March 2019

The Economics of Fintech and Digital Currencies

Edited by Antonio Fatás

A VoxEU.org Book

CEPR Press

The Economics of Fintech and Digital Currencies

CEPR Press

Centre for Economic Policy Research
33 Great Sutton Street
London, EC1V 0DX
UK

Tel: +44 (0)20 7183 8801
Email: cepr@cepr.org
Web: www.cepr.org

ISBN: 978-1-912179-18-3

The Economics of Fintech and Digital Currencies

Edited by Antonio Fatas

A VoxEU.org eBook

CEPR Press

Research and Policy Network
Fintech and Digital Currencies

Centre for Economic Policy Research (CEPR)

The Centre for Economic Policy Research (CEPR) is a network of over 1,200 research economists based mostly in European universities. The Centre's goal is twofold: to promote world-class research, and to get the policy-relevant results into the hands of key decision-makers.

CEPR's guiding principle is 'Research excellence with policy relevance'.

A registered charity since it was founded in 1983, CEPR is independent of all public and private interest groups. It takes no institutional stand on economic policy matters and its core funding comes from its Institutional Members and sales of publications. Because it draws on such a large network of researchers, its output reflects a broad spectrum of individual viewpoints as well as perspectives drawn from civil society.

CEPR research may include views on policy, but the Trustees of the Centre do not give prior review to its publications. The opinions expressed in this report are those of the authors and not those of CEPR.

Contents

Part 4: Cryptocurrencies, ICOs, and regulation

Foreword

In late 2018 CEPR established a new type of research network – a Research and Policy Network (RPN) – with the main aims of building a community of researchers around a particular topic and ensuring that policy issues are considered over a longer time period than is often the case when a single piece of output is produced and the researchers involved then move on. An RPN consists of 15-30 experts, many of whom are CEPR Research Fellows or Affiliates, with an interest in a topic of high policy relevance and where academic research and collaboration with policymakers can have a high impact.

The RPN on Fintech and Digital Currencies, established on 1 September 2018 for an initial three-year term, is led by Professor Antonio Fatás (INSEAD and CEPR), the editor of this eBook. The main goal of the network is to generate, coordinate and disseminate academic research related to the broad issue of the potential of new technologies to change the way financial markets operate or institutions compete. The nature of the topics means that the network brings together a community of researchers from different fields of economics (finance, macroeconomics, industrial organisation). In addition, it seeks to foster a dialogue among academics and policymakers (central bankers and regulators) about the optimal policies to deal with these changes in financial markets.

This is the first of what we hope will be a series of eBooks emanating from CEPR's Research and Policy Network on Fintech and Digital Currencies. It brings together a set of eleven contributions from members of the network on some of the key areas where changes are becoming more visible. The chapters cover four main topics:

- **Technology and governance.** Can these new technologies be compatible with the strict requirements of financial markets? Can decentralised systems replace the traditional financial market with its reliance on intermediaries and a central authority?
- **The economics of blockchain.** Is blockchain technology and its decentralised consensus mechanism viable in financial markets?

- **Private and public digital currencies.** Can private digital currencies such as Bitcoin compete with traditional currencies? Do digital currencies (including those issued by a central bank) make the financial system more robust and efficient?
- **Regulation of cryptocurrencies and initial coin offerings (ICOs).** How should regulation approach new assets such as cryptocurrencies and ICOs? Should we ignore them or regulate them like traditional securities, or do we need new rules to deal with their digital nature?

CEPR thanks Antonio Fatás for his editorship of this eBook, Anil Shamdasani and Sophie Roughton for their work on its production, and Kirsty McNeill for her efforts in administering the network's activities. CEPR, which takes no institutional positions on economic policy matters, is glad to provide a platform for an exchange of views on this topic.

Tessa Ogden
Chief Executive Officer, CEPR
March 2019

Introduction

Antonio Fatás
INSEAD and CEPR

In recent years, financial markets have seen the arrival of new technologies, opening a debate about the extent of their consequences. Are we about to witness significant disruptions to the nature of money, for example, or the way new ventures are funded? The potential for radical changes has been met with both excitement and a good dose of scepticism. And the rapid increase and sudden crash in the prices of major cryptocurrencies over the last two years has been a wake-up call to how optimistic views of the disruptive possibilities of these new technologies can disappoint. But, at the same time, while the Bitcoin price remains far from its record levels, there are many areas where progress is being made and new technologies are still receiving the attention of aspiring entrepreneurs and established financial institutions, as well as central banks and regulators.

In September 2018, CEPR launched a new Policy and Research Network on "Fintech and Digital Currencies" to foster a dialogue between researchers and policymakers on all issues related to technology and financial markets ('fintech'). This eBook brings together eleven chapters from members of the network on the current state of the debate. It summarises current research on the impact of these changes as well as the views of policymakers on how to manage the possible disruption in financial markets.

Technology and governance

The first three chapters deal with both the new possibilities created by the technologies as well as the potential limits to their adoption. The chapters stress the need for some form of centralised authority to manage the requirements in financial markets. Chapter 1, by Stephen Cecchetti and Kim Schoenholtz, focuses on the changes taking place in the technology used to maintain financial records. Different technologies have

different implications for governance and access rights. Both of these issues make it practically impossible to imagine the widespread adoption of open-access ledgers (such as blockchain) in financial markets.

Chapter 2, by Katrin Tinn, discusses the benefits of the adoption of hash-linked timestamping technology in financial contracts. While the benefits are clear, the chapter also raises questions about the governance of these technologies and suggests that permissioned systems might be the right way to move forward.

Chapter 3, by Edgardo Di Nicola Carena, Pierfrancesco La Mura and Alessandro Rebucci, analyses one particular application of timestamping technology, namely, the creation of a global patent office. In this case, transparency and the ability to reach a global community represent significant benefits. But, as in the previous two chapters, the authors also stress the need to rely on a central authority for the purpose of governance.

The economics of cryptocurrencies

Chapter 4, by Harald Uhlig and Linda Schilling, analyses the equilibrium price of a cryptocurrency under the assumption that it succeeds in the future and co-exists with a traditional currency (such as the US dollar). The analysis shows why speculation in the periods before adoption might not be possible in equilibrium. In addition, the authors explore the monetary policy implications of the future existence of such an alternative currency.

Chapter 5, by Raphael Auer, presents a pessimistic view of the viability of cryptocurrencies. In particular, the author highlights that the proof-of-work technology behind cryptocurrencies such as Bitcoin is subject to an externality similar to the tragedy of the commons. As a result, the income necessary to ensure a well-functioning consensus mechanism will fall short and liquidity will shrink. The author then discusses possible changes to the available technology that could address this imperfection.

Private and public digital money

The next three chapters delve into the question of how new technologies are changing the way we think about money and the potential competition between private and public (digital) money. Chapter 6, by Markus Brunnemeier and Dirk Niepelt, starts with a typology of different forms of money and then discusses the consequences of introducing digital central bank currency (CBDC). Under some assumptions, there is an equivalence between private and public money and, as a result, introducing central bank digital currencies would not have macroeconomic effects.

Chapter 7, by David Andolfatto, also analyses the introduction of CBDC but in a different setting. The objective here is to understand the effects that the introduction of CBDC might have on lending as well as the stability of the financial system. The model sketched in the chapter dismisses some of the common criticisms of CBDC by showing that it would have no negative consequences on lending and it would not increase the instability of the financial system.

Chapter 8, by Aleksander Berentsen and Fabian Schär, discusses 'stablecoins' – cryptocurrencies whose price is kept fixed in units of a traditional currency. Several alternatives that have been proposed and the authors suggest that the on-chain, fully collateralised option may be the best available, although it is still a work in progress because of the inherent risks in the technology being used.

Cryptocurrencies, ICOs, and regulation

One of the recent innovations in financial markets is the new funding model behind initial coin offerings (ICOs). Chapter 9, by Antonio Fatas and Beatrice Weder di Mauro, discusses some of the potential benefits and risks of ICOs. The evidence is mixed – the market has grown very fast but the high failure rate of ICOs, combined with abundant examples of fraudulent schemes, raises serious concerns about the long-term viability of this market. In addition, empirical analysis shows a very high correlation of ICO returns with Bitcoin or Ethereum prices, suggesting that the bubble-type behaviour of those cryptocurrencies was behind the hype of ICOs.

The final two chapters look at the challenges that these innovations pose to regulators. Chapter 10, by Raphael Auer and Stijn Claessens, discusses the benefits and costs of regulating cryptocurrencies. Empirical analysis shows that news about regulation affect the prices of these assets, signalling that national regulators do have some power. But regulating cryptocurrencies could imply giving credibility to these new assets. The alternative – i.e. 'benign neglect' – is not optimal either because of the negative consequences of an unregulated market that funds illegal activities or tax fraud. A potential solution is to enforce a minimum amount of regulation along the lines of anti-money laundering activities.

In a related analysis, Chapter 11, by Marlene Amstad, presents the different approaches that regulators around the world have followed when it comes to fintech innovations. The two most common approaches are ignoring them (i.e. leaving them unregulated) or treating them like other traditional securities. The author suggests a third alternative that takes into account the special nature of these new technologies and designs regulation that is tailored to their specific features.

What next?

The chapters in this eBook have addressed several of the most pressing issues in the debate over what to expect from, and what to do about, new technologies in financial markets. The hype and then crash in the Bitcoin price offers an illustration of how some of the early excitement might have been premature. The various contributors to the book have identified changes that could help these technologies move forward to become viable in an environment – financial markets – where governance and regulation are central. The reality is that efforts to incorporate new technologies in financial markets have not slowed down; if anything, they have accelerated and are likely to lead to new innovations that might address some of the early weaknesses. The academic research behind this book remains a work in progress and should, over time, help policymakers design an optimal response to changes in the technology environment of financial markets.

Part 1
Technology and governance

1 Finance and blockchain

Stephen G. Cecchetti and **Kermit L. Schoenholtz**[1]
Brandeis International Business School and CEPR; NYU Stern School of Busines

> "Only 1% of 3,138 chief information officers at companies surveyed by Gartner last year said they had 'any kind of blockchain adoption'…."
> *The Wall Street Journal*, 7 May 2018.

Blockchain is all the rage. We are constantly bombarded by reports of how it will change the world. While it may alter many aspects of our lives, our suspicion is that they will be in areas that we experience only indirectly. That is, blockchain technology mostly will change the implementation of invisible processes – what businesses think of as their *back-office* functions.

In this chapter, we briefly describe blockchain technology, the problem it is designed to solve, and the impact it might have on finance.

Blockchain basics

Blockchain is a record-keeping mechanism; a 21st century version of the recording systems that have been around since people started chiselling marks on cave walls. Over the millennia we have moved from ledgers that are carved into clay and stone to ones that are digital.

To be more specific, consider the problem of tracking the ownership of a share of equity. Imagine that there is a sequential list of all owners, with the name of each

1 We thank Morten Bech, Ethan Cecchetti, and Hanna Halaburda for patiently explaining many aspects of how the blockchain works and how its applications to economics and finance. An earlier version of this chapter appeared on www.moneyandbanking.com.

crossed out, except for that of the current owner. The key question is the following: who has the right to cross out a name and write in a new one?

Put another way, the challenge we face is to create a tamper-proof and universally accepted way of recording things like ownership of assets, obligations of one person to provide a product or service to another, levels of inventories, personal identities, and the like. What we require is that the system be a reliable, secure, and trusted mechanism for accessing and updating essential records that cannot be hijacked by someone with ill intent.

