University on October 4, 2018. https://www.bankofcanada.ca/2018/10/money-for-nothing-a-central-bankers-take-on-cryptoassets/

Abstract

The market for cryptoassets has exploded in size in the 10 years since bitcoin was launched. The technology underlying cryptoassets, blockchain, has also been held up as a technology that promises to transform entire industries. In this paper we examine what is new about cryptoassets and their technology and how they may affect core central bank functions. We do this by outlining what we think are the three most important research and policy questions for central bankers around cryptoassets and cryptocurrencies specifically. First, what is fundamentally new about the technology that underpins cryptocurrencies and other cryptoassets? Second, how do cryptocurrencies affect a central bank's role in the economy? Third, given the two challenges of a rise of cryptoassets and a decline in the use of cash, should digital payments be left entirely to the private sector or should central banks issue their own digital currencies? We discuss these three policy questions and highlight what aspects of them are most important to central bankers. Finally, we raise several new questions to help guide researchers in studying cryptoassets and their underlying technology.

Bank topics: Digital currencies; Payment clearing and settlement systems; Bank notes; Financial services
JEL codes: E4, E41, E42, E51, E58, H4, P43

Résumé

La taille du marché des cryptoactifs a explosé ces dix dernières années, depuis le lancement du bitcoin. On a aussi présenté la technologie à la base des cryptoactifs, soit la chaîne de blocs, comme étant susceptible de transformer des pans entiers de l'économie. Dans cette étude, nous examinons ce que les cryptoactifs et la technologie connexe apportent de nouveau, et les conséquences possibles pour les grandes fonctions des banques centrales. Pour ce faire, nous définissons ce qui constitue, selon nous, les trois plus importantes questions que les banques centrales doivent aborder dans leurs recherches et leurs politiques sur les cryptoactifs et, plus précisément, sur les cryptomonnaies. Premièrement, en quoi la technologie qui sous-tend les cryptomonnaies et les autres cryptoactifs est-elle, en essence, innovante? Deuxièmement, quelle est l'incidence des cryptomonnaies sur le rôle des banques centrales dans l'économie? Troisièmement, compte tenu des défis que représentent la percée des cryptoactifs et de la baisse de l'utilisation de l'argent comptant, faut-il laisser les paiements numériques relever exclusivement du secteur privé ou les banques centrales devraient-elles émettre leur propre monnaie numérique? Nous abordons ces trois questions en insistant sur leurs aspects les plus importants pour les banques centrales. Enfin, nous soulevons plusieurs nouvelles questions afin d'aiguiller la recherche sur les cryptoactifs et la technologie sous-jacente.

Sujets : Monnaies numériques; Systèmes de compensation et de règlement des paiements; Billets de banque; Services financiers
Codes JEL : E4, E41, E42, E51, E58, H4, P43

"No mo fiat money we don't do that/

Get urself some coins fo the banks take ur stash"

— "Bitcoin's Here" by Zhou Tonged[1]

1. Introduction

The market for cryptoassets has exploded since the launch of bitcoin—the world's first cryptoasset based on blockchain technology.[2, 3] With around 2,000 cryptoassets in existence today, much has been made of their potential to upend the financial system. Even more has been made of the potential for a broader range of applications of the blockchain technology underlying cryptoassets. This technology promises to transform entire industries, from financial services to the supply chain management for food, tracking livestock such as chicken and cows.[4]

In this discussion paper, we examine what cryptoassets bring to the table that is new and how they may affect core central banking functions. We also outline what we think are the most important open research and policy questions for central banks in this area. Our hope is that we can help temper the hype that surrounds discussion of cryptoassets and provide some focus for ongoing work on the issue.

Over the past couple of years, a myriad of different uses for cryptoassets has been rapidly expanding: payment methods, securities and utilities. We will focus primarily on the means of payment aspect—that is, potential cryptocurrencies—because money and payments are of utmost importance to central banking. These are *potential* currencies since none yet fulfills all the traditional functions of money: a medium of exchange, store of value and unit of account.

The rest of the paper is organized around three overarching questions:

1) ***What is fundamentally new about the technology that underpins cryptocurrencies and other cryptoassets?*** Many of the issues are similar to those being studied by researchers of corporate governance and asset pricing. But there are also some novel economic questions, such as how a blockchain is designed to ensure that everyone's incentives are aligned to result in truthful reporting of movements of cryptoassets on the blockchain.
2) ***How do cryptocurrencies affect a central bank's role in the economy?*** We look at whether cryptocurrencies could form the basis of a "desirable" monetary policy regime

---

[1] See the cover of Drake's song, "Started from the Bottom," about Bitcoin success at https://youtu.be/pID03RrmKow.

[2] Bitcoin was created in 2009 by an unknown individual or individuals going by the pseudonym Satoshi Nakamoto. The underlying technology used creates what is commonly known as a "blockchain," which is a type of distributed ledger technology.

[3] We define a cryptoasset as an asset that is recorded on a blockchain or using distributed ledger technology.

[4] L.-A. Javier, "Yes, These Chickens Are on the Blockchain," Bloomberg Businessweek (April 9, 2018).

and what the implications might be when it co-exists with public currencies. Here, too, many outstanding research questions need to be answered.

3) ***Given the two challenges of a rise of cryptoassets and a decline in the use of cash, should digital payments be left entirely to the private sector or should central banks issue their own digital currency?*** The place to start here is to determine whether central bank currency is a public good, which we argue it is. That said, this line of inquiry raises deeper questions related to the uniqueness of money in each of its functions and the role a central bank digital currency could have in this regard compared with physical cash. Another large group of questions lies in understanding how a central bank digital currency would affect the rest of the financial system, particularly deposit-taking institutions.

These are fundamental questions for any monetary or financial economist, which make this an exciting time to be doing research in this area. We believe that we may be at a turning point where the monetary landscape 10 to 15 years from now could look radically different than it does today. Innovation in this area could have a fundamental impact on social welfare and research and policy work is needed in guiding it to the best outcome for the people in the economy.

To set the stage, we paint the landscape for cryptoassets before addressing each of the questions in turn.

2. Cryptocurrencies and the cryptoasset landscape

Assessing the full span of the cryptoasset landscape is a more difficult task than with other asset classes, such as equities and, more recently, financial derivatives. Thanks to some new datasets, several observations about the cryptoasset landscape and how it has evolved over the past decade can nonetheless be made.[5]

The first observation is that, while cryptoassets are often discussed as a single asset class, they have become quite heterogeneous in terms of underlying economic function. Early cryptoassets (e.g., bitcoins) were originally created to be decentralized digital currencies. Authorities now tend to distinguish between the following large classes of cryptoassets:

- *Cryptocurrencies.* These are tokens generally intended to fill the role of a currency and are designed to be used to make purchases of goods and services. An example is bitcoin, as originally envisioned, while Litecoin and Monero are other examples.

- *Security tokens*. These tokens allow buyers to take some form of position in a firm. Many of the initial coin offerings (ICOs) over the past couple of years fall into this category, although there are significant differences among them in terms of their design. A straightforward example is a token that represents equity in an organization built on a blockchain platform where "the token-holder receives future cash flows from a successful project" (Hu, Parlour and Rajan 2018). Another example is Nexo, which is a crypto loan company that pays out a portion of the profits to Nexo token holders.[6]

[5] The main dataset we use is the cointmarketcap.com historical database of cryptoassets.

[6] See Nexo Token Terms at nexo.io.

- *Utility tokens.* These tokens enable the user to consume some good or service specific to the platform (Hu, Parlour and Rajan 2018). The classic example of a utility token is Ethereum's ether.

This broad categorization is used by some securities regulators, such as the Swiss regulator Finma (Finma 2018). There is still much debate on the exact definition and boundaries between these categories. The difficulty for regulators is not only that there are shades of grey between different types of cryptoassets.[7] They also may change types over the lifecycle of a project; many that start off primarily as a fundraising tool (i.e., a security token) are intended to eventually be either a currency or a utility token. The issue of evolving purpose and use is hardly new. The Octopus card in Hong Kong started off as a means to pay bus fare, but over time the number of goods and services that could be paid for with this card has multiplied to include goods such as fast food and coffee (Ma et al. 2008).

Unfortunately, the data are not categorized precisely along these lines, so we will focus on what is available. The dataset provided by coinmarketcap.com disaggregates the cryptoasset market into four broad buckets. The first two buckets are simply bitcoin and ether, the two most prominent assets in this space.[8] The next bucket is called altcoins, which are mined and exchanged using their own blockchains; these include Litecoin or Dogecoin. The final and newest bucket is for tokens that are programmed and exchanged on general purpose blockchains, such as the Ethereum blockchain; examples of these are the many ICOs that have happened in recent years.

*The second observation about the cryptoasset landscape is that trading volume has exploded over the past year and a half (**Chart 1**).* While cryptoassets may not yet be prominent enough to pose immediate financial stability concerns, they are prominent enough to warrant active monitoring and assessment.[9] In fact, the trading volume of cryptoassets is currently about the same as that of US municipal bonds, which is also roughly the same as that of Canadian-dollar spot foreign exchange markets.[10] Moreover, during the peak of trading in 2017, Bitcoin and tokens rivalled US corporate bond trading volumes. This raises the question of how the composition of the market has changed over time.

---

[7] Walch (2019) discusses how decentralization should be thought about in the context of the determination of a cryptoassets type.