The four types of ledgers

In thinking about the challenge of maintaining records – a ledger – consider differences along two dimensions: the structure of the database in which the records are stored, and how we establish that any changes are legitimate. Along the first dimension – *ledger structure and ownership* – the database and its ownership can be either *centralised* or *distributed*. And, on the second dimension – *access rights* – the system can have *limited access* in which a restricted number of people (or entities) can make alterations, or *open and public access* (also called 'permissionless') so that anyone can participate. In either case, following a legitimate modification, all versions are immediately updated, guaranteeing agreement on the current state.

This two-by-two classification system leads to four ledger frameworks. To understand this taxonomy, Tables 1 and 2 provide a set of nonfinancial and financial examples.[2]

The upper-left cell of each table is the case of a centralised database with limited, proprietary access rights. This case captures the ledger practices of human civilisation until now. There is one central ledger containing the authoritative record of ownership or obligations that can only be changed by the organisation or person maintaining it. While there may be copies, there is only one definitive version. Examples are everywhere – hospital records and records of securities ownership are just two.

2 For a more detailed discussion with examples, see Haeringer and Halaburda (2018) and Dwyer (2016).

Table 1 Ledger structure and ownership, and access rights: Nonfinancial examples

		Access rights	
		Limited/Propietary	Open/Public
Ledger structure and ownership	Centralised	Hospital records (current systems)	Customer ratings (user review websites)
	Distributed	Supply chain inventory* (closed, trusted networks)	Property title* (proof of work/stake systems)

Note: *Potential implementations.

Table 2 Ledger structure and ownership, and access rights: Financial examples

		Access rights	
		Limited/Propietary	Open/Public
Ledger structure and ownership	Centralised	Securities ownership records (current systems)	CFPB Consumer Complaint Database (user review websites)
	Distributed	CLSnet (closed, trusted networks)	Bitcoin (proof of work)

Note: CFPB is the Consumer Financial Protection Bureau.

Turning to the top-right cell, this is the case of an open-access, but centralised recording system that allows anyone to write and read. Lacking security, this mechanism is of limited use. Nevertheless, examples exist. In the nonfinancial realm, these include the customer rating systems employed by Amazon, eBay, TripAdvisor and the like. Wikipedia uses this protocol for creating and updating entries. Given the security concerns, financial examples are more difficult to find. One instance is the Consumer Complaint Database of the Consumer Financial Protection Bureau (CFPB).

The bottom rows cover the range of distributed (or decentralised) databases. The distinction here is that there are now many copies of the ledger, all with equal standing. So long as they follow an agreed set of rules, anyone who has a copy can make a

change. Put another way, participants directly interact with each other. And, as with the centralised systems, there are two cases: limited access and permissionless.

Blockchain technology seeks to implement distributed systems, providing automatic mechanisms that create trust, ensuring there are no conflicting changes, and preventing malicious actors from making unauthorised or improper changes. It has the potential to record transactions between two parties, maintaining an agreed sequence, without reliance on potentially costly third-party verification.

To prevent people from arbitrarily attacking the system, violating trust, and making illegitimate modifications, the ability to alter the ledger is based on a scarce resource. In the limited-access model, the scarce resource is identity – only specific people or institutions can make modifications. The idea of an open system is to make identity irrelevant – anyone can join, leave, and re-join as often as desired. Here the scarce resource that allows alterations to the ledger can be something like computational power or a stake (possibly financial) in the system.

In the open system, participants can make changes so long as they follow the rules. Importantly, the rules must prevent a bad actor from capturing the system. The original Bitcoin protocol, where the scarce resource is computational power, is immune from takeover so long as no one controls more than half of the computing power. But, as has been pointed out repeatedly, the system is incredibly expensive, generating substantial deadweight loss. Electricity costs alone exceed $3 billion per year.

The uncertain future of blockchain

Both financial and nonfinancial uses of blockchains remain limited, with the obvious exceptions of cryptocurrencies. In Table 1, we list two possible nonfinancial applications – supply chain inventory management and property title records – but so far as we know, neither has yet been implemented on a broad scale.

Where is this all heading? Without a further theoretical breakthrough, open distributed systems appear both costly and slow. Estimates for the Bitcoin protocol, for example, are that speeds cannot exceed seven transactions per second. In contrast, there may be some promise in distributed systems that are proprietary. We suspect that most of the

corporate developers working on such projects have this kind of architecture in mind, perhaps in the hopes of creating a profitable monopoly. Unfortunately, a monopolist would be unlikely to lower transactions costs in the way that the advocates of open distributed systems hope.

Conceivably, a blockchain system could securely track the ownership of every financial instrument and exposure in the global economy. While this is a very tall order, it would be truly revolutionary. Financial market participants could overcome information asymmetries, improving risk pricing and capital allocation. Authorities could monitor position concentrations and other risks to the financial system. And, money laundering and terrorist finance would be easier to police.

In practice, we are still a long way off. Before we can map the entirety of the financial system, we need to be able to identify both entities and instruments globally.[3] But even if such identifiers are in place, we question whether people would be happy with the result. It would create a *world without privacy* in which everyone's balance sheet and transactions are public. Even if a much less invasive version were to become possible, it would be deeply ironic if blockchain, a technology initially championed by libertarians disenchanted by government and fiat money, ended up by narrowing the range of individual freedoms.

Today, blockchain faces a major problem of *scalability*. The fastest proprietary blockchain systems currently can handle no more than several thousand transactions per second.[4] To put this into perspective, at its peak the Depository Trust & Clearing Corporation (DTCC) processes 25,000 equity transactions per second (roughly the same as VISA's payments processing capacity). DTCC (2018) points out that any new technology would have to have a maximum capacity of 2 to 3 times this peak – more

3 For a discussion of global legal entity identifiers (LEIs) and global financial instrument identifiers (FIIs), see Cecchetti and Schoenholtz (2017b).

4 Since all copies of a distributed ledger must be revised before anyone can record the next transaction, the speed of light materially limits the rate at which these systems can operate. If, for example, there a ledger is in both New York and London, at a minimum, it will take between 20 to 40 milliseconds for a transaction in one location to be recorded in the other. This means that fully distributed systems cannot process more than 50 transactions per second. Some degree of centralisation, combined with geographic proximity, lowers this latency and increases the maximum throughput.

than 50,000 equity transactions per second. For the foreseeable future, given physical constraints on the speed of transmission for such a large volume of information, we see no way that the financial system can escape its reliance on centralised clearing and settlement systems.[5]

Conclusion

All that said, we really have little idea where this will lead. A decade since the appearance of Nakamoto's (2008) paper that launched Bitcoin, we have more than 1,000 crypto-clones. But where are the broader applications of the blockchain technology? We expect that it will find increased use in the clearing, payments, and settlement system (Cecchetti and Schoenholtz 2017a). Perhaps it also will be applied across a range of other activities, such as recording property titles or managing the supply chain both within and across firms or for a variety of accounting and audit functions. Such applications would likely focus on cases with limited numbers of transactions and where speed is less important. But, for now, we anticipate the development and implementation of proprietary systems, not those with open access.

References

Bank for International Settlements (BIS) (2018), "Cryptocurrencies: looking beyond the hype", Annual Economic Report, June.

Budish, E (2018), "The Economic Limits of Bitcoin and the Blockchain",NBER Working Paper No. 24717.

Cecchetti, S G and K L Schoenholtz (2017a), "Modernizing the U.S. Payments System: Faster, Cheaper, and More Secure", www.moneyandbanking.com, 31 July.

5 Permissionless distributed systems of the type use for Bitcoin also face a severe incentive problem. As Chapter V of the most recent BIS Annual Economic Report (BIS 2018) describes in detail, the possibility that the system will be taken over means that it is impossible to guarantee finality. Budish (2018) derives the condition under which Bitcoin-style systems will be attacked and captured by a malicious actor.

Cecchetti, S G and K L Schoenholtz (2017b), "Managing Risk and Complexity: Legal Entity Identifier", www.moneyandbanking.com, 30 October.

Depository Trust and Clearing Corporation (DTCC) (2018), "Modernizing the U.S. Equity Markets Post-Trade Infrastructure", January.

Dwyer, G P (2016), "Blockchain: A Primer", MPRA Paper 76562, University Library of Munich.

Haeringer, G and H Halaburda (2018), "Bitcoin: A Revolution?", Baruch College Zicklin School of Business Research Paper No. 2018-05-01.

Nakamoto, S (2018), "Bitcoin: A Peer-to-Peer Electronic Cash System".

About the authors

Stephen G. Cecchetti is the Rosen Family Chair in International Finance at the Brandeis International Business School. Before rejoining Brandeis in 2014, he completed a five-year term as Economic Adviser and Head of the Monetary and Economic Department at the Bank for International Settlements. During his time at the BIS, Cecchetti participated in the numerous post-crisis global regulatory reform initiatives. In addition to his other appointments, Cecchetti served as Director of Research at the Federal Reserve Bank of New York; Editor of the J*ournal of Money, Credit, and Banking*; and is currently Research Associate of National Bureau of Economic Research and Research Fellow of the Centre for Economic Policy Research since 2008. Cecchetti has published widely in academic and policy journals, and is the author of a leading textbook in money and banking. Together with Kim Schoenholtz, he blogs at www.moneyandbanking.com.

Kim Schoenholtz is the Henry Kaufman Professor of the History of Financial Institutions and Markets in the Economics Department of NYU Stern School of Business. He also directs the Stern Center for Global Economy and Business. Previously, Schoenholtz was Citigroup's Global Chief Economist from 1997 until 2005. Schoenholtz currently serves on the Financial Research Advisory Committee of the U.S. Treasury's Office of Financial Research. He also is a panel member of the U.S. Monetary Policy Forum and a member of the Council on Foreign Relations. Previously, he served on the CEPR

Executive Committee.Schoenholtz is co-author of a popular textbook on money, banking and financial markets and of a blog on the same topic at www.moneyandbanking.com. Schoenholtz was a Visiting Scholar at the Bank of Japan's Institute for Monetary and Economic Studies from 1983 to 1985. He holds an M.Phil. in economics from Yale University and an undergraduate degree from Brown University.

2 Distributed ledger technologies and start-up financing

Katrin Tinn
Imperial College Business School

Innovations related to distributed ledger technologies have gained widespread interest in the past few years, partly due to the development of Bitcoin and other cryptocurrencies. While the question of whether there can be a sustainable value and price associated with an 'outside the system' fiat money is an interesting one, focus has shifted towards assessing the benefits brought by the underpinning blockchain technology itself, i.e. the possibility of having reliable and verifiable shared digital records of any data, be it ownership rights, transaction records, supply chain data or contractual rights.

What is this digital ledger technology innovation about? It stems from computer science research by Haber and Stornetta (1991, 1997), who highlighted the cryptographic benefits of hash-linked, chronologically ordered and timestamped records. Under this structure, past records are particularly difficult – if not impossible – to change ex post. This is because each data block contains a difficult-to-reverse reference to the previous block (via a complex enough hash function), and thus effectively contains references to all previous blocks. This ensures that any modifications of past data cannot be done without it being visible (the hash function will be very different subject to even very minor modifications, and the more time passes the more difficult it is change past records). Importantly, this distributed ledger structure allows the verification of both the fact that a record was made, and the time when it was recorded.

Does it require decentralisation? Beyond Bitcoin, there are other prominent crypto-assets and platforms that enable the creation of new digital assets, or 'tokens'. A notable example is the Ethereum platform, where the ethereum coin is a necessary input for creating 'smart contracts' that use the functionalities of the Ethereum platform. This platform has enabled many firms to raise financing in return for 'token rights', so-called

initial coin offerings (ICOs). These tokens can offer a share of the future revenues or profit the firm generates, a right to access the platform, or any other rights that can be described by a computer code that is stored on a distributed digital ledger in a similar way as the ownership rights of a bitcoin. The greatest enthusiasts praise the decentralised nature of these developments, while at the other end there are sceptics who dismiss everything related to crypto-currencies, crypto-tokens and blockchain (the term often used to describe the underlying digital ledger technologies described) as a temporary 'hype' or 'bubble'. Both sides, as well as the middle, include some prominent names.

Yet, decentralisation and the possibility to avoid intermediaries and governments may not the essential value driver of this technology, as better record keeping is valuable in itself. Indeed, many governments, central banks, financial intermediaries and other firms have taken an interest in this technology. A noticeable early country-level example is Estonia, which has adopted the same core principles of storing fundamental and sensitive digital data on their citizens, residents and firms, in hash-linked and timestamped blocks on a public distributed ledger[1] since 2008 (the same year Bitcoin was launched). Furthermore, many blockchain initiatives that feature in the media[2] are about improved reliable record keeping rather than decentralisation. Relatedly, another prominent development associated with these technologies is the Hyperledger project that aims to develop digital ledger solutions for businesses involving the largest and most prominent finance and technology firms.[3] It has also been recognised by the research community that new digital ledger technologies enable verifiable record keeping (e.g. Catalini and Gans 2017).

Does this technology have a broader relevance for economics and corporate finance, beyond new interesting crypto-assets and efficient book-keeping? Verifiable records can have the immediate efficiency benefits of making the status quo better (e.g. Yermack 2017). For example, better records can reduce the cost of issuing debt (for example, by making verification costs lower and making it easier to transfer the collateral).

1 See https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/

2 See https://www.economist.com/technology-quarterly/2018/09/01/the-promise-of-the-blockchain-technology

3 See https://www.hyperledger.org

For this reason, it is argued that distributed ledger technology will have a significant impact on the way start-ups raise funds, on corporate governance, and on the design and the nature of financial contracts.

It is well known that a firm with a creative and value-generating business idea, but not enough own funds or collateral assets, is likely to find it difficult to finance its project because future cash flows generated by the project cannot be credibly pledged. This has aggregate consequences as innovative ideas often come from new start-ups that have greater incentives to innovate compared to incumbents, whose innovation may cannibalise their own profits, as highlighted in the literature of creative destruction and endogenous growth (Aghion and Howitt 1992). Innovative start-ups are also often most constrained when it comes to raising funds – these firms may lack collateral, debt may be impossible as well as unsuitable compared to equity, and venture capital or angel investment are scarce (Lerner et al. 2012). One of the most important traditional frictions is that a firm with a creative and value generating business idea, but not enough own funds or collateral assets, cannot finance its project because future cash flows generated by the project cannot be credibly pledged due to asymmetric information (Tirole 2010). While venture capitalists or angel investors may mitigate the problem for a few firms, there are unlikely to be enough of those to fund innovative ideas.

Think of a fledgling entrepreneur who has an innovative platform business idea that requires an initial cost of development. Suppose the firm is in Brazil and a number of retail investors who agree that this idea is good are in the UK, the US, Canada, France, and so on. In a traditional environment it would be too risky for these international investors to invest in such a business as it is likely to be too costly for them to check whether the business generates the expected returns. The Brazilian entrepreneur may – and in fact *should* if he/she is rational – under-report sales. Consequently, there is value in centralised intermediation and in minimising verification costs via debt contracts, as famously pointed out in the costly state verification literature (Townsend 1979, Diamond 1984, Gale and Hellwig 1985).

Yet, one may consider that the prevalence of debt contracts may be a legacy of historical frictions. New innovations in digital ledger technologies make it theoretically possible for firms to credibly pledge their future cash flows; UK retail investors could be

assured that each sale of the aforementioned Brazilian firm is credibly recorded and the verification that it happened could be nearly costless for the international investors.

In a recent paper (Tinn 2018), I explore the optimal and traditional contracts in an environment where the borrower and the lender can contract on sales records that are pledgeable and timestamped, benefiting from the core features of hash-linked timestamping technology. I highlight that there is indeed added value in having timestamps when raising financing. This is particularly important when entrepreneurs learn from past data, which in turn affects their incentives to continue making efforts to generate sales (in the aforementioned example, this could take the form of maintaining the quality of the app, as well as marketing the product). Learning from past data is the reason why a simple equity contract is typically not the best in this environment – when learning is important, the start-up firm would prefer a flexible profit-sharing rule to obtain a lower share of revenues in states where it finds it easy to sell its product and a higher one in pessimistic times. In my paper, I describe a number of stochastic environments and the resulting optimal contracts in these environments.

Overall, my research shows that the widespread adoption of new digital ledger technologies is not necessarily good news for traditional contracts that have been designed for traditional environments where primary frictions are due to verification costs, and where learning is infrequent and slow. Debt and equity contracts become more expensive when we learn from data.

There are further policy issues to be considered. First, faster learning from data and related effects on incentives are ongoing regardless of digital ledger technologies. These technologies can yet help to mitigate likely negative effects. Second, while there are economic and technological benefits in hash-linked and timestamped record keeping, there are many open questions, such as who should be entitled to verify the records. On the one hand there are experimentation and innovation benefits of decentralisation in the system used by Ethereum, which relies on a fully decentralized 'proof-of-work' verification system (at least so far) that is costly and has its weaknesses.[4] On the other

4 Verification under proof of work is costly due to transaction costs (Easley et al. 2018); this and supply constraints imposed by proof of work systems can limit adoption (Hinzen et al. 2019); mining nowadays is also not that decentralised as a large part of it conducted by a small number of mining pools (e.g. Cong et al. 2018).

hand, permissioned verifications systems (such as those adopted by the Hyperledger project) that rely on a central authority for verification may be more cost efficient and robust, but also less open to contract innovation which may be needed.

References

Aghion, P and P W Howitt (2008), *The economics of growth*, MIT press.

Catalini, C and J S Gans (2017), "Some Simple Economics of the Blockchain", Rotman School of Management Working Paper No. 2874598.

Cong, L, Z He and Jiasun Li (2018), "Decentralized Mining in Centralized Pools", George Mason University School of Business Research Paper No. 18-9.

Diamond, D W (1984), "Financial intermediation and delegated monitoring", *The Review of Economic Studies* 51(3): 393-414.

Easley, D, M O'Hara and S Basu (2018), "From Mining to Markets: The Evolution of Bitcoin Transaction Fees".

Gale, D and M Hellwig (1985), "Incentive-Compatible Debt Contracts: The One-Period Problem." *The Review of Economic Studies* 52(4): 647–663.

Haber, S and W S Stornetta (1991), "How to Time-Stamp a Digital Document", *Advances in Cryptology-CRYPT0'90*.

Haber, S and W S Stornetta (1997), "Secure names for bit-strings", in *Proceedings of the 4th ACM Conference on Computer and Communications Security*.

Hinzen, J F, K John and F Saleh (2019) "Proof-of-Work's Limited Adoption Problem".

Lerner, J, A Leamon and F Hardymon (2012), *Venture capital, private equity, and the financing of entrepreneurship: The power of active investing*, John Wiley & Sons.

Tirole, J (2010), *The theory of corporate finance*, Princeton University Press.

Tinn, K (2018), "'Smart' Contracts and External Financing".

Townsend, R M (1979), "Optimal contracts and competitive markets with costly state verification", *Journal of Economic theory* 21(2): 265-293.

Yermack, D (2017), "Corporate Governance and Blockchains", *Review of Finance* 21(1): 7–31.

About the author

Katrin Tinn is an Assistant Professor of Finance at Imperial College Business School. Her research focuses on applied theory in financial economics and information economics. Her latest research is on FinTech and the role of crowdfunding and distributed ledger technologies (blockchain) in raising external capital and facilitating learning about future demand. She has also published research on the interaction between technological innovation, equity markets and endogenous growth. In addition to academic positions, she has also worked in commercial banking and asset management, ECB, IMF, and EBRD. She gained her PhD in Economics from the London School of Economics.

3 Blockchain technology and government applications: A proposal for a Global Patent Office

Edgardo Di Nicola Carena, Pierfrancesco La Mura, and **Alessandro Rebucci**[1]
MEA Group; HHL Leipzig Graduate School of Management; Johns Hopkins Carey Business School and CEPR

Theory suggests that patenting is necessary to protect innovators and can complement competition policy in fostering innovation and growth (Aghion et al. 2014).[2] Existing national patent systems, however, are lengthy, costly, and market-specific. As the ongoing dispute between the US and China vividly illustrates, they fall well short of protecting property rights effectively in the context of international trade in goods, services, and assets.

In this chapter we propose the application of blockchain technology to the design and development of a Global Patent Office (GPOX). The aim is to stimulate interest in the design and implementation of a decentralised international patenting system that is secure, accurate, and cost-efficient for both the sponsoring institutions and the end-users, the inventors. While this chapter is not a 'whitepaper' for such an application, it aims at catalysing attention, resources, and interest on such a possibility because it could have large economic impact, with significant positive externalities across the globe.

1 We thank James Calvin for comments. The usual disclaimers apply

2 The evidence is more mixed (Sampat, 2018; Hall, 2018), but remains supportive of the theory.

The idea to use blockchain to decentralise the functions of a patent office is not too far-fetched. Bitcoin is already used by private companies in the patenting field to store the hash value of documents related to inventions, or to timestamp the creation of a document, taking advantage of the sequence of characters that can be inserted when marking a transaction output as invalid.[3] And these hash values can be admitted, like any other piece of evidence, in national enforcement proceedings. However, blockchain usage for this purpose can be pushed much further to fully manage the submission, editing, review, and storage of content subject to intellectual property right protection.[4]

To achieve this, there is need to develop an open, community-based protocol to encrypt and store patents, trademarks, software, documents, graphical objects, and 3-D printed prototypes. The blockchain can contain either the actual content or the hash value in order to universally timestamp the content itself. More specifically, the registered invention is broadcasted to the GPOX network. The GPOX research community validates with the current criteria of originality, applicability, and replicability. Validation contributions will carry a reward in either cash or GPOX tokens. Tech experts and patent lawyers will continue to play a key role in the process, in order to assess and eventually validate a patent for final formal registration, but differently than in the traditional system. Their credibility and reliability can be established through algorithms that take into account the track record of previous works, successful disputes, and judgements from other peers.

Newer inventions enter in full, ideally the complete file. Older inventions could be re-registered on the GPOX database simply with reference to their traditional identification number, amplifying the reach and scope of the existing national patent systems. For inventions entered in full, adherence to submission standards can be checked through automated intelligent filters and natural language processing techniques.