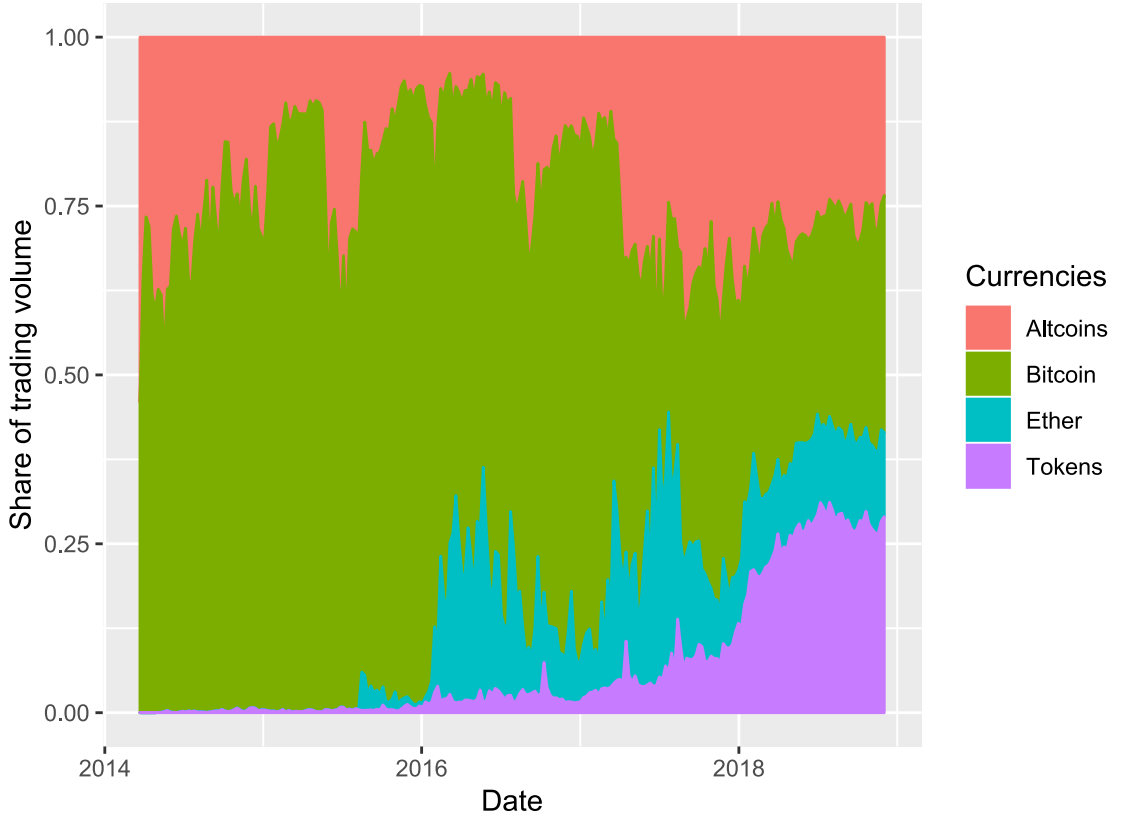
[8] Bitcoin is the largest, oldest and most liquid of the cryptoassets. Ethereum is becoming the de facto standard blockchain used by most other distributed applications and tokens.

[9] The Financial Stability Board assessed that cryptoassets do not yet appear to pose issues for financial stability but that this could change rapidly given the pace of change in this market as such it also developed a monitoring framework for cryptoassets (FSB 2018).

[10] According to a survey conducted by the Canadian Foreign Exchange Committee, daily volumes in April 2018 were about US$20.7 billion for the Canadian-dollar spot market and the daily volume for all cryptoassets was US$19.5 billion in the same period. See www.cfec.ca.

*The third observation is that, while bitcoin may still be the rock star in this asset class, it appears to be aging fast (**Chart 2**).* Bitcoin had the lion's share of weekly trading volumes, measured in US dollars, as late as 2015; however, its share fell below 50 per cent in 2017 as other cryptoassets gained market share. Trading in tokens (cryptoassets that do not have their own blockchain) and altcoins has increased to around the same volume as bitcoin, while ether is holding its own.

Chart 2: Share of weekly trading volume by asset type



Source: Coinmarketcap.com Last observation: November 30, 2018

*The fourth observation is that the market for tokens is like a revolving door (**Chart 3**).* Entry and exit of these cryptoassets started to pick up quite smartly in 2015, coinciding with the introduction of Ethereum, which became a primary platform for most cryptoassets.[11] The introduction of cryptoassets such as Ethereum, Litecoin, Monero and EOS, among many others, show that at least some of the entry of new coins and tokens represents a kind of creative destruction with new coins and tokens improving on older coins and tokens.

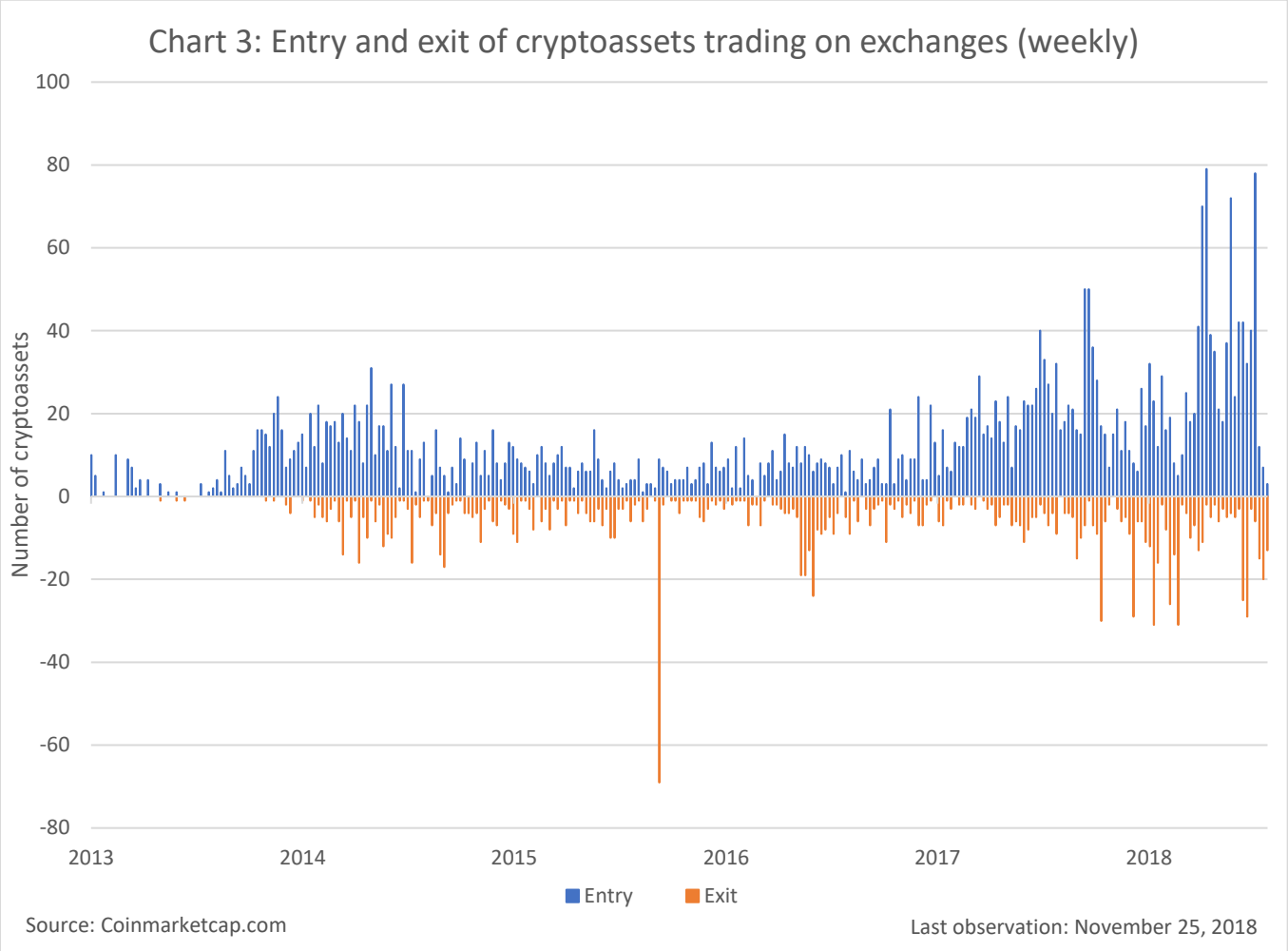
Even as the number of cryptoassets traded really took off in 2017, many assets failed. This may have been due to failure of the cryptoasset (e.g., there was no interest in the asset, or it was a scam).[12] It may also have been due to the failure of the exchange itself, which left the cryptoasset without a trading venue. For example, there was a spike in exits in the second week of 2016 when the Cryptsy exchange failed.[13] This turnover in the cryptoasset space also implies that, as

[11] There is a potential survivorship bias in this dataset because the pricing data are not recorded from crypto exchanges automatically. Instead, promotors of a cryptocurrency can contact the website for inclusion (coinmarketcap.com) subject to a few conditions (for details, see coinmarketcap.com FAQ).

[12] The website deadcoins.org is a good resource for the reasons different cryptoassets failed.

[13] Analysis revealed that virtually all these cryptoassets ceased to be mined by early 2018. Those that were still being mined were being mined by only a small number of miners (i.e., less then a dozen machines).

Lane (2018) points out, regulators need to examine cryptoassets from a number of angles, including the integrity of markets and investor protection, to ensure investors can trust these markets. The steep drop-off of in new assets at the end of our sample is likely partly due to the collapse in prices of cryptoassets. But part of this collapse in prices is also likely due to this lack of regulation until recently, subsequent fraud in the ICO market and, hence, lack of trust.