All submitted content can be initially put in 'stealth mode', in a way that ensures time-stamping, but only its creator/owner (other authorised party) can access it. At any time, the owner can decide to switch the whole or part of the content to 'visible mode', while

3 See https://en.bitcoin.it/wiki/OP_RETURN

4 See https://join.utopian.io/ on how such a mechanism might work for software products.

keeping the original time-stamp. At this time, the whole content must be made accessible to anyone through either dedicated public servers or a fully decentralised filing system. The GPOX platform would allow anyone to browse any open intellectually protected object and to review and annotate it. The novelty of an innovation in the GPOX system can be challenged by either referencing internal or external sources.

Once up and running, GPOX could be financially self-sufficient. The platform/protocol will use an incentive-based system of rewards for contributors of submissions, reviewers, upvotes and downvotes, akin to the one used in Steem applications.[5] R&D entities will register their inventions on the platform, paying a submission fee. If ownership is transferred, the inventor gets registration costs back plus the market value of the invention assessed by the GPOX community within the platform. If ownership is not transferred, a maintenance fee is assessed annually for the life of the patent.

Any individual submitting new content subject to intellectual property right protection can choose to submit a legally binding, digitally signed form that transfers the rights of her/his invention in exchange for tokens created by the GPOX platform and bound to the invention itself. From that time, GPOX tokens bounded to the innovation will represent its ownership and could be freely exchanged and traded on the secondary market. This would establish a link between the protection of the invention to its financing and acquisition. In the long term, such a system could be used as a source for crowdfunding of pure ideas, which are much harder to finance than viable business entities even in the most advanced financial markets like those of the US.

GPOX's ambition is to become a simplified and efficient source of intellectual protection that is globally accepted. Patent trials routinely rely on a variety of sources of evidence, but their validity is usually specific to each country, making the international

5 Steem (https://steem.io/), developed by Steemit Inc, is a blockchain platform that hubs and supports the creation of applications and the trading of related coins through its own Smart Media Token (SMT) protocol. In Steem, a transaction is approved, through delegation, from a majority of Steem power, which can be earned by writing content that receives appreciation or editing other contributors' content. The mechanism of delegation makes the transactions less depending on the network and faster than most other cryptocurrencies. There is no proof of work, but only proof of brain (for contributor rewards) and delegated proof of stake (for transaction approvals) (see https://steem.com/steem-bluepaper.pdf).

patenting system incredibly expensive. In a legal proceeding, the time-stamped objects and the community reviews – especially when submitted by R&D professionals – could be used to support the novelty of the invention and to claim its rights, together with other more conventional tools. Initially, GPOX could operate alongside the national offices, prompting them to modernise and improve in the same way public exchanges compete for trading businesses nationally and internationally. But thanks to its lower costs, shorter approval times, and supranational validity, such a system has the potential to become the leading source of originality certification, especially in business areas in which the standard protection system is not working well, such as software and algorithms, and to stimulate the world supply of inventions in these areas.

How feasible is to implement such a blockchain application? It is now well understood that blockchain technology (i.e. encrypted decentralised ledgers) has potentially widespread applicability, well beyond the world of cryptocurrencies. It therefore applies wherever ledger-based record keeping has a role to play. Examples include medical record-keeping, land and property registry, financial contracting, accounting standards and certification, and so on. What is less clearly understood is that not all ledger-based record keeping activities can be profitably decentralised via blockchain technology. The point has recently been formalised by Abadi and Brunnermeier (2019), who show that a fully decentralised (and secure) ledger cannot be more cost efficient (and hence profitable) than a centralised one.

This may be one reason why many blockchain applications have struggled to take off or failed soon after launch. The China Academy of Information and Communications Technology claims in a recent report that only 8% of the over 80,000 blockchain projects ever launched are still active today, with an average lifespan of roughly 1.22 years.[6] This is two percentage points below the probability of death of small and young firms in the US reported by Acemoglu et al. (2018). As an example, despite the promises and strengths of the system, Steem decentralised applications found it quite hard to grow

6 Source: Remarks by He Baohong, Director of CAICT's Cloud Computing and Big Data Research Institute, at the China International Big Data Industry Expo 2018.

and expand.[7] It is very unlikely at the moment that we will see popular applications like Facebook, YouTube, Snapchat, and Instagram being challenged by the corresponding Steem applications without massive financial marketing investment; massive adoption requires significant marketing investment.

While the system of reward and fees outlined above can make GPOX financially self-sufficient in the long run, in order to prevent risks of bifurcation as witnessed in the cryptocurrency markets, there is the need for a sponsoring institution. One possibility is to task the WTO with the launch and initial adoption support of the GPOX application. The WTO already has a mandate on protection and enforcement of intellectual property under its Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement negotiated during the 1986-94 Uruguay Round.[8] But TRIPS has proven not effective over the years in resolving disputes in this area, as the Apple-Samsung case exemplifies.

The ongoing dispute on protection of property rights between the US and China is a golden opportunity to launch such a new multilateral initiative. It is possible to see how a platform designed along the lines above, under the auspices of the WTO, could address several of the issues on the table, resolving problems created by lack of trust and credibility with a community-based system of certification. It would be hugely popular in China, which is very eager to promote widespread adoption of blockchain technology and is also looking for ways to accommodate US demands without losing face domestically. The European Community has already developed a supranational patent office and would have important experience and know-how to contribute. And the US, currently enjoying the strongest and most successful national patent office, would have a way to extend its reach into the new economy on a global scale for years to come.

Blockchain is a complex new technology with ample transformative potential, but its economics suggests that it might be more suitable to securely decentralise services

7 Steemit recently fired 70% of its workforce and is rethinking its business model (https://cryptoslate.com/steemit-lays-off-70-of-workforce-hard-times-ahead/).

8 Fundamental research has historically been subsidised by governments. Indeed, the internet was developed for defense purposes by the US Department of Defense, and internet applications took years to become mainstream in government and business.

supplied by the government rather than the market. A good place to start is a Global Patent Office (GPOX) under the auspices of the WTO that may be faster, cheaper, and more universally recognisable and enforceable than the existing system of competing national offices.

References

Abadi, J and M K Brunnermeier (2019), "Blockchain Economics," CEPR Discussion Paper 13420.

Acemoglu, D, U Akcigit, H Alp, N Bloom, and W Kerr (2018), "Innovation, Reallocation, and Growth." *American Economic Review* 108 (11): 3450-91.

Aghion, P, U Akcigit, and P Howitt (2014). "What Do We Learn From Schumpeterian Growth Theory?", in *Handbook of Economic Growth*, edition 1, volume 2, pp. 515-563, Elsevier.

Hall, B H (2018), "Is there a role for patents in the financing of innovative firms?", forthcoming in *Industrial and Corporate Change*, (see also https://voxeu.org/article/innovative-startup-firms-and-patent-system).

Sampat, N B (2018), "A Survey of Empirical Evidence on Patents and Innovation", NBER Working Paper 25383.

About the authors

Edgardo Di Nicola Carena is Head of Machine Learning and Artificial Intelligence, MEA Group in Milan. He received his Ph.D. in electronic engineering from Politecnico di Milano, Italy. After a few years as Research Associate at the University of Cambridge focused on technology for oil exploration, he founded a start-up company developing machine-learning and big data products and services. He is currently heading a team of applied researchers focused on developing artificial intelligence applications for large corporations.

Pierfancesco La Mura holds the Chair of Economics and Information Systems at HHL Leipzig Graduate School of Management. He received a Doctorate in Economic Analysis from Bocconi University and a Ph.D. in Economic Policy and Analysis from the Stanford University Graduate School of Business. He was a postdoctoral researcher at the Stanford Computer Science Department, and at the Center for Rationality, the Hebrew University of Jerusalem. He was a lecturer at the Central European University, Hebrew University, and HHL Leipzig Graduate School of Management.

Alessandro Rebucci is Associate Professor of Finance at the Johns Hopkins Carey Business School, holding a joint appointment with the Carey Business School Edward St. John Real Estate Program and the Economics Department of the JHU Krieger School of Art and Science. Rebucci is a CEPR Research Fellow (IMF Programme) and a NBER Faculty Research Fellow (IFM Program). He is also Associate Editor of the *Journal of International Money and Finance* and *Economia* (the journal of the Latin American Economic Association). Previously he held research and policy positions at the International Monetary Fund (1998-2008) and the Inter-American Development Bank (2008-2013).

Part 2
The economics of cryptocurrencies

4 Some simple Bitcoin economics

Linda Schilling and **Harald Uhlig**
Ecole Polytechnique, CREST; University of Chicago and CEPR

Cryptocurrencies, in particular Bitcoin, have received a large amount of attention of late. The total market capitalisation of cryptocurrencies reached nearly $400 billion in December 2018, according to coincodex.com.

As Figures 1 and 2 show, the bitcoin price increased dramatically between 2016 and 2018 to a peak of nearly $20,000 (source: coindesk.com). It then seemed to stabilise at around $6,000, before dropping by more than $2,000 to its new plateau somewhere around $3,500 at the time of writing (end of January 2019). As Figure 3 show, its volatility is still quite substantial, and is currently around 4% for its daily price change. These developments make understanding the valuations of cryptocurrencies increasingly urgent.

Figure 1 Bitcoin price, July 2010 to July 2018 (US$)

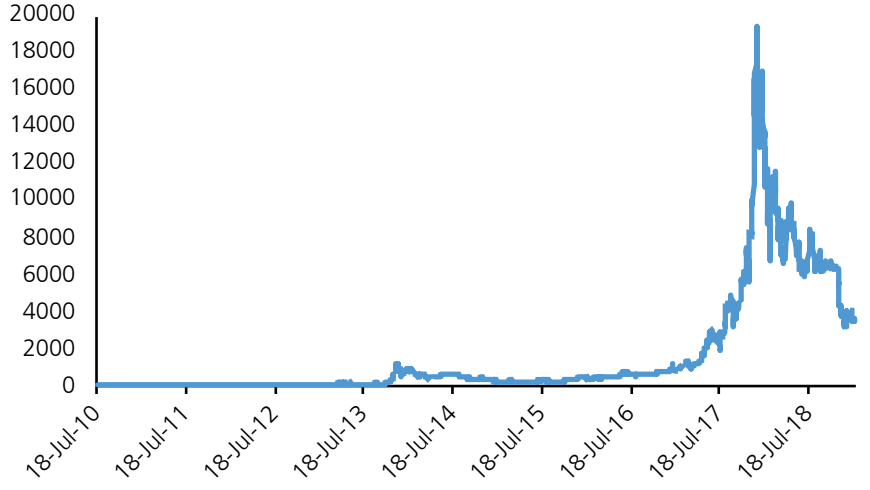


Figure 2 Bitcoin price, November 2017 to January 2019 (US$)