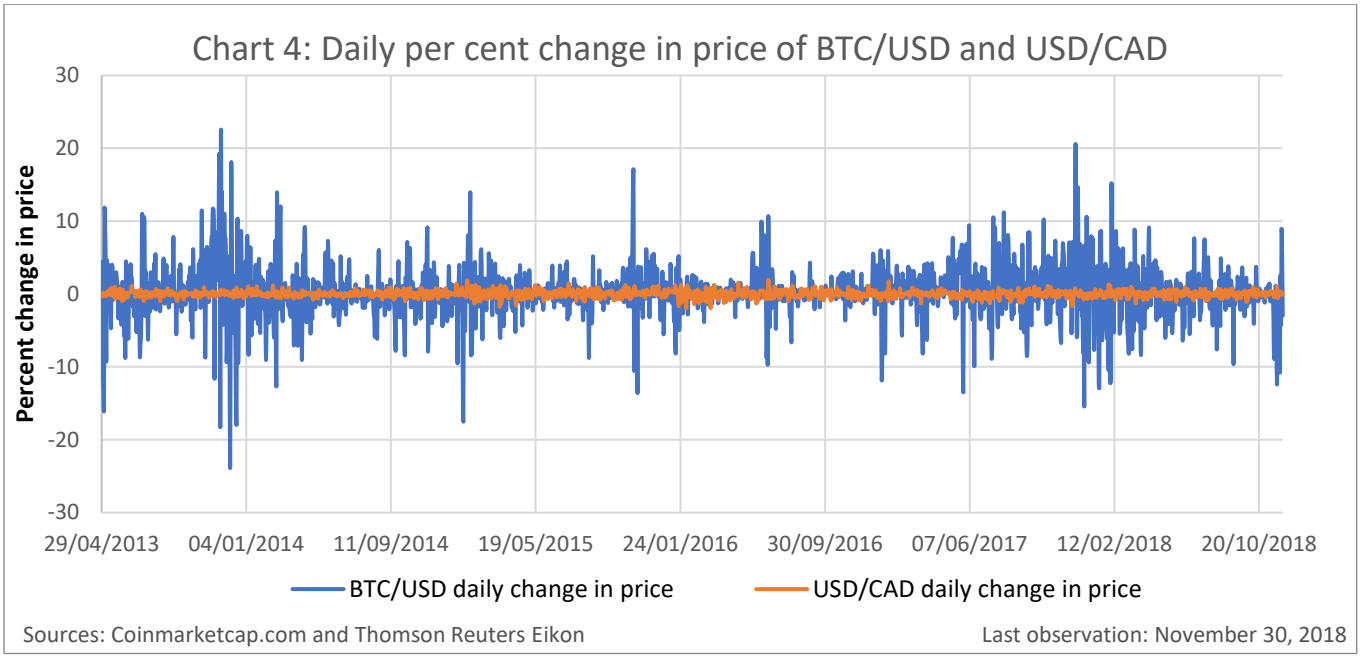


*The last observation is that the volatile price of cryptoassets makes them a very poor means of payment (**Chart 4**).* Bitcoin's shortcomings as a payment medium were highlighted by Wilkins (2014) and by many others.[14] Further experience and research has supported this. The BTC (bitcoin)/USD exchange rate compared with the volatility of the CAD/USD exchange rate is a common example of this point. The high price volatility of bitcoin imposes a large short-term risk to its users, and the relevance of this risk is accentuated by the fact that bitcoin is not the unit of account in most cases, for either goods and services or wages. In the early stages of cryptocurrency adoption, it is common to see a steep increase in the exchange rate due to

[14] More recent comments by Carstens (2018) and BIS (2018) make similar points.

speculative motives, opening the door to price "bubbles" (Bolt and Van Oordt 2016; Athey et al. 2016).

In fact, recent studies support the idea that the majority of those who hold cryptoassets do so for investment purposes, not for transactions. Recent research finds that a substantial amount of the volume of transactions take place in exchanges, with the implication that investors play a major role in the transaction volume of bitcoin. For instance, Brauneis et al. (2018) find that, by May 2018, 90 per cent of all Bitcoin exchange volume was accounted for by volume on exchanges.[15] They also find that a relatively small amount of bitcoin is used for purchases or other transactions, legal or illegal. Supporting Canadian evidence comes from recent surveys of bitcoin use in Canada by Henry, Huynh and Nicholls (2018, forthcoming). These surveys find that as the price of bitcoin has risen, so has the interest in and ownership of it. Henry, Huynh and Nicholls (forthcoming) find that 58 per cent of bitcoin owners hold it for investment purposes. Only 10 per cent of those who own bitcoin say the main reason for owning it is payment related.



3. Do cryptoassets offer something fundamentally new?

Given the rapid growth and popularization of cryptoassets since their creation, the natural question is whether aspiring cryptocurrencies promise something fundamentally new in terms of economic services. Is the label "revolutionary" justified in that they could eventually remove the need for trusted third parties?

[15] Athey et al. (2016) find similar results.

Innovation in financial services, including means of payment, is hardly novel. Even though the financial system has become more elaborate in many ways over time, financial intermediation and banks have been around since well before Shakespeare had Polonius instruct his son to "neither a borrower nor a lender be."[16] Money has changed throughout time; from cowrie shells in 1200 BC, to early coins, to, finally, paper money. In fact, debt itself was at one point a financial innovation around 5,500 years ago (Graeber 2011).

To get to the bottom of what cryptoassets might deliver, and consider what open questions there are for research, it is best to start with what the underlying distributed ledger technology (DLT or "blockchain" in popular parlance) can deliver.[17] DLT, and its variants, essentially offers two main economic services: one is well established and the other innovative.

The well-established service is recordkeeping in a ledger. There is evidence of bookkeeping as far back as 3300 BC (Gleeson-White 2012). Double-entry bookkeeping emerged in commerce in 14th century Italy (Peragallo 1969) and has been credited by economic historians for nothing less than the birth of capitalism (Yamey 1949).[18] In fact, the monetary economics literature has argued that money itself is essentially another form of imperfect recordkeeping using physical tokens in a decentralized setting (Ostroy 1973; Townsend 1987; Kocherlakota 1998).

The innovative service lies in the distributed consensus mechanism. This mechanism defines how the community comes to a consensus in updating the ledger (i.e., adding new blocks in the blockchain). This is foundational to avoid dissent about the correct state of the blockchain and possible manipulation by any individual.[19] The method for achieving consensus is often based on cryptographic proof of work.

In some cases, the ability to modify this ledger is open to all (e.g., Bitcoin and Litecoin), while in others it is restricted to pre-approved users. This latter case is termed a permissioned blockchain (e.g., Ripple and Hyperledger). The key feature of blockchain systems is that records are ordered and bundled in blocks that are linked together to form a database of every transaction ever made. The blockchain structure is innovative because it makes older records immutable and allows information sharing among all participants.[20]

In this way, the blockchain constitutes a shared communal memory for the users. Blockchain technology allows records to exist in a decentralized way in a digital context. Most important is the ability to append such a digital ledger through a distributed consensus mechanism among

---

[16] Shakespeare, *Hamlet*.

[17] Blockchain is a specific type of a distributed ledger. Other non-blockchain DLTs exists, such as R3 Corda or IOTA's Tangle network. Since we are not focusing on these technical details, we will use DLT and blockchain interchangeably in this paper.

[18] This was because it prompted a new way of looking at capital (capital = assets – liabilities).

[19] In computer science this is known as the Byzantine General's problem (Lamport, Shostak and Pease 1982). It is a classic problem in distributed data processing, and the key innovation in Bitcoin was a solution to this problem.

[20] While immutability is innovative by allowing widespread sharing, it does pose some operational challenges since it makes errors more difficult to fix.

strangers without recourse to a centralized authority. This distinguishes it from other types of record keeping.

This could result in important efficiency gains for users in many applications within and outside the financial system by removing redundancy in current record-keeping mechanisms that are often fragmented and require multiple points of input and verification by intermediaries. Improved efficiencies would be more than welcome given the age and need for renewal of many legacy systems. Potential efficiencies and the need to update legacy systems are two of the reasons many organizations, including the Bank of Canada, are conducting experiments using blockchain technology.

That said, these experiments show that efficiency gains are not always realized, especially when the existing system is already very efficient. The initial phases of the Bank of Canada's project to experiment with a DLT-based interbank large-value payments system is an example of this kind of result, mainly because the existing system is highly centralized and efficient.[21] That said, efficiency gains may be more likely in other payment systems that are less efficient, for example, because they involve multiple intermediaries across jurisdictions. This is one reason why the Bank of Canada, Monetary Authority of Singapore and Bank of England have examined cross-border payments and uses of DLT in this process.[22]

It is also critical to understand the underlying economic mechanisms embedded in the technology and any specific application. In fact, this lies at the heart of much of the research and remaining questions around DLT and cryptoassets.

The consensus mechanisms used in blockchain applications prevent cheating by creating competition over who (a "miner" in cryptocurrencies such as bitcoin) can validate and add a block of transactions to the blockchain. A popular type of consensus mechanism is the proof-of-work (PoW) protocol where miners expend work to have a chance to be the miner chosen by the system to update the blockchain. As we will examine below, these consensus mechanisms have different incentive effects. These mechanisms aim to protect against common forms of cheating, such as spending the same token twice (the so-called "double-spending problem"). One issue with decentralized consensus is that it naturally places limits on the speed of updates to the shared ledger and hence a limit on how a blockchain could scale (BIS 2018, 99).

The decentralized incentive structure is purported to be "trustless." However, it is not completely trustless in general; there is no need to trust your counterparty, but there is a need to trust the protocol, its developers and the miners. One example of a vulnerability that can arise in the system design is the possibility that the ledger could be distorted by a 51 per cent attack.[23] This is not just a theoretical possibility; several altcoins, such as Bitcoin Gold, have had issues due to

---

[21] Chapman et al. (2017).

[22] See Bank of Canada, Bank of England and Monetary Authority of Singapore (2018).

[23] A 51 per cent attack is a situation where a miner or a group of miners, for financial gain, controls the majority of computers working on validating transactions and therefore allows the miner or miners to manipulate the blockchain and selectively reject and confirm new transactions.

51 per cent attacks in which miners have banded together to manipulate the ledger.[24] Trust in the people who develop the computer code that supports the cryptoasset is also critical. Users need to know that the code is free from bugs, is resilient to tampering and does what it claims. The issue with the Bitcoin "Bug" that came to light in September 2018 is an example of why this is important.[25]

These issues have raised many important lines of inquiry for researchers. They relate to the sort of incentives the various actors in the cryptoasset space have and how these incentives differ from those faced by more traditional financial sector actors. This set of incentives presents a new twist on traditional research questions. For example, in terms of corporate governance problems, what incentives does an ICO provide to a firm to complete the ICO's token platform? With respect to open source development of cryptoassets, how does the development community organize and govern itself?[26] In in addition to governance, an important issue for legal experts to pursue is whether coders have fiduciary duty (Walch 2018).

Blockchain technology also presents economic problems that are, at least in part, novel. One intriguing example is the so-called "blockchain trilemma" recently articulated by Abadi and Brunnermeier (2018). They show that, in the case of a general blockchain, an ideal ledger should be (i) correct, (ii) decentralized and (iii) cost efficient. They then lay out an argument and a model suggesting that no ledger can simultaneously meet all three criteria. This trilemma comes from the incentives for potential forking and verification of the blockchain. For example, a permissioned blockchain could be correct and cost efficient. However, it is no longer completely decentralized, and users with permission to write to the blockchain could have economic rent from controlling the updating process to the blockchain, further reducing efficiency. In contrast, an open blockchain like Bitcoin may be decentralized and correct, but this comes at the cost of efficiency since a PoW protocol is needed to provide the appropriate incentives.

We can see aspects of this trilemma in play right now. For instance, Bitcoin is decentralized and the ledger is essentially correct. But the structure is very inefficient. The consensus process is onerous to ensure the correctness of the ledger. This is done by imposing a computational burden in the form of a very high energy cost, as well as a slow speed for processing transactions. We give a rough estimate that this cost could be higher than 20 times total annual Canadian electricity consumption if bitcoin was used for all Canadian retail payments. In contrast, as mentioned earlier, the second phase of the Bank of Canada's Project Jasper used a different DLT that was correct and more efficient, but substantially more centralized.[27] An outstanding question is whether further improvements to the technology could eventually reduce the practical

---

[24] Kharif (2018).

[25] For more details, see Hertig (2018) and Van Wirdum (2018).

[26] Read Lerner and Tirole (2002) for some of the ongoing questions around open source development. Many of these questions carry over in some form to cryptoasset and blockchain development.

[27] Project Jasper phase 2 and phase 3 used Corda, which has a centralized notary to achieve consensus.

importance of these trade-offs (e.g., by finding cheaper mechanisms to ensure correctness of the ledger without resorting to increased centralization).

The incentive structure itself presents another novel economic problem. Recent research by Chiu and Koeppl (2018) uses a model of economic behaviour to formalize the economic incentives of the PoW protocol in a bitcoin blockchain. They show that the constraints that PoW put on the blockchain consensus problem to avoid double spending of bitcoin are similar to incentive compatibility constraints in mechanism design.

While PoW is the most common type of consensus mechanism, there are other types of mechanisms such as proof-of-stake (PoS) and practical Byzantine fault tolerance (PBFT), that are under active development in the cryptoasset space.[28] There is a new line of academic research on whether these other consensus mechanisms could also support cryptoasset trading and blockchains (e.g., Saleh [2018] for PoS).

Further unanswered questions relate to the place cryptocurrencies hold in the larger financial ecosystem. Rather than eliminating the need for intermediaries, many different types of financial services have emerged because they are better at solving market frictions (access, security, matching, asymmetry of know-how) than individual users of cryptocurrencies are. These services include digital wallets, payment gateways and exchanges. They rely on centralization and the corresponding need for trust in their services. This potentially allows for risks related to market integrity and consumer protection, including fraud, market manipulation, money laundering and terrorist financing. While not a risk to financial stability at this point, the Financial Stability Board has recognized the importance of monitoring the evolution of the assets and the surrounding ecosystem (FSB 2017, 2018).

The bottom line is that cryptoassets and the underlying blockchain technology may allow for some efficiency gains, at least under certain circumstances (e.g., by eliminating third-party verification). That said, this may come at the expense of reduced efficiency from the consensus mechanism. Moreover, and rather ironically, the need for trust in a third party and intermediaries has not been eliminated as envisioned by some proponents; it has only been shifted.

4. Implications for a central bank's role in monetary policy

So what implications do cryptocurrencies have for a central bank's core mandate—monetary policy? The current inflation-targeting regime has served many jurisdictions very well over the past few decades. In the Canadian case this is explicit in the periodic renewal of the inflation-control target framework. The emergence of cryptocurrencies does not currently present any impediment to successful implementation of the monetary policy framework in Canada (or in other economies with solid monetary policy regimes). We also do not think that existing cryptocurrencies would provide a viable basis for an alternative framework in this context.

---

[28] The Practical Byzantine Fault Tolerance takes its name from the Byzantine Generals Problem, which deals with how a group (Byzantine generals in the original parable) can make a common decision with faulty communications between them and the existence of malicious general who may send fake messages. See Lamport, Shostak and Pease (1982) for a full description of the problem. Ethereum developers are actively developing Ethereum 2.0, which would use PoS instead of PoW (Bambrough 2018).

That said, the cryptoasset space is a useful laboratory in which to examine longer-term questions about whether a cryptocurrency could ever support a viable monetary policy regime. This is especially true because prominent cryptoassets, such as bitcoin, can be thought of as an asset and preprogrammed monetary policy combined. It is one of the reasons some investors in cryptocurrencies originally found them attractive; they provide discipline and commitment to a predefined monetary policy rule.

Take the bitcoin blockchain and protocol as an example. It was designed to be a sort of digital gold with a rigid increase in bitcoins through time to avoid manipulation by anyone. A thought experiment would be to imagine a monetary regime based on this, with bitcoin as a new version of a gold standard. Some bitcoin proponents support the idea of a digital gold for many of the same reasons that others argue in favour of a return to a gold standard (Paul 2011).

A cryptoasset standard or new gold standard would, in fact, likely eventually meet the same fate as the original gold standard. The main difference between bitcoin and gold is that bitcoin is created by the actions of miners who increase the supply in a programmed way, while gold supply comes from the random discovery of new gold mines and their extraction. Yet, bitcoin does not resolve the biggest issue: as with actual gold, this "digital gold" would not allow for a welfare-maximizing monetary policy to respond to shocks to the economy (Weber 2016). In both cases the long-run implication for both a gold standard and a bitcoin standard is deflation since there would be a fixed supply of money and an increase in the size of the economy.

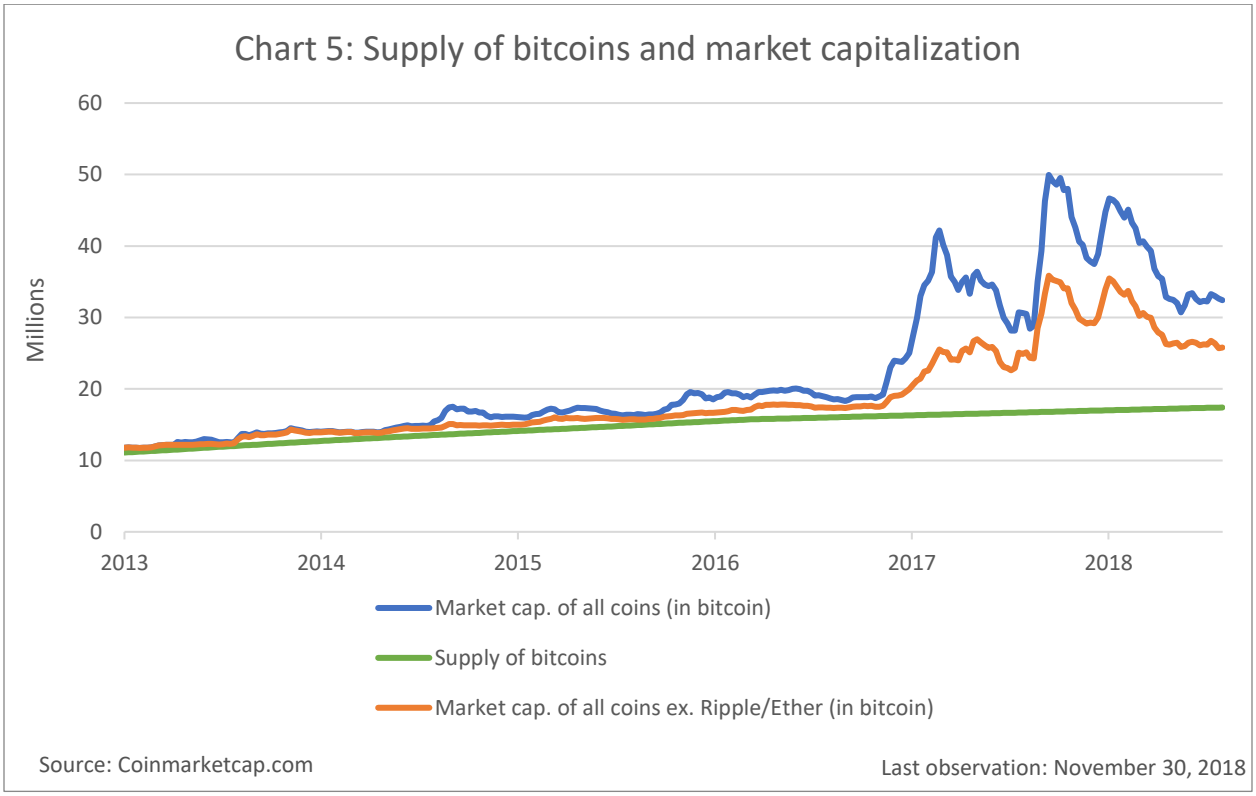
If the idea of a strict commodity standard based on a cryptocurrency has dim prospects, we could think of it in the context of a money supply target rule like what was attempted by the Bank of Canada from 1975 to 1982. We could imagine an economy where bitcoin was the primary currency would be similar to this kind of regime. This would not be an exact comparison since the Bank of Canada experience was to follow a money supply rule while a cryptocurrency standard would be an exact rule, since, in a protocol such as the bitcoin protocol, each winning miner gets a predefined reward for mining a block.[29]

It is likely this kind of a rule-based cryptocurrency regime would fail as well. Our experience with money growth targeting taught us the hard way that the demand for money is too unstable to be targeted as part of a monetary policy rule. Financial innovation led to financial institutions offering new deposit accounts and financial products that changed the public's behaviour. This, in turn, led of to a breakdown of the relationship between the money supply we could measure and inflation.