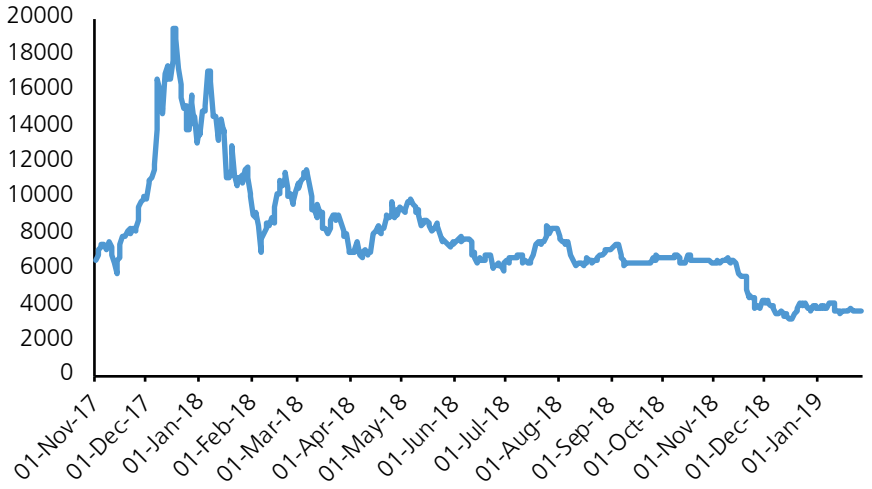
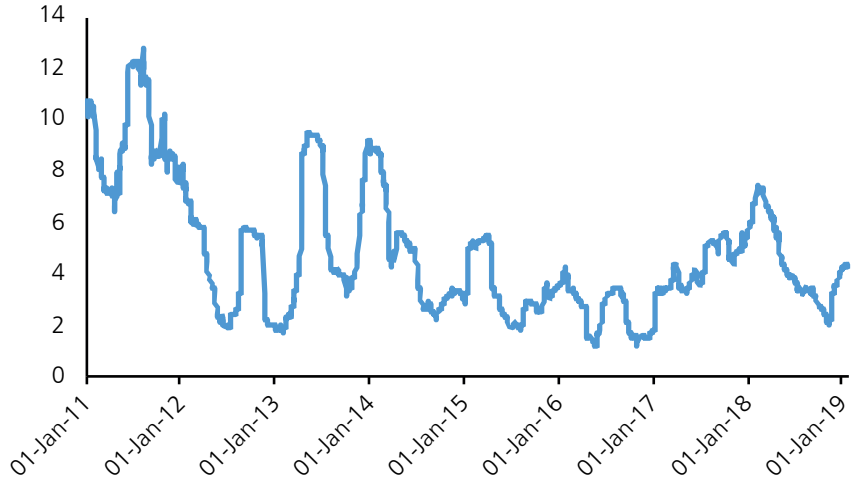


Figure 3 Bitcoin price volatility (daily log changes, 90-day standard deviation, in percent)



There is no Bitcoin central bank

According to a *Financial Times* article in June 2018, the Bank of International Settlements (BIS) traces the instability of crypto prices back to the lack of a crypto central bank. The fact that the value of Bitcoin is not controlled by a designated central bank constitutes a major difference to traditional currencies.

The US Federal Reserve, for instance, injects or withdraws dollars from circulation in order to meet its policy goals, such as a stable rate of inflation. The supply of bitcoin, in contrast, evolves due to decentralised computing activities of 'miners' and can only increase over time. Due to this feature, a traditional tool for promoting price stability is unavailable for cryptocurrencies. The BIS addresses 'unstable value' as one major challenge to cryptocurrencies becoming major currencies in the long run.

Exchange rate indeterminacy and currency speculation

Bitcoins, like dollars, are intrinsically worthless – both are fiat currencies. The co-existence of two fiat currencies, and its analysis, is nothing new. If both are used as a medium of exchange in an economy, then their exchange rate is indetermined, as Kareken and Wallace (1981) showed in a celebrated paper.

With Bitcoin in particular, or cryptocurrencies more generally, new issues arise, however. In particular, the absence of a Bitcoin central bank and the increasing but bounded supply of bitcoins introduce new and potentially important aspects. The observed random fluctuations in the bitcoin price loom large and are absent in the analysis by Kareken and Wallace. Finally, traders may look upon Bitcoin and other cryptocurrencies as an investment, speculating on their rising prices, rather than as a medium of exchange. What are the implications for bitcoin pricing, and for the monetary policy of the traditional currency, when these novel aspects are taken into consideration? In two new papers (Schilling and Uhlig 2018, 2019), we provide some key results.

The setting

We analyse the dual role of Bitcoin (or any other cryptocurrency) as both a medium of exchange as well as an object of speculation. We envision a future world in which both dollars and bitcoins serve as fully accepted means of payment to buy a perishable consumption good. We study the frictionless case in Schilling and Uhlig (2018) and expand the analysis to include transaction costs and exchange rate costs in Schilling and Uhlig (2019). Crucially, we assume that both dollars and bitcoins are intrinsically worthless. In contrast to other assets, holding either of these currencies yields neither dividends nor utility. The only use of fiat currencies is that they can be used to purchase goods. We assume that there is a central bank achieving an exogenously given stochastic inflation target for the dollar, while there is no central agency controlling the value of Bitcoin.

The 'no Bitcoin speculation' result

Our model permits that agents hold back bitcoins to speculate on its future price rise. We find, however, that under reasonably mild assumptions this will not happen in equilibrium. Instead, agents spend both all their dollars and bitcoins in each period. The intuition for the result is an intricate tango between buyers and sellers. If the price of bitcoin were so low today that buyers would not want to part with them to purchase goods, then goods sellers would want to hold bitcoins too and would refuse to sell against dollars. In equilibrium, it must be the case that both sides of the trade are happy. Therefore, if dollars and bitcoins are both used at all, then all of them will change hand at each time period, in equilibrium.

This may not look like the world we currently see. Perhaps there are in fact a large number of traders out there who only hold bitcoins in order to speculate on their appreciation. The model and this line of reasoning then serves to sharpen the intuition about when such a speculative phase must end and why.

A bitcoin pricing equation

Second, we show that in expectation, tomorrow's bitcoin price (expressed in dollars) equals today's bitcoin price corrected by the correlation between the bitcoin price evolution and a nominal pricing kernel, given by the dollar inflation-corrected marginal consumption. Our pricing formula resembles standard consumption-based capital asset pricing model (CCAPM) results (Sharpe 1964, Lintner 1975, Cochrane 2005). This stems from the fact that both the CCAPM and our pricing equation are derived from intertemporal consumption-based models.

There is a significant difference, however. The CCAPM prices assets on the basis that, in equilibrium, agents should be marginally indifferent between consuming more today versus tomorrow. By contrast, our pricing equation arises from the additional indifference between using bitcoins versus dollars for both buyers and sellers. Consequently, our pricing equation exploits intratemporal considerations and our pricing kernel can take a somewhat different form from those used in the CCAPM literature. Intuitively, the expected real return for holding bitcoins, corrected for risk aversion, needs to equal the real return for holding dollars. If this condition was violated, either sellers would refuse to accept one of the currencies or buyers would refuse to part with them. Our pricing formula therefore only requires that agents spend some bitcoins as well as dollars.

The pricing formula can be rewritten in terms of the correlation of the future bitcoin price with the dollar inflation-corrected marginal consumption. If this correlation is negative, then the bitcoin price, expressed in dollars, increases in expectation. On the other hand, under positive correlation, the bitcoin value drops in expectation. In the special case of no correlation (for instance, under risk neutrality of agents and a constant dollar price level), the bitcoin price is a martingale, implying that today's bitcoin price is the best forecast of tomorrow's bitcoin price. Again, note the difference from standard asset pricing results, where such a lack of correlation would instead imply that the asset price increases at the rate of interest.

The crowding out of bitcoins and a bound for the real bitcoin value

Third, we show, if the real value of bitcoin is positively correlated with the marginal utility of consumption, then the total purchasing power of the entire bitcoin stock vanishes over time. This result represents one important implication of the bounded supply of bitcoins. The result holds because the real bitcoin price process is a strict supermartingale (i.e. falls in expectation), given the assumed positive correlation.

Fourth, we show that there exists an upper bound for the real bitcoin value which depends on the maximum output the economy can produce and the current bitcoin stock. The upper bound falls as the bitcoin stock continues to grow. The result is interesting in that it hinges on the fact that the stock of bitcoin can never decline and thus never go to zero, a feature not satisfied by traditional fiat money. In particular, the last two results are driven by the absence of a Bitcoin central bank.

Implications for dollar monetary policy

The competition between bitcoin and the dollar in our model gives rise to an inflation-dependent bitcoin pricing formula. Therefore, bitcoin prices interact with dollar monetary policy. We show that this has both a conventional and an unconventional implication for the dollar central bank. For the conventional implication, we assume that the bitcoin price fluctuations are exogenous. The dollar central bank then needs to take these fluctuations, as well as the supply of cryptocurrency, into account for its dollar supply decisions in order to achieve its desired inflation target. The more goods transactions that are conducted with bitcoins rather than dollars, the more the central bank will have to take the bitcoin price fluctuations and supply into account. For the unconventional perspective, suppose that the dollar inflation target materialises for a broad range of dollar injections. The market clearing condition then implies that the dollar central bank can steer the bitcoin price. More possibilities can arise; in Schilling and Uhlig (2018) we provide a starting point and theory for thinking about these issues.

Ultimately, however, the implications for central banks may be considerably more far-reaching. Central banks used to be monopolists in supplying money, and we may witness

the upending of this comfortable status quo. The current design of cryptocurrencies such as Bitcoin may still lack a number of desirable features, and it may seem that central banks will simply be better at providing the market place with instruments of liquidity and means of payments. We are only at the beginning of the evolution of this market, however, and privately issued monies already provide some advantages over monies offered by central banks. The range of smart contracts that it is currently feasible to embed in Bitcoin transactions extends considerably beyond what is possible with current cash transactions, but also with future central bank digital currency, as currently envisioned. Transactions with cryptocurrencies may offer protection in terms of privacy that a central bank might be tempted to violate. It should come as no surprise if the competitive forces of the market place were to drive innovations beyond what government-run agencies such as central banks will do on their own. Where will this take us? Time will tell.

References

Cochrane, J (2005), *Asset Pricing* (Revised Edition), Princeton University Press.

Financial Times (2018), "'Environmental disaster': BIS warns on cryptocurrencies", 18 June.

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

Lintner, J (1975), "The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets", in W T Ziemba and R G Vickson (eds), *Stochastic Optimization Models in Finance*, Academic Press, pp. 131-155.

Schilling, L and H Uhlig (2018), "Some Simple Bitcoin Economics", NBER Working Paper 24483.

Schilling, L and H Uhlig (2019), "Currency Substitution under Transaction Costs", forthcoming in *American Economic Review Papers & Proceedings*.

Sharpe, W F (1964), "Capital asset prices: A theory of market equilibrium under conditions of risk", *The Journal of Finance* 19(3): 425-442.

About the authors

Linda Schilling is an Assistant Professor at the economics department of Ecole Polytechnique CREST. She holds a Ph.D. in Economics from the University of Bonn. Her research interests are in financial economics, finance and microeconomic theory with the main focus on financial regulation, financial intermediation, and asset pricing.

Harald Uhlig is the Bruce Allen and Barbara Ritzenthaler Professor of Economics at the Kenneth C. Griffin Department of Economics of the University of Chicago since 2007, and was chairman of that department from 2009 to 2012. Previously, he held positions at Princeton, Tilburg University and the Humboldt Universität Berlin. His research interests are in quantitative macroeconomics, financial markets and Bayesian econometrics. He served as co-editor of *Econometrica* from 2006 to 2010 and as editor of the *Journal of Political Economy* since 2012 (head editor since 2013). He is a consultant of the Bundesbank, the ECB and the Federal Reserve Bank of Chicago. He is a fellow of the Econometric Society and a recipient of the Gossen Preis of the *Verein für Socialpolitik*, awarded annually to an economist in the German-language area whose work has gained an international reputation.