Another way to think about this is that the money demand of an economy fluctuates with economy activity. Financial institutions serve to create an elastic supply of bank deposits and other forms of inside money to meet this demand. This makes the link between money supply and inflation unstable. Williamson (2018) makes the point that bitcoin's supply function makes it unusable as a payment system for similar reasons; that is, by itself, it is not elastic enough to meet fluctuating demand at a stable price.

[29] The current reward for the winning miner to process a block of transactions is 12.5 coins. This amount is won, and a block created, every 10 minutes and will halve every four years (210,000 blocks) until about 21 million bitcoins have been mined.

We can see that, even though Bitcoin has defined an algorithm for a transparent supply function, which is stable and reasonably predictable, it is not the only supply of cryptoassets (**Chart 5**). As we saw in Section 2, financial innovation has resulted in growth in altcoins and other types of cryptoassets. There is nothing stopping someone from setting up a bitcoin clone or trying to make a better version. As demand for cryptocurrencies has prompted new crypto coins to be created, growth in the supply of crypto coins has become not only stronger but also less transparent and more unpredictable. The orange line in Chart 5 excludes Ripple's XRP and Ether, given their size and more specialized nature, while the blue line includes them.



One could argue all day about which of these assets are money—we have argued none of them is right now—and what drives the creation of new cryptocurrencies. If any cryptocurrencies were to become more like money, we could imagine a new crop of studies that would be reminiscent of research in the 1980s and earlier about monetary aggregates (M1, M1+, M2, M3 and so on). In this case, the chance of finding a stable cryptocurrency demand function would be made even more difficult because of the uncertainty of relative value of different cryptocurrencies. In general, the lack of frictions between different currencies means their relative prices are indeterminate (Kareken and Wallace 1981). The case of cryptoassets is no different, mainly because it is so easy to create perfect substitutes (Garratt and Wallace 2018).

The obvious implication of this is that it is quite unlikely that a regime based on cryptocurrency would be a viable alternative to a credible central bank at supporting domestic price stability. That said, how would domestic monetary policy be affected if cryptocurrencies were to become

more prominent as means of payment? First, it would be weakened if the use of cryptocurrency became prominent enough because monetary policy transmission requires borrowing and other transactions in sovereign currency. This situation would share similarities to dollarized economies (He 2018). In addition, even if monetary control were not completely lost, coordination issues could arise between the central bank whose objective was to control inflation and the private issuers whose objectives were to maximize profits (Zhu and Hendry 2019).

A common theme that emerges from many historical studies is that government regulation is required for peaceful coexistence of public and private money. In fact, this is an area where we have something useful to learn from history because national and private currencies with a common unit of account have coexisted in several jurisdictions and at different times in the past.

Weber (2015) argues that post-1864 national bank notes in the United States were able to form a safe uniform currency because of several government interventions: (i) federal government insurance; (ii) regulations so that the notes were redeemable in lawful money on demand at the issuing bank at face value, and a bank had to accept the notes of other banks at par in the payment of debts; and (iii) the introduction of a gross note clearing facility by the Treasury for national bank notes, with all clearing costs borne by the issuing bank.

In Canada, a high level of government regulation was also required to ensure that private bank notes were a safe and uniform currency (Fung, Hendry and Weber 2017). Canada achieved uniformity through double liability of bank shareholders, bank notes being the first lien on a failed bank's assets, a private sector bank note insurance scheme, and a strong mechanism for the redemption at par of bank notes of other banks at the expense of the issuing banks.

The experience of Sweden has a slight nuance that is relevant; in the Swedish case, government intervention was not required to achieve private bank note uniformity. This was probably because government notes were strongly in place before private bank notes (in contrast to the United States and Canada where private notes came first), so the private banks may have set up the mechanism for par exchange to become a competitive alternative (Fung, Hendry and Weber 2018). Nonetheless, significant government regulation was still used to ensure that private notes were safe instruments.

Each of these historical episodes are peppered with instances of financial stress: the panic of 1907 in the United States prompted the creation of the Federal Reserve System. Yet, many of the theoretical models that look at how the co-existence of sovereign and private monies would affect monetary policy assume essentially a stationary environment in terms of economic institutions that includes the use of one dominant currency. It would be interesting to see how the results would change in an environment of financial stress or if coexistence could in and of itself create the stress. At a minimum, constraints on the central bank's ability or willingness to provide services of lender of last resort in cryptocurrency (as opposed to sovereign currency) would be very relevant.

5. What about a central bank digital currency?

Given all these innovations, a key question is whether a central bank should issue its own digital currency. This question is precipitated not only by the emergence of cryptocurrencies but also by technological advances such as increased acceptance of debit and credit cards at retailors and the increase in online shopping that have hastened the decline in the use of cash.

By digital currency, we mean a central bank digital currency (CBDC) used by the public to conduct retail transactions and also usable as a store of value; implicitly, this also suggests continued use of central bank liabilities as the unit of account. The idea of a CBDC it is one of the most important questions related to money and means of payment that governments and central banks have faced in a very long time.[30] The Swedish Riksbank is particularly advanced in work in this area, and the Bank of Canada, the Bank of England and others are also pursuing longer-term research on CBDCs.[31]

To inform discussion on whether a central bank should issue a CBDC, many related research questions will need to be addressed.[32] We will focus on the following three:

- Should we care about the decline of the use of cash as a means of payment and a store of value?
- What are the exact roles that fiat currency plays in a modern economy?
- How would the risks to the financial system differ if there were a CBDC?

Implications of the decline in the use of cash

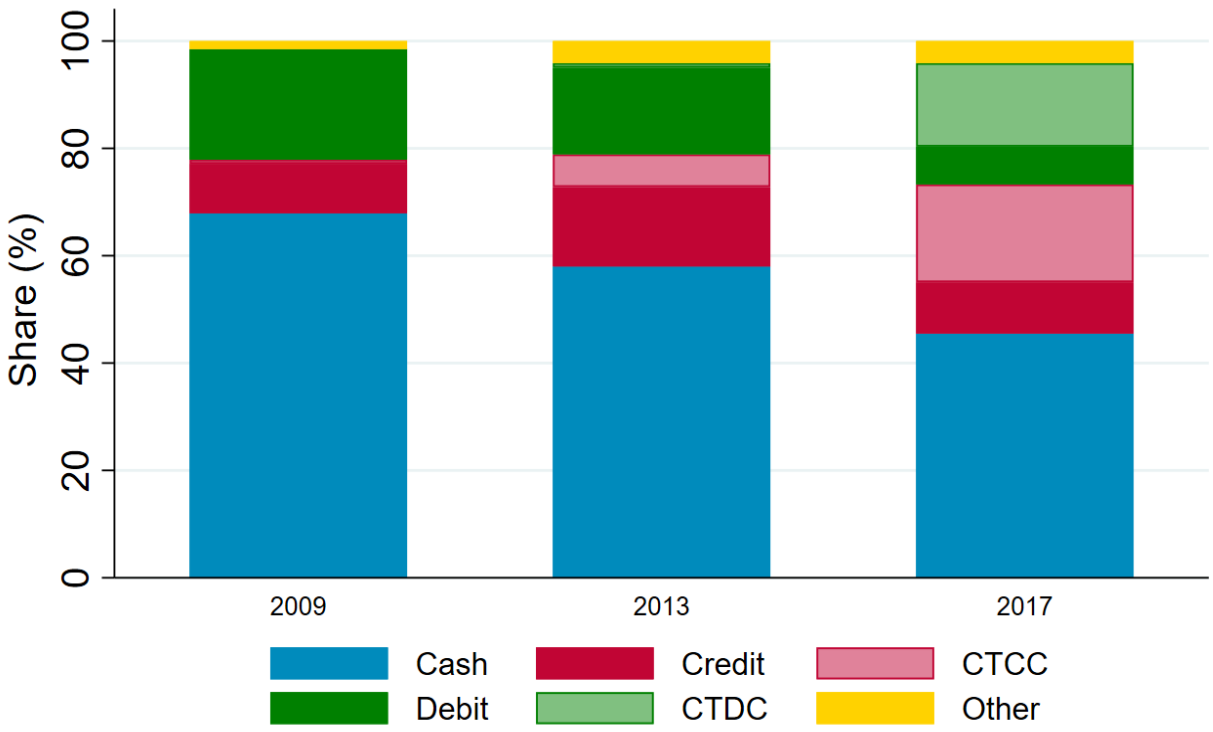
The use of cash at the point of sale has been decreasing over the past 10 years in a number of advanced economies. The share of cash transactions in Canada has declined substantially, by about one-third in the past eight years, mainly replaced by debit and credit, including contactless methods (**Chart 6**). Moreover, people have become more open to using other means of payment beyond debit and credit. For example, adoption of mobile payment apps tripled from 2013 to 2017. Digital currency ownership and usage for transactional purposes remain relatively low (Henry, Huynh, and Nicholls forthcoming; Henry, Huynh and Welte 2018). This trend of increasing non-cash payment usage is common across different countries (Bech et al. 2018).

[30] The issue has been raised in many jurisdictions. For example, in the United States, the Subcommittee on Monetary Policy and Trade, US House of Representatives, held a hearing entitled The Future of Money: Digital Currency, in which witnesses were asked to testify on "the merits of any uses by central banks of cryptocurrencies."

[31] See the Bank of Canada's most recent medium-term plan, its digital currency webpage and the Riksbank reports.

[32] An interested reader is invited to read Engert and Fung (2017) who examine the different motivations for a central bank issuing a CBDC and the implications of this issuance.

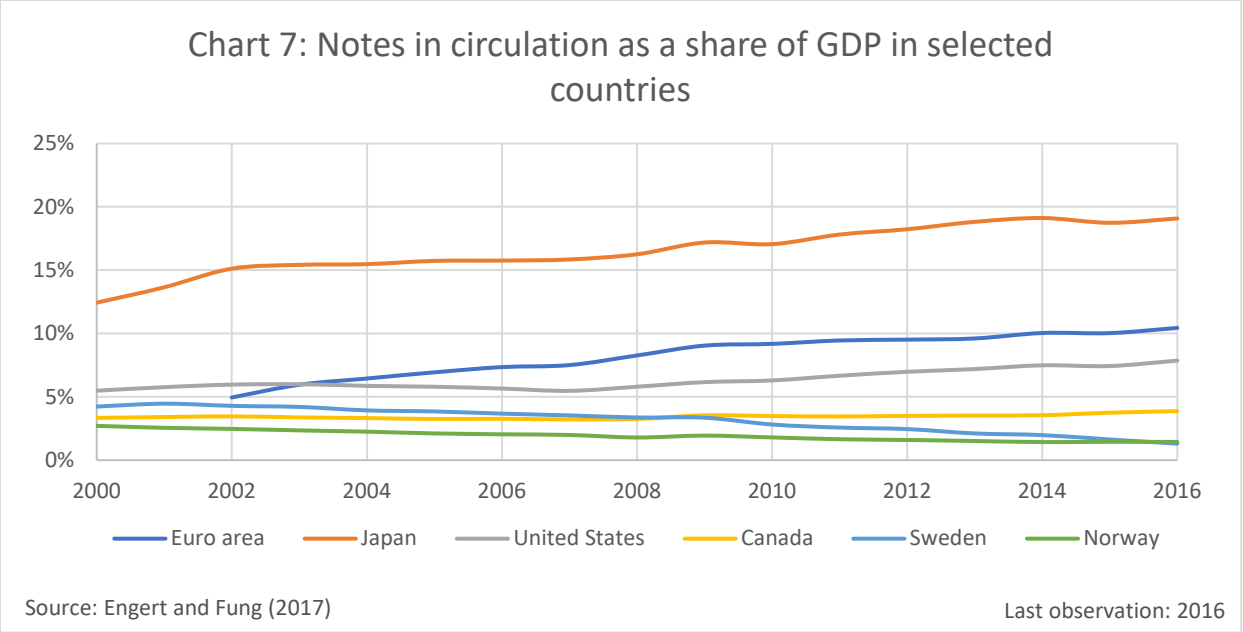
Chart 6: Share of different means of payment for transactions less than $15 in Canada



Note: CTDC refers to contactless debit cards, and CTCC refers to contactless credit cards.

Source: Henry, Huynh and Welte (2018)

While cash use has declined markedly, cash holdings have remained constant or even increased as a share of nominal GDP for most advanced economies over the past 10 years (**Chart 7**). Obvious exceptions to this trend would be Sweden and Norway. Research suggests that this increase in cash holdings is being driven by demand for large-denomination notes primarily for use as a store of value (Bech et al. 2018).



A central banker may not need to worry about the decline in use of cash for several reasons. First, social welfare may be enhanced because the private sector may be more innovative in the introduction of new means of payment that could be faster and easier than cash in some transactions (Chiu and Wong 2014). Second, the impact on a central bank's revenue model in terms of lower seigniorage revenue could be mitigated by various means, such as charging fees and charging for overdrafts, or by government financing. Third, a central bank could still fulfill its mandate as long as private inside money is denominated in sovereign currency and there is the right regulation and structure (Engert, Fung and Hendry 2018).

That said, there are also reasons we might worry about these trends. The elimination of cash by the public would rob it of access to a means of payment that is unique—both legal tender and a risk-free store of value. Cash also competes with other private means of payment. This is important to reducing the economic rents in this sector of the economy and is a means for depositors to exert discipline on financial institutions.

While many may take cash for granted, it performs a crucial role as the default option in the vast majority of retail transactions. This role means cash has a central place in the economic life of people; it is still the most widely accepted means of payment at the point of sale and the most accessible to all users regardless of access to the financial system (Henry, Huynh, and Welt 2018). In this sense it is also a socially inclusive option because people do not need a bank account to use it to buy goods and services, unlike many electronic payment systems (Chiu and Wong 2014).

This accessibility relies on a two-sided market whereby the use of a means of payment by a consumer needs to be balanced with its acceptance by the merchant (Rochet and Tirole 2003). In these types of markets, the reduction in the use of the platform on one side of the market may cause a reduction in its acceptance on the other side and eventually lead to a collapse of the

platform.[33] That means that a reduction in the use of cash by consumers may lead to it no longer being widely accepted as a means of payment, as we have seen in some Nordic countries (Sveriges Riksbank 2017, 2018). In addition, due to network externalities it may be the case that this collapse in cash may be sub-optimal.

Without cash as a competing means of payment, the remaining payment providers could have increased market power, which would lead to decreased competitiveness and possibly higher prices for payment services for consumers and merchants. In addition, some may find they have decreased access to payment services (e.g., people living in remote regions). In this situation, a properly designed CBDC could allow continued access to a competitive means of payment for all users.

A well-designed CBDC could also provide a few additional benefits relative to bank notes. First, it could promote competition among online payment providers, which is an area where physical cash is deficient. Second, it would make it safer to settle large transactions in central bank money by reducing the risk of theft.[34] Third, if there were a separate payment system for the CBDC, there is a potential to reduce operational risk in the system by diversifying methods of payment. This also implies it would be beneficial to keep physical currency available in the case of a large-scale cyber event, provided there were adequate contingencies for cash distribution systems.

The role fiat currency plays in a modern economy

This leads to the second question. Is there a public interest reason for a central bank to issue a CBDC? The first place to start in answering this question is to consider whether the use of money is a public good.[35, 36] We argue that it is:

- *The use of money as a means of payment is non-rivalrous.* Although the object of money most certainly is rivalrous, the acceptance of money in return for goods by one person does not prohibit or affect the acceptance and use of money by another.

- *The use of cash is non-excludable in its current form*. Anyone can use cash. It is akin to a token that does not depend on a network (or other infrastructure) to ensure that settlement of a transaction is successful or that a user has a store of value. Other methods of payment can exclude consumers, which is part of where the potential for market power comes from.

---

[33] A classic example in the literature is a video game system where few buyers of the system lead to fewer video games being developed for it by developers, leading to lower sales and even less demand for it, and so on.

[34] This would depend crucially on whether a CBDC is anonymous and a bearer instrument. The latter would imply that a reduction in the threat of theft would be negligible.

[35] The criteria of a public good are that it is non-rivalrous and non-excludable.

[36] Tobin (1987) makes a similar case for central bank digital currency, that the public good is the trust in the system.

A subtler public benefit from the provision of central bank money is that its availability as a ready asset helps underpin trust in the financial system. This is because it provides an outside option to all people who conduct financial transactions—from buying groceries to buying derivatives.

An outstanding question is whether the use of a CBDC could also be a public good like the use of money. This is a question for economic research to answer because the nature of physical cash usage as a public good may be tied, in part, to its form. An important role in the near term for monetary theorists is to understand what characteristics of physical cash make it essential to the economy and whether a CBDC with those characteristics would also be essential.[37] For example, certain design features could make CBDC more excludable than cash (e.g., if the central bank were to restrict access or prevented certain types of transactions).

A related set of questions, which are both policy-related and practical, touch on what form should a CBDC take. For instance, should a CBDC be anonymous like cash or simply private? While this is largely a policy choice, it could be informed by a much better understanding of the social value of privacy (a question that extends well beyond simply CBDC design to other areas, such as data). Other design choices relate to whether it should be account- or token-based and whether it should bear interest.[38] As you will see below, these choices have implications for how well a CBDC might support or undermine the stability of the financial system (Lane 2018).

Financial system implications of a private versus central bank digital currency

As we have argued, physical cash has traditionally filled the role as a safe store of value that is very liquid since it is the default means of payment. This is important not only for individuals but also for the financial system as a whole.

One of the key functions of a financial system is to match savers with investors. It does this through maturity transformation of long-term and illiquid investments into short-term liquid instruments, such as bank deposits and shares in money-market mutual funds (MMFs). This transformation is beneficial to economic welfare because it provides insurance against the unexpected need for liquidity (Diamond and Dybvig 1983). It also provides market discipline (Calomiris and Kahn 1991) and deals with lack of commitment in contracting (Brunnermier and Oehmke 2013). This maturity transformation/liquidity provision makes the financial system inherently fragile and prone to crises and flights away from risky assets.

The use of a digital currency raises several concerns with regards to the financial system, regardless of whether it is public or private.

[37] Recent research at the Bank of Canada on this issue is summarized in Davoodalhosseini and Rivadeneyra (2018).

[38] For an example of interesting discussion of some of these design features, see Bordo and Levin (2017).

A private digital currency could very well increase the fragility of the financial system through issues such as credit risk and misaligned incentives:

- It would not serve as a good risk-free store of value without the proper backing. This would cause problems for the financial system and economy in the event of a crisis, for two reasons. First, the operator (if there is one) may not consider the network externalities involved with the operation of a digital currency, especially in a crisis. Second, when faced with aggregate uncertainty, private sector claims (inside money) cannot provide the same level liquidity as public sector claims (Holmström and Tirole 1998).

- Depending on the design, it could increase the speed with which funds move from the banking system. Such fast movement of funds could be especially problematic if the issuer has objectives that differ from maximizing social welfare.

- A private issuer (or in the case of a cryptocurrency, the creator or operators) would not internalize the network economies inherent in payment systems sufficiently to invest in appropriate operational safeguards. A successful digital currency would have potentially large network economies in use, like all payment instruments exhibit, and could become too big to fail.

We can see how some of these drawbacks could materialize in the case of stable crypto coins, such as Tether. Stable coins are cryptocurrencies designed to provide a stable one-to-one exchange rate with the US dollar (or some basket of currencies) and act as a safe store of value in the cryptoasset space.[39] The creation and redemption mechanism is like an MMF in that it is backed by safe assets, such as insured bank deposits or government securities. In this set up, an investor can trade the reference currency in exchange for the stable coin at a fixed price. This reference currency is then used to buy collateral that backs the stable coin. These stable coins could be vulnerable to runs like MMFs were during the financial crisis, especially if it is not transparent what backs them and if the coins are the liability of the issuer (as is the case with centralized stable coins). If they are not fully backed by safe assets, holders of stable coins may suffer losses in the event of a default of the issuer.[40]

[39] Stable coins use different mechanisms to maintain parity with their reference currency or currencies. Some, such as Tether, are centralized and the coins are backed by assets such as bank deposits held by the issuer of the coin. Others are decentralized, such as Synthetix, are backed by other cryptoassets as collateral and are pegged to have a stable price relative to a fiat currency such as the US dollar.