5 The doomsday economics of 'proof-of-work' in cryptocurrencies

Raphael A. Auer[1]
Bank for International Settlements

Much of the allure surrounding Bitcoin and related cryptocurrencies stems from the facts that no government is needed to issue them, and they can be held and traded without a bank account. Instead, they are exchanged via simple technical protocols for communication between participants, as well as a publicly shared ledger of transactions (a blockchain) that is updated by a decentralised network of 'miners' via costly computations (i.e. 'proof-of-work') (see Figure 1).

What is the economic potential of this new means of exchange? In a new paper (Auer 2019), I analyse the underlying economics of how Bitcoin achieves payment finality – i.e. how it seeks to make a payment unalterable once included in the blockchain, so that it can be considered as irrevocable. I then discuss the future of this type of cryptocurrency in general.[2]

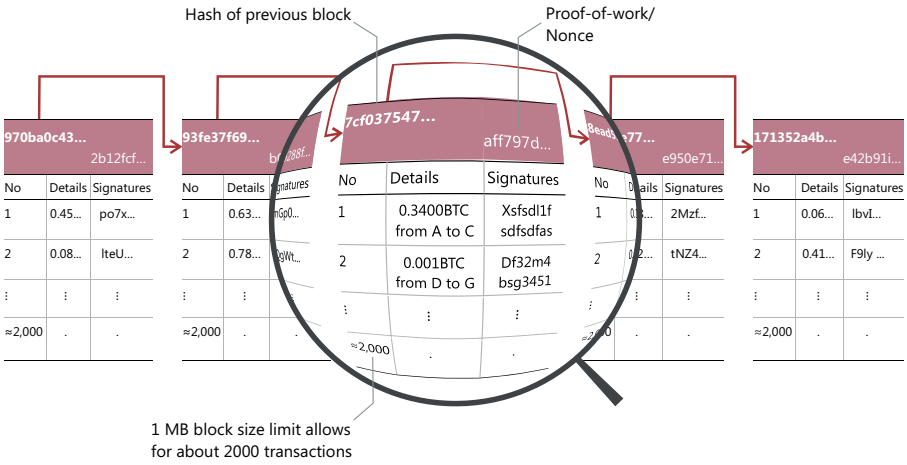
The key innovation of Nakamoto (2008) is to balance the cost and reward for updating the blockchain by creating incentives to ensure that updates are correct. The updating process deters forgeries by imposing a cost on updating the blockchain. At the same time, accurate updating of the blockchain confers a reward on the so-called miners who do the updating. Miners, or their computers, effectively compete to solve a mathematical problem. Presenting a solution proves that they have done a certain amount

1 The views expressed here are those of the author and should not be attributed to the Bank for International Settlements.

2 My focus lies on the technical elements underlying Bitcoin and its blockchain, as devised by Nakamoto (2008), but my conclusions extend to cryptocurrencies that are slightly modified clones of Bitcoin (e.g. Bitcoin Cash, Bitcoin SV, or Litecoin) or digital tokens that, so far at least, share the crucial reliance on proof-of-work to underpin their payment finality (e.g. Ethereum or Monero).

of computational work. Such 'proof-of-work' allows a miner to add a block of newly processed transactions to the blockchain, collecting fees from the subject transactions as well as 'block rewards' – newly minted bitcoins that increase the outstanding supply.

Figure 1 Cryptographically chained, valid blocks of transactions form Bitcoin's blockchain



Notes: The publicly available ledger is updated in bunches of transactions, and each update is termed a 'block'. Blocks, in turn, are chained to each other sequentially, thus forming a 'blockchain'. The blockchain is updated much like adding individual pages with new transactions to a ledger, with page numbers determining the order of the individual pages. Each block is a small file that includes a number of payment transactions, stating the amount, the payer and the payee, and also the transaction fee. The original Bitcoin protocol restricts each block to a maximum file size of 1 MB, which in practice implies that around 2,000 transactions can be included in each block. Only transactions including the valid digital signature associated with the transferred funds are accepted into a block. A new block is added to the blockchain only about once every ten minutes. Adding a block to the existing block chain requires a valid proof-of-work (also called a 'nonce'), which involves a hash function that takes a random text input and produces from this an output according to set rules. The key property of the SHA256 hash function used in the Bitcoin protocol is that the output is unpredictable – to get a desired result, the only solution is thus to try many starting values randomly, which creates a computing cost. Cryptographic chaining of blocks is achieved by including summary information from the previous block in the proof-of-work of the current block.

Source: Auer (2019).

The costs and rewards of Nakamoto's updating process are the focus of my discussion. Two questions are raised. First, how efficient is the fundamental architecture of deterring forgeries via costly proof-of-work? And second, can the market for transactions actually generate rewards that are valuable enough to ensure that payment finality is really achieved?

Analysing these two elements uncovers fundamental economic limitations that cloud the future of cryptocurrencies based on proof-of-work. In sum, with the current technology, it is not even clear whether such cryptocurrencies can keep functioning as

they do at the time of writing. This statement is unrelated to well-known restrictions on the scale of such payment systems or the volatility of cryptocurrencies.[3] Rather, it concerns the fundamentals of Nakamoto's updating process, which has two limitations that interact in a fateful manner.

The first limitation is that proof-of-work axiomatically requires high transaction costs to ensure payment finality. Counterfeiters can attack bitcoin via a 'double-spending' strategy: spending in one block and later undoing this by releasing a forged blockchain in which the transactions are erased. I analyse the concept of '*economic payment finality*' in a blockchain. That is, a payment can be considered final only once it is unprofitable for any potential adversary to undo it with a double-spending attack.[4] If the incentives of potential attackers are analysed, it is clear that the cost of economic payment finality is extreme (see also Budish 2018 on this issue). For example, for finality within six blocks (roughly one hour), back of the envelope calculations suggest that mining income must amount to 8.3% of the transaction volume – a multiple of transaction fees in today's mainstream payment services.

The underlying intuition is simple: double-spending is very profitable. In fact, attackers stand to gain a much higher bitcoin income than does an honest miner. While honest miners simply collect block rewards and transaction fees, counterfeiters collect not only any block rewards and transaction fees in the forged chain, but also the amount that was double-spent (i.e. the value of the voided transactions). This '*attacker advantage*' ultimately translates into a very high required ratio for miners' income as compared with the transaction volume (the amount that can be double-spent).

The second fundamental economic limitation is that the system cannot generate transaction fees in line with the goal of guaranteeing payment security. Either the system works below capacity and users' incentives to set transaction fees are very low,

3 On limited scale and volatility, see in particular Bank for International Settlements (2018).

4 This economic concept differs starkly from the operational considerations of finality in Nakamoto (2008), who examines a double-spending attack by a large miner controlling a significant fraction of the network's computational power. Nakamoto's definition of payment finality (although not explicitly spelled out as such) is thus operational: the deeper a payment is buried in the ledger, the less likely an adversary with given computational resources will succeed in a double-spending attack.

or the system becomes congested.[5] Underlying this is a key externality: the proof-of-work, and hence the level of security, is determined at the level of the block one's transaction is included in, with protection also being provided by the proofs-of-work for subsequent blocks. In contrast, the fee is set by each user privately, hence creating a classical free-rider problem, amounting to a veritable '*tragedy of the common chain*'. While each user would benefit from high transaction fee income for the miner, the incentives to contribute with one's own fee are low.

My key takeaway concerns the interaction of these two limitations: proof-of-work can only achieve payment security if mining income is high, but the transaction market does not generate an adequate level of income.[6] As a result, liquidity is set to deteriorate substantially in years to come.

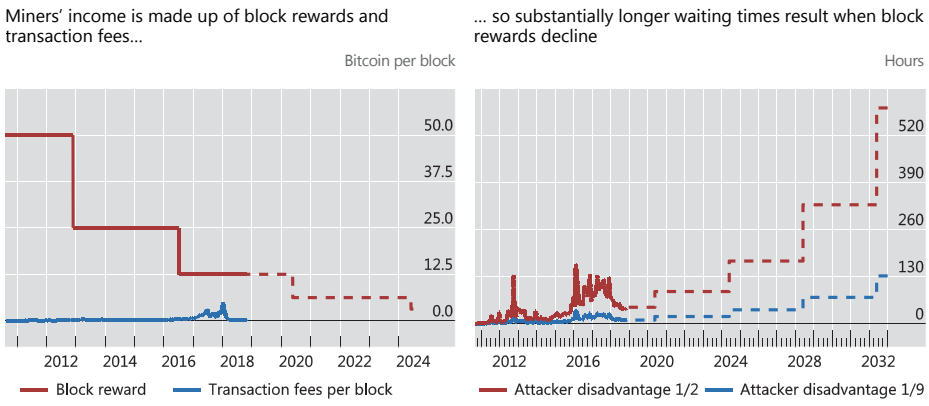
The backdrop is that the bulk of miners' current income consists of block rewards (Figure 2, left-hand side). But block rewards are being phased out (e.g in Bitcoin and many of the clones that have 'forked' from it, the next time block rewards will halve is in 2020). Whenever block rewards decrease, the security of payments decreases and transaction fees become more important to guarantee the finality of payments. However, the economic design of the transaction market fails to generate high enough fees. A simple model suggests that ultimately, it could take nearly a year, or 50,000 blocks, before a payment could be considered 'final' (Figure 2, right-hand side).

Given these considerations, I conclude with a discussion of how technological progress is set to affect the efficiency of Bitcoin and related cryptocurrencies. So-called second-layer solutions such as the Lightning Network that mount further layers of exchange on the blockchain can improve the economics of payment security. However, while they are seeing some adoption (Figure 3, left-hand side), they are no magic bullets, as they face their own scaling issues.

5 See, for example, Huberman et al. (2017) and Easley et al. (2018) for analysis of the case of congestion and associated queuing.

6 Note that Huberman et al. (2017) examine congestion in the market for transaction fees while assuming that "the mining resources are sufficient to guarantee the system's reliability and security" (p. 4), a focus very similar to Easley et al. (2018). In contrast, Budish (2018) examines the economics of security (i.e. of double-spending attacks), but not how mining income is determined. In Auer (2019), I combine these approaches to show how the economics of security and the market for transaction fees interact, i.e. how the market of transactions determines payment security and what this implies for the future liquidity of bitcoin.