[40] See Hochstein (2018) for the case of verifying the safe asset holdings of Tether.

A CBDC could circumvent some of these issues and thereby achieve relatively higher social welfare:

- A central bank, by design, has the public interest in mind when it conducts its operations.[41] It would therefore consider any externalities that arise due to the issuance of a digital currency. This, of course, implies the need to understand and quantify, if possible, the extent of the network externalities of a payment system.

- A CBDC would not be a debt of any private individual and, hence, not subject to counterparty credit risk. Not only is this advantageous in stable times to provide some market discipline to banks and competition with bank deposits, but it would also provide a safe haven for people in the case of systemwide financial stress. This is crucial since liabilities of private agents in the economy would all be affected in this type of event and would therefore not be a safe store of value.[42] In contrast, a CBDC would be a liability of the central bank and be backed by the resources of government, which has a unique position relative to private sector agents in that it is not subject to default in its own currency. An interesting question for research in this regard is the extent to which deposit insurance provides a viable substitute.

However, the fact that a CBDC would compete with bank deposits and provide safe haven is a doubled-edged sword. Currently, there is a tension between the use of physical cash and other interest-bearing liquid financial assets as a store of value, in large part because of the storage costs of bank notes. This tension helps determine the demand for bank deposits relative to cash. The introduction of a CBDC could fundamentally change the demand for bank deposits, both in normal times and during a financial crisis. This change would depend on the design of a CBDC and the sensitivity of demand deposits to the interest rate.

For instance, if a CBDC were interest-bearing and account-based (e.g., a deposit at the central bank), it would provide direct competition with bank deposits in normal times, as well as a place to run in the case of concern about bank safety. A key benefit of a CBDC during a crisis is that it would be a safe store of value, but could directly increase the likelihood and speed of a bank run if it is not properly designed to mitigate this risk. One would expect that the issue would be somewhat diminished if the CBDC were dissimilar to a bank account, for example, token-based, and especially if it did not bear interest. In addition, it is possible for central bank to design policies (e.g., lending facilities to banks) to at least reduce risks to financial stability (Andolfatto 2018).

---

[41] For example, the *Bank of Canada Act* makes it clear that the mandate of the Bank is to "regulate credit and currency in the best interests of the economic life of the nation…" https://laws-lois.justice.gc.ca/eng/acts/B-2/page-1.html#h-1

[42] An interested reader is encouraged to read Holmström and Tirole (2013), which gives a book-length treatment of the role of liquid asset creation in the private sector.

Clearly, we need to better understand how the economic decisions of bank depositors might change during a bank run when a CBDC is available; in fact, it is difficult to imagine how a central bank could achieve the appropriate design, let alone issue a CBDC, without further research in this area. A practical place for research to start could be to generate estimates of the interest rate elasticity of demand deposits and early guesses about the cross-elasticity of demand deposits and a CBDC. In general, it will be important to understand how changing dynamics between a CBDC and bank deposits could affect the macroeconomy, with an early example of research in this area by Keister and Sanches (2018). In this assessment, we also need to account for the benefits of strong discipline to private issuers of money-like instruments.

It is essential to make progress on the many unanswered questions related to whether the central bank should issue a CBDC, before some inadequate private digital currency gains traction as the de facto currency of an economy. In Canada, this seems unlikely right now because cash is still an important part of the economy (albeit declining) and the use of cryptocurrencies is very low. That said, it is possible that the technology and preferences could evolve quickly, particularly if some of the deficits of cryptocurrencies that we highlight above are addressed. In this case, central banks and governments should be ready to make informed decisions on how best to respond.

Conclusions and topics for further study

We are at an important juncture in the history of central banking. While cryptocurrencies do not appear to be gaining traction in advanced economies such as Canada, the situation is changing quickly. Trading activity in the broader cryptoasset class has risen to levels comparable to US municipal bonds and Canadian foreign exchange markets.

We have examined what cryptoassets bring to the table that is new and how cryptocurrencies and other private digital currencies might affect core central banking functions if they were to become more widely used. Like many, we think that the underlying technology to cryptoassets—blockchain—holds promise in terms of efficiency gains in financial services. That said, we argue that there are a couple of situational ironies in the cryptoasset landscape: the need for trust abounds in what is supposed to be a "trustless" technology; and what is purported to be a "decentralized solution" is highly concentrated. It is also unlikely that a cryptocurrency could form the basis of stable or desirable monetary policy regime. In fact, the money supply rule underpinning cryptocurrencies like bitcoin may turn out to be more of a disadvantage than an advantage in this regard.

Clearly the emergence of cryptocurrencies, paired with a declining use of cash in transactions, has increased interest in the question of whether a central bank should issue its own digital currency. The Bank of Canada, along with other central banks, is pursuing an active research agenda in this area. The place to start is to determine the conditions under which it would be in the public interest to issue a CBDC, if any. We argue that, while cash is a public good, a number of important policy and design questions need to be answered before determining whether a CBDC would be in the public interest. Clearly the implications for the broader financial system, especially deposit-taking institutions, need to be assessed in conjunction with other benefits and risks.

We have outlined what we think are the most important research and policy questions for central banks in this area, with the hope of providing some focus for ongoing work on the issue. These are related to gaining a better understanding of the following:

(i) *The underlying incentives of the various actors in the cryptoasset space, and how they might differ from those faced by more traditional actors.* The questions here are wide-ranging, from the incentives embedded in the different consensus mechanisms of DLT technologies to the trade-offs between trust and decentralization in the broader crypto ecosystem.

(ii) *How the co-existence of sovereign and private monies would affect financial stability and monetary policy under situations of financial stress, or if coexistence itself could create the stress.* Since no cryptocurrency currently serves as a good money right now, this set of questions is forward-looking and could benefit from models that can generate financial stress.

(iii) *The implications of a CDBC for social welfare, and related trade-offs.* The final question will require, at a minimum, answers to policy and design issues related to the public-good role that the use of physical cash currently plays and how a central bank can ensure this role continues as the use of physical cash declines. It also requires a better understanding of how bank funding and bank business models could change if a CBDC were available, and how a CBDC could be designed to mitigate the risk of potential destabilizing effects of bank runs.

We think it is an exciting time to be an economic researcher in this area; the results of this research promise to be useful and impactful and have the potential to fundamentally change the way modern economies and financial systems function.

References

Abadi, J. and M. Brunnermeier. 2018. "Blockchain Economics." Princeton University.

Andolfatto, D. 2018. "Assessing the Impact of Central Bank Digital Currency on Private Banks." Federal Reserve Bank of St. Louis Working Paper No. 2018-026B.

Athey, S., I. Parashkevov, V. Sarukkai and J. Xia. 2016. "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence." Stanford University Graduate School of Business Working Paper No. 3469.

Bambrough, B. 2018. "Ethereum Price Jumps on Major Bank Approval and Approaching Proof-Of-Stake." *Forbes*, November 5, https://www.forbes.com/sites/billybambrough/2018/11/05/ethereum-price-jumps-on-major-bank-approval-and-approaching-proof-of-stake/#7af7bd0a5621.

Bank of Canada, Bank of England and Monetary Authority of Singapore. 2018. *Cross-Border Interbank Payments and Settlements: Emerging Opportunities for Digital Transformation*. Joint report.

Bank for International Settlements (BIS). 2018. "V. Cryptocurrencies: Looking Beyond the Hype." BIS *Annual Economic Report 2018*: 91–114.

Bech M. L., U. Faruqui, F. Ougaard and C. Picillo. 2018. "Payments Are A-Changin' but Cash Still Rules." *BIS Quarterly Review* (March).

Bolt, W. and M. van Oordt. 2016. "On the Value of Virtual Currencies." Bank of Canada Staff Working Paper No. 2016-42.

Bordo, M. D. and A. T. Levin. 2017. "Central Bank Digital Currency and the Future of Monetary Policy." National Bureau of Economic Research Working Paper No. 23711.

Brauneis, A., R. Mestel, R. Riordan and E. Theissen. 2018. "A High-Frequency Analysis of Bitcoin Markets." Available at SSRN: http://dx.doi.org/10.2139/ssrn.3249477.

Brunnermeier, M. K. and M. Oehmke. 2013. "The Maturity Rat Race." *Journal of Finance* 68 (2): 483–521.

Calomiris, C. W. and C. M. Kahn. 1991. "The Role of Demandable Debt in Structuring Optimal Banking Arrangements." *American Economic Review* 81 (3): 497–513.

Carstens, A. 2018 "Central Banks and Cryptocurrencies: Guarding Trust in a Digital Age." Remarks at Brookings Institution, Washington, DC, April 17.

Chapman, J., R. Garratt, S. Hendry, A. McCormick and W. McMahon. 2017. "Project Jasper: Are Distributed Wholesale Payment Systems Feasible Yet?" Bank of Canada *Financial System Review* (June): 59–69.

Chiu, J. and T. Koeppl. 2018. "Incentive Compatibility on the Blockchain." Bank of Canada Staff Working Paper No. 2018-34.

Chiu, J. and T. Wong. 2014. "E-Money: Efficiency, Stability and Optimal Policy." Bank of Canada Staff Working Paper No. 2014-16.

Canadian Foreign Exchange Committee. 2018. "CFEC Releases Results of April 2018 Foreign Exchange Volume Survey." July 24.

de Vries, A. 2018. "Bitcoin's Growing Energy Problem." *Joule* 2 (5): 801–805.

Davoodalhosseini M. and F. Rivadeneyra. 2018. "A Policy Framework for E-Money: A Report on Bank of Canada Research." Bank of Canada Staff Discussion Paper No. 2018-05.

Diamond D. W. and P. H. Dybvig. 1983. "Bank Runs, Deposit Insurance, and Liquidity." *The Journal of Political Economy* 91 (3): 401–419.

Engert, W. and B. Fung. 2017. "Central Bank Digital Currency: Motivations and Implications." Bank of Canada Staff Discussion Paper No. 2017-16.