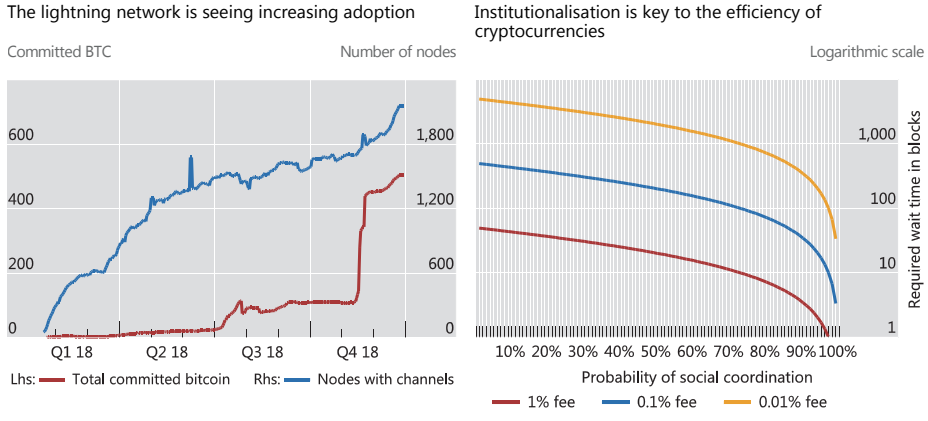
Figure 2 Block rewards have made up the bulk of mining income



Notes: All bitcoins in existence have been issued via 'block rewards'. Every new block added to the block chain increases the total supply, with the newly created bitcoins being credited to the miner who adds the block. Block rewards were set to 50 bitcoins per block initially and are halving every 210,000 blocks (see left-hand panel), a formula ensuring that the total supply of bitcoins will be 21,000,000. Miners' income is made up of block rewards and transaction fees (also see left-hand panel). The lines displayed in the right-hand panel show the implied waiting time (number of block confirmations before merchants can safely assume that a payment is irreversible) required to make an economic attack unprofitable: the attacker rents mining equipment on a short-term basis and executes a change-of-history attack. Calculations of the implied waiting times are based on equation (7) in Auer (2019) and assume transaction fees of 0.18 bitcoin per block, which corresponds to average transaction fees during the period 30 Apr 2018–31 Oct 2018. Dashed pattern indicates predicted values.

Source: Auer (2019).

Figure 3 Looking ahead: Can new technologies counter the deterioration of Bitcoin liquidity?



Notes: The left-hand panel shows the volume of bitcoins that have been committed to the Lightning Network (mainnet) as well as the number of active nodes. The right-hand panel shows the impact on the required waiting times (number of block confirmations before merchants can safely assume that a payment is irreversible) in the case that social coordination is used to undo a double-spending attack. Calculations are based on equation (7) in Auer (2019), assuming that block rewards are zero. The horizontal axis denotes the probability that the network of bitcoin users will coordinate and undo any double-spending attack. The vertical axis shows the resultant required waiting times for various levels of transaction fees.

Source: Auer, R (2019).

In order to prevent liquidity from ebbing away, Bitcoin and other cryptocurrencies would need to depart from using proof-of-work – a system that is not sustainable without block rewards – and embrace other methods for achieving consensus on blockchain updates. Among many proposed developments, the most prominent is 'proof-of-stake' – a system in which coordination on blockchain updates is enforced by ensuring that transaction verifiers pledge their coin holdings as guarantees that their payment confirmations are accurate. Yet, because such a system lacks the solid grounding offered by proof-of-work (which proves actual offline activity), its success may rest on additional overarching coordination mechanisms (i.e. some degree of implicit or explicit coordination by an institution).

Judging based on the current technology, the overall conclusion is that in the digital age too, good money is likely to remain a social rather than a purely technological construct (e.g. Carstens 2018, Borio 2018). That cryptocurrencies might in future profit from social coordination or institutions is also highlighted by the very same algebra that shows the doomsday economics of pure proof-of-work. The point is that their payment efficiency could be greatly improved by introducing an institutional underpinning to undo double-spending attacks should they occur (see Figure 3, right-hand side). In this light, one key question for future research is whether and how technology-supported distributed exchange could complement the existing monetary and financial infrastructure.

References

Auer R (2019), "Beyond the doomsday economics of "Proof-of-work" in cryptocurrencies", BIS Working Papers No. 765.

Bank for International Settlements (2018), *Annual Economic Report*, June.

Borio, C (2018), "On money, debt, trust and central banking", keynote speech at 36th Annual Monetary Conference, Cato Institute, Washington DC, 15 November.

Budish, E (2018), "The economic limits of bitcoin and the blockchain", *NBER Working Papers* no 24717.

Carstens, A (2018), "Money in the digital age: what role for central banks?", lecture at the House of Finance, Goethe University, Frankfurt, 6 February.

Easley, D, M O›Hara and S Basu (2018), "From mining to markets: the evolution of bitcoin transaction fees", *Journal of Financial Economics,* forthcoming.

Huberman, G, J Leshno and C Moellemi (2017), "Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", *Columbia Business School Research Papers* no 17-92.

Nakamoto, S (2008), "Bitcoin: a peer-to-peer electronic cash system", white paper.

About the author

Raphael A. Auer is Principal Economist in the Monetary and Economic Department of the Bank for International Settlements (BIS). He is also a CEPR Research Affiliate and president of the Central Bank Research Association. Prior to joining the BIS, he was Senior Economist, Deputy Head of International Trade and Capital Flows, Economic Advisor and Member of the Directorate at the Swiss National Bank; as well as an associated research professor at the Konjunkturforschungsstelle (KOF) of the Swiss Federal Institute of Technology (ETH). During 2009-10, he was a Globalization and Governance Fellow at Princeton University. He holds a PhD in economics from MIT.

Part 3

Private and public digital money

6 Digital money: Private versus public

Markus Brunnermeier and **Dirk Niepelt**
Princeton University; Study Center Gerzensee and University of Bern

The financial system is undergoing fundamental change. Fintechs and bigtechs are pushing the technological frontier, redefining business models, and forcing banks to adapt. In parallel, new forms of money and alternative payment systems are emerging. Alipay, Apple Pay, Bitcoin and new types of digital central bank money compete with traditional bank deposits. What are the macroeconomic consequences of these new means of payment? We address five key concerns that are frequently put forward:

1. Aren't digital currencies just a hype, now that crypto 'currencies' like Bitcoin have proved too volatile and expensive to serve as reliable stores of value or mediums of exchange? This confuses things. A central bank digital currency (CBDC) is like cash, only digital; Alipay, Apple Pay, WeChat Pay, and so on are like deposits, only handier; and crypto currencies are not in any way linked to typical currencies, but they live on the blockchain.
2. Doesn't a CBDC or 'Reserves for All' choke investment by cutting into bank deposits? No, because new central bank liabilities (namely, a CBDC) would fund new investments, and this would not in any way imply socialism or a stronger role of government in investment decisions.
3. Wouldn't a CBDC cut into the profits that banks generate by creating deposits? Less money creation by banks would certainly affect their profits. But if this were deemed undesirable (by the public, not by shareholders and management) then banks could be compensated.

4. Wouldn't 'Reserves for All' render bank runs more likely, undermining financial stability? We argue that, in fact, the opposite seems more plausible.
5. Aren't deposit insurance, a CBDC, Vollgeld/sovereign money, and the Chicago Plan all alike? There are indeed close parallels between the different monetary regimes. In a sense, "money is changing and yet, it stays the same".

Let us be more explicit.

Crypto is private digital money, but different

Apple Pay, Alipay, M-Pesa and other monies issued by fintechs and bigtechs typically constitute claims to central bank money, or claims to claims to central bank money, or claims to claims to claims to… In this respect, they parallel traditional bank deposits, which also represent commitments to deliver central bank money. Most crypto currencies are different. They do not promise euros, dollars, or Swiss francs (unless their issuers actually invest in fiat currencies and render the crypto stuff redeemable). In fact, the prices of crypto currencies fluctuate wildly relative to the prices of monies issued by central banks. This makes crypto currencies much less useful as means of payment but maybe more useful for hedging purposes (or as easy-to-hide stores of value). From a macroeconomic point of view, crypto currencies pose similar challenges to policy makers as dollarisation – the national currency loses its singularity and, as a consequence, the central bank part of its influence over domestic monetary conditions.

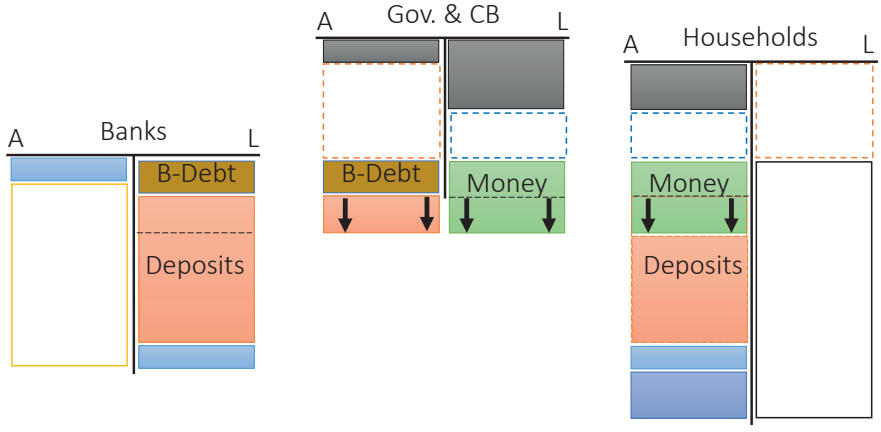
While crypto currencies are quite different from the money issued by banks, they are even more different from central bank-issued money. What would happen, then, if central banks were to issue digital money for the general public, 'Reserves for All', as suggested for example by Tobin (1985, 1987)?

'Reserves for All' would neither choke investment nor herald socialism

True, if people were to swap some of their bank deposits into a CBDC then banks would lose a source of funding. But the central bank would gain funds, and these would have to be invested somewhere. The central bank could start funding real investment – an experiment in 'socialism', and likely a bad one because private banks are arguably better equipped to screen loan applications and monitor projects (and better insulated against political pressure). Alternatively, and preferably, the central bank could pass the funds through to commercial banks, effectively leaving the environment for banks completely unchanged. The important point to note is that a substitution of monies (a CBDC for deposits) only requires new sources of bank funding, not new ownership and control over real assets.

Figure 1 illustrates the effects of the pass-through operation on the balance sheets of banks, the central bank, and households.

Figure 1 The pass-through operation



Notes: The arrows in the green rectangles indicate that households hold fewer deposits but more central bank-issued money, for example in the form of a CBDC. The central bank passes the funds through to banks by holding more deposits, as depicted by the arrows in the red rectangle on the asset side of the central bank's balance sheet.

Banks can be compensated

When issuing deposits in exchange for loans or other assets, banks typically borrow cheaply and lend dearly. (Today, there are some exceptions to this rule as some central banks charge negative interest on the reserves banks hold with them while deposits mostly pay non-negative interest.) Deposit holders go along with this because bank money is useful not only as a store of value but also as a means of payment – money has liquidity value. By creating this value out of 'thin air' (subject to limitations), banks generate seignorage profits. Less bank money creation would eat into those profits.

Some may consider that unfortunate, because they like bank shareholders or are worried about banks' capital base. Others might like it. In any case, the distributive implications of replacing commercial bank by central bank issued money are manageable – banks could easily be compensated if this were so desired.

'Reserves for All' may not increase the risk of bank runs

A frequently made argument against the introduction of a CBDC points to the danger of increased run risk. According to this argument, a CBDC would not foster 'traditional' bank runs where non-banks try to withdraw deposits and convert them into cash. Instead, it would give rise to a novel form with volatile deposit withdrawals in response to swings in sentiment and shifts into a safe-haven CBDC since such swaps would be very easy to conduct and nearly costless.

It is far from obvious, however, whether the introduction of a CBDC would make bank runs more likely. First, when the central bank issues the CBDC and passes funds through to private banks, then the central bank becomes a large, possibly the largest, depositor. But a large depositor that pursues an optimal policy internalises the run externalities and therefore might refrain from running itself. As a consequence, the incentives for the remaining small depositors to run also fall. Hence, a CBDC combined with pass-through funding can make runs *less* rather than more likely.