Engert, W., B. Fung and S. Hendry. 2018. "Is a Cashless Society Problematic?" Bank of Canada Staff Discussion Paper No. 2018-12.

Financial Stability Board. 2018. "Crypto-asset Markets Potential Channels for Future Financial Stability Implications." FSB Policy Documents.

———. 2017. "Financial Stability Implications from FinTech." FSB Policy Document.

Finma. 2018. "FINMA publishes ICO guidelines." Press release, February 16, https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/.

Fung, B., S. Hendry and W. E. Weber. 2017. "Canadian Bank Notes and Dominion Notes: Lessons for Digital Currencies." Bank of Canada Staff Working Paper No. 2017-5.

———. 2018. "Swedish Riksbank Notes and Enskilda Bank Notes: Lessons for Digital Currencies." Bank of Canada Staff Working Paper No. 2018-27.

Garratt, R. and N. Wallace. 2018. "Bitcoin 1, Bitcoin 2, ...: An Experiment in Privately Issued Outside Monies." *Economic Inquiry* 56 (3): 1887–1897. doi:10.1111/ecin.12569

Gleeson-White, J. 2012. *Double Entry: How the Merchants of Venice Created Modern Finance.* New York/London*:* W.W. Norton and Company.

Graeber, D. 2011*Debt: The first 5000 years*. New York: Melville House Publishing.

He, D. 2018. "Monetary Policy in the Digital Age." *Finance & Development* 55 (2): 13–16, International Monetary Fund, Washington, DC.

Hertig, A. 2018. "The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret." *Coindesk*, September 24, https://www.coindesk.com/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret.

Henry, C. S, K. P. Huynh and G. Nicholls. 2018. Bitcoin Awareness and Usage in Canada. *Journal of Digital Banking* 2 (4): 311–337.

———. Forthcoming. "Bitcoin Awareness and Usage in Canada: An Update." *Journal of Investing.*

Henry, C. S., K. P. Huynh and A. Welte. 2018. "2017 Methods-of-Payment Survey Report." Bank of Canada Staff Discussion Paper No. 2018-17.

Hochstein, M. 2018. "Tether Review Claims Crypto Asset Fully Backed – But There's a Catch." *Coindesk*, June 20, https://www.coindesk.com/tether-review-claims-crypto-asset-fully-backed-theres-catch.

Holmström B. and J. Tirole. 1998. "Public and Private Supply of Liquidity." *Journal of Political Economy* 106 (1): 1–40.

———. 2013. *Inside and Outside Liquidity*. Cambridge, MA: The MIT Press.

Hu, A, C. A. Parlour and U. Rajan. 2018. "Cryptocurrencies: Stylized Facts on a New Investible Instrument." Available at SSRN: https://ssrn.com/abstract=3182113 or http://dx.doi.org/10.2139/ssrn.3182113

Javier, L. 2018. "Yes, These Chickens Are on the Blockchain." Blooomberg Businessweek, April 9, https://www.bloomberg.com/news/features/2018-04-09/yes-these-chickens-are-on-the-blockchain.

Kareken, J. and N. Wallace. 1981. "On the Indeterminacy of Equilibrium Exchange Rates." *The Quarterly Journal of Economics* 96 (2): 207–222.

Keister, T. and D. Sanches. 2018. "Should Central Banks Issue Digital Currency?" Working Paper.

Kharif, O. 2018. "Cryptocurrency Attacks are Rising." Blooomberg, May 30, https://www.bloomberg.com/news/articles/2018-05-29/cryptocurrency-attacks-are-rising-as-rouge-miners-exploit-flaw.

Kocherlakota, N. R. 1998. "Money Is Memory." *Journal of Economic Theory* 81 (2): 232–251.

Lamport, L., R. Shostak and M. Pease. 1982. "The Byzantine Generals Problem" *ACM Transactions on Programming Languages and Systems* 4 (3) 382–401.

Lane, T. 2018. "Decrypting "Crypto" Speech at Haskayne School of Business, University of Calgary, Calgary, Alberta, October 1.

Lerner, J. and J. Tirole. 2002. "Some Simple Economics of Open Source." *The Journal of Industrial Economics* 50 (2): 197–234.

Ma, L. C. K., P. Banerjee, J. H. Y. Lai and R. H. Shroff. 2008. "Diffusion of the 'Octopus' Smart Card E-payment System: A Business and Technology Alignment Perspective." *International Journal of Business and Information* 3 (1): 115–128.

Nexo. 2018. "Nexo Token Terms." Accessed on December 5, https://nexo.io/assets/downloads/NEXO-Token-Terms.pdf.

Ostroy, J. M., 1973. "The Informational Efficiency of Monetary Exchange." *American Economic Review* 63 (4) 597–610.

Paul, R. 2011. *Gold, Peace, and Prosperity: The Birth of a New Currency*. Auburn, Alabama: Ludwig von Mises Institute.

Peragallo, E. 1969. Review of *History of Accounting and Accountants,* by Richard Brown. *The Accounting Review* 44 (4): 854–56. http://www.jstor.org/stable/243691.

Rochet, J. and J. Tirole. 2003. "Platform Competition in Two-Sided Markets." *Journal of the European Economic Association* 1 (4): 990–1029. https://doi:10.1162/154247603322493212

Saleh, F. 2018. "Blockchain Without Waste: Proof-of-Stake." Available at SSRN: http://dx.doi.org/10.2139/ssrn.3183935.

Sveriges Riksbank. 2017. "E-krona Project, Report 1" (September).

———. 2018. "E-krona Project Report 2" (October).

Tobin, J. 1987. "The Case for Preserving Regulatory Distinctions." In *Restructuring the Financial System*. Federal Reserve Bank of Kansas City: 167–183.

Townsend, R. M. 1987. "Economic Organization with Limited Communication." *American Economic Review* 77 (5): 954–971.

Walch, A. 2018. "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains." Available at SSRN: https://ssrn.com/abstract=3203198.

———. 2019. "Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems." In *Crypto Assets: Legal and Monetary Perspectives*. Oxford University Press forthcoming 2019. Available at SSRN: https://ssrn.com/abstract=3326244.

Weber, W. E. 2015. "Government and Private E-Money-Like Systems: Federal Reserve Notes and National Bank Notes." Bank of Canada Staff Working Paper No. 2015-18.

———. 2016. "A Bitcoin Standard: Lessons from the Gold Standard." Bank of Canada Staff Working Paper No. 2016-14.

Wilkins, C. A. 2014. "Money in a Digital World." Speech at Wilfrid Laurier University, Waterloo, Ontario, November 13.

———. 2018. "Money for Nothing? A Central Banker's Take on Cryptoassets." Speech at Princeton University's career speaker series, Princeton, New Jersey, October 4.

Williamson, S. 2018. "Is Bitcoin a Waste of Resources?" Federal Reserve Bank of St. Louis *Review* 100 (2).

van Wirdum, A. 2018. “The Good, the Bad and the Ugly Details of One of Bitcoin’s Nastiest Bugs Yet.” *Bitcoinmagazine*, September 21, https://bitcoinmagazine.com/articles/good-bad-and-ugly-details-one-bitcoins-nastiest-bugs-yet/.

Yamey, B. S. 1949. “Scientific Bookkeeping and the Rise of Capitalism.” *The Economic History Review,* New Series 1 (2/3): 99–113. doi:10.2307/2589824.

Zhu, Y. and S. Hendry. 2019. “A Framework for Analyzing Monetary Policy in an Economy with E-money.” Bank of Canada Staff Working Paper No. 2019-01.

Appendix: Electricity calculations for a blockchain payment system

How much electricity would be needed to have all Canadian payments settled on a proof-of-work blockchain? The answer to this question is very complicated and depends on multiple factors that depends on multiple factors. Below we conduct a very rough back-of-the-envelope calculation to give an estimate that could serve as a starting point to answer this question. We use the following strong assumptions:

1. We assume the current properties of the bitcoin blockchain.
2. We assume no change in miner demographics and network topology that would affect bitcoin electricity consumption.
3. We assume that transaction throughput scales linearly with electricity consumption.

All three are strong assumptions, but this allows us to highlight what would need to change to have a bitcoin payment system that could reasonably be used as a widespread payment instrument.

Essentially, we need to see how many transactions the current bitcoin blockchain supports and compare this number with how many transactions are conducted in Canada. This will let us know how many times larger the Canadian payments landscape is compared with the bitcoin blockchain. Assuming we could replace all Canadian payment infrastructure with multiple bitcoin-type blockchains then allows us to hypothesize how much electricity might be used by multiplying the number of blockchains by the observed electricity usage of the current bitcoin blockchain. We can then compare it with how much electricity Canadians currently use.

To calculate an electricity estimate we require four quantities:

- **Bitcoin electricity usage**: According to Digiconomist, the bitcoin blockchain uses approximately 125 million kilowatt-hours per day of electricity. This translates to 45,625 million kilowatt-hours over the whole year, which implies 173.375 billion megajoules of power per year, or 173.375 petajoules of power per year.
- **Bitcoin transaction volume**: According to Blockchain, the bitcoin blockchain settles about 223,000 transactions per day or 81.33 million transactions per year. In scientific notation this is 81.33x1E6.
- **Canadian electricity usage**: According to Natural Resources Canada, the total electricity use in Canada was about 1,783.8 petajoules of power in 2015.
- **Canadian retail payment transaction volume**: According to Payments Canada, Canadians made 22 billion transactions in 2017. In scientific notation this is 22x1E9.

We can now find our rough estimate. To settle Canadian payments would require the capacity of 22x1E9/81.33x1E6 = 270.5 bitcoin blockchains given the current transactional volume of bitcoin. This in turn would imply 270.5x173.375 = 46898.4 petajoules of electricity if we assume the same electrical usage of current bitcoin blockchains, or equivalently 46,898.4/1,783.8 = 26.3 times the current annual power consumption of Canada. This is presumably an overestimate given our assumptions, but it allows us to highlight the fact that changes to the bitcoin technology and usage need to be substantial before it could be used as a retail payment method.