Second, with the CBDC the central bank gains an informational advantage because it immediately learns from fund inflows when a run is about to start. The central bank can therefore engage more quickly as a lender of last resort, it can more easily prevent

costly fire-sales, and it can better prevent a liquidity problem from morphing into a solvency crisis. If the remaining depositors are aware of this ability to intervene earlier, and more effectively, then they may become less wary themselves, which again reduces the risk of a deposit run.[1]

A related question is whether the central bank would lose control over its balance sheet once the CBDC is introduced. Indeed, a central bank that passes through funds from non-banks to banks lengthens its balance sheet, and if the volume of funds varies over time, so does the length of the balance sheet. There is no reason, however, to be concerned with the length of the central bank's balance sheet per se (especially if some items on the asset and liability side net out) except for the implications on credit risk exposure. This exposure can be minimised with the appropriate collateral policy.

If today, deposits are perfectly liquid and risk-free because of unconditional deposit insurance backed by government guarantees and a lender of last resort, then a CBDC combined with pass-through funding would simply make implicit government guarantees explicit. If deposits are risky, in contrast, then the newly introduced CBDC would have to be accompanied by transfers or taxes in order to exactly replicate outcomes under the contemporaneous regime. In either case, the net wealth and liquidity positions of agents would remain unchanged even if their gross positions reflected in balance sheets might change.

The Chicago Plan, narrow banks and sovereign money (Vollgeld)

The Chicago Plan from the 1930s (Knight et al. 1933, Fisher 1935, 1936), which argues in favour of narrow banks, simply amounts to an introduction of a CBDC that fully replaces deposits. As described above, one way to end fractional reserve banking without changing equilibrium outcomes would be for the central bank to supply deposits – at the same price and conditions as depositors currently do – to banks. This is not what

1 The central bank may also set an unattractive (possibly negative) interest rate on CBDC accounts to avoid that the CBDC is more attractive than cash as a safe-haven asset. Of course, the central bank has to be careful that changes in the CBDC interest rate do not serve as a coordination device for households to start a run.

the proponents of the sovereign money (Vollgeld) proposal envision. According to their proposal, banks should no longer issue deposits but fund themselves from different sources instead. Banks would lose a source of profits – seignorage rents from liquidity creation – and change their policies, with potential implications for macroeconomic outcomes. Of course, it is not clear how the abolition of money creation by banks could ever be enforced in the first place.

Money is changing and yet, it stays the same – an equivalence benchmark

In a recent paper (Brunnermeier and Niepelt 2019), we make this discussion precise. We show formally that as long as a CBDC can serve as a (not necessarily efficient) means of payment for some transactions currently conducted with deposits, a swap of the former for the latter does not have macroeconomic consequences as long as certain conditions are satisfied. Our equivalence result should be construed as a benchmark result that helps to organise one's thinking about complex economic relationships, in the spirit of Modigliani and Miller (1958), Barro (1974), and many other equivalence results in economics. There may exist only a few circumstances under which the sufficient conditions for equivalence literally apply; nevertheless, they give a clear sense of possible sources of non-equivalence in real-world settings.

Maybe the most restrictive condition for the irrelevance of a swap relates to politics (Niepelt 2018). Irrelevance would require, for example, that political decision makers are willing to compensate bank owners for the losses they suffer due to reduced seignorage profits. We doubt that voters would accept this. In fact, one important motivation for the Vollgeld (sovereign money) initiative recently rejected by Swiss voters was to shift rents from banks to taxpayers.

Whether a *non*-neutral monetary reform would be for the better or the worse is a question that our equivalence result cannot address. Answering this would require an explicit characterisation of equilibrium in model economies, as well as serious quantitative and welfare analyses. For policy discussions about monetary reform, we therefore do not propose a set of definite answers, but an analytical framework and a robust road map.

References

Barro, R J (1974), "Are government bonds net wealth?", *Journal of Political Economy* 82(6): 1095-1117.

Brunnermeier, M and D Niepelt (2019), "On the equivalence of private and public money", mimeo, January.

Knight, F (with seven other Chicago economists) (1933), "Memorandum on banking reform", Franklin D. Roosevelt Presidential Library, President's Personal File 431.

Fisher, I (1935), *100% Money*, Adelphi, New York.

Fisher, I (1936), "100% money and the public debt", *Economic Forum* (April-June): 406-420.

Modigliani, F and M Miller (1958), "The cost of capital, corporation finance and the theory of investment", *American Economic Review* 48(3): 261-297.

Niepelt, D (2018), "Reserves for All? Central Bank Digital Currency, Deposits, and their (Non)-Equivalence", CEPR Discussion Paper 13065.

Tobin, J (1985), "Financial innovation and deregulation in perspective", *Bank of Japan Monetary and Economic Studies* 3(2): 19-29.

Tobin, J (1987), "The case for preserving regulatory distinctions", *Chapter 9 in Restructuring the Financial System, Proceedings of the Economic Policy Symposium, Jackson Hole*, Federal Reserve Bank of Kansas City, pp. 167-183.

About the authors

Markus K. Brunnermeier is the Edwards S. Sanford Professor at Princeton University. He is a faculty member of the Department of Economics and director of Princeton's Bendheim Center for Finance. He is also a research associate at NBER, CEPR, and CESifo and a member of the Bellagio Group on the International Economy. He is a Sloan Research Fellow, Fellow of the Econometric Society, Guggenheim Fellow and the recipient of the Bernácer Prize granted for outstanding contributions in the fields of

macroeconomics and finance. He is/was a member of several advisory groups, including to the IMF, the Federal Reserve of New York, the European Systemic Risk Board, the Bundesbank and the U.S. Congressional Budget Office. Brunnermeier was awarded his Ph.D. by the London School of Economics (LSE). His research focuses on international financial markets and the macroeconomy with special emphasis on bubbles, liquidity, financial and monetary price stability.

Dirk Niepelt is director of the Study Center Gerzensee, professor at the University of Bern, and research fellow at CEPR and CESifo. He was an invited professor at several universities, held visiting positions at the ECB and the IMF, and served on the board of the Swiss Society of Economics and Statistics. Prior to completing his doctoral education, he worked at applied research institutes. Niepelt received his PhD in economics from the Massachusetts Institute of Technology and holds licentiate and doctorate degrees from the University of St. Gallen. His interests in economics include macroeconomics, international economics, and public finance.

7 Central bank digital currencies and private banks

David Andolfatto
Federal Reserve Bank of St. Louis

The recent surge of interest in privately issued cryptocurrencies has led a number of economists to investigate the possibility of central bank versions of a digital currency (e.g. Bech and Garratt 2017, Engert and Fung 2017, Kahn et al. 2019). Some, like Bordo and Levin (2017), see a great deal of merit in the proposal. Others, like Cecchetti and Schoenholtz (2017), see less benign consequences. These authors express major worries over the potential repercussions of a central bank digital currency (CBDC) on bank funding, bank credit, and financial market stability– a concern also raised by Bank of England Deputy Governor Ben Broadbent (Broadbent 2016).

Unfortunately, there is not much in the way of evidence or even theory to help shape our views on the matter.[1] In a recent paper (Andolfatto 2018b), I develop a simple theoretical framework to help organise our thinking on the question of how the introduction of a CBDC is likely to impact private banks with market power. Perhaps not surprisingly, I find that the effects are likely to depend on monetary policy and the regulatory landscape. Nevertheless, I think it is of some interest to identify exactly how and why this may be the case.

My framework of analysis combines a version of the Diamond (1965) overlapping-generations model of government debt with the Klein (1971) and Monti (1972) model of a monopoly bank. There are two types of individuals populating the economy, which

1 In some ways, a CBDC is similar to old-style postal savings systems, especially in the manner they competed against commercial banks. Some evidence of the impact of, for example, the US Postal Savings System (1911-1967) would be helpful in this regard. In terms of theory, some related work has been done by Barrdear and Kumhof (2016) and Keister and Sanches (2018).

I refer to as 'workers' and 'investors'. Workers supply the labour that is needed to produce goods and services. Investors have the capacity to transform this labour into a capital good that yields a future return of goods and services. Essentially, investors need to borrow labour and workers want to save for the future. In an ideal world, investors and workers would form cooperatives, with labour and capital combined to produce output that is shared between them. But in my model people are non-cooperative and do not fully trust each other, so an exchange medium is necessary (Gale 1978). In particular, I assume that investor–worker credit arrangements are not practical – workers will only accept money on a *quid pro quo* basis for labour services rendered.

Money takes the form of interest-bearing bank deposit liabilities (digital currency) and zero-interest physical currency (cash).[2] Digital currency can be issued by the private bank and the central bank. In either case, it is made redeemable on demand at par for cash. The private bank has a reserve account with the central bank. Monetary policy consists of setting a policy interest rate that, for simplicity, serves as both a lending and deposit rate for the private bank. That is, the private bank may earn interest on reserves if reserve balances are positive, or it may hold negative reserve balances and pay the policy rate on borrowed reserves. Non-bank individuals can hold deposits with the central bank that yield a different interest rate (the 'CBDC rate'). I assume that non-bank deposits with the central bank cannot be negative. That is, only the private bank is permitted to extend credit to individuals.

Workers in my model differ in terms of their income and face a fixed cost of accessing the bank sector. Consequently, low-income workers in my model will choose to remain unbanked, and must be paid in cash. High-income workers choose to access the interest-bearing deposit accounts made available by the central and private bank. The share of workers choosing to access the bank sector is shown to be increasing in the deposit rate offered by banks. I assume that both central and private banks offer the same payment services so that depositors are indifferent as to where they hold their money. As a result,

2 A digital currency in my model consists of standard account-based money with transactions cleared by a central account manager. The use of distributed ledger technology makes little sense in this context (Berentsen and Schar 2018, Andolfatto 2018a).

the private bank will be compelled to offer at least the CBDC rate on its deposits if it is to retain its depositor base.[3]

Let me now describe the nature of economic activity in my model. At the start of a period, investors need to borrow money to finance their payroll of workers who are employed in the construction of capital. Investors can only acquire funding from the private bank. As a first pass, I assume that investment projects are risk-free and that investors can be relied upon to repay their bank loans. The private bank creates money in the act of lending, crediting each investor's bank account by the amount of the money loan. The model has the intuitively plausible property that the volume of bank lending and capital investment is decreasing in the lending rate. The private bank charges lenders the profit-maximising lending rate which, for the monopolist, trades off profit margin against loan volume. Having acquired a money loan, investors pay their banked workers by deposit transfer and pay their unbanked workers with cash. Workers save their money, which they use to purchase goods and services in the future. Investors use sales of their future output to repay their bank loans and to finance their own consumption.

The model's main proposition asserts that, absent binding liquidity constraints, the private bank's lending behaviour is unaffected by the CBDC (in particular, the CBDC interest rate). This result is a consequence of the fact that, for the Klein-Monti monopoly bank, the profit margin on loans is determined by the lending rate net of the central bank's policy rate, which represents the opportunity cost of commercial lending.[4] The absence of any binding regulatory constraint – such as a reserve or capital requirement, a liquidity-coverage ratio, or a restriction on the amount of reserves that can be borrowed – plays an important role in generating this result. But what this shows is that it is not the CBDC *per se* that can be expected to impact bank lending; rather, it is the way in which the regulatory framework may interact with the CBDC competition that potentially alters the monopoly bank's lending practices. The regulatory framework can, of course, be changed to suit the needs of the public.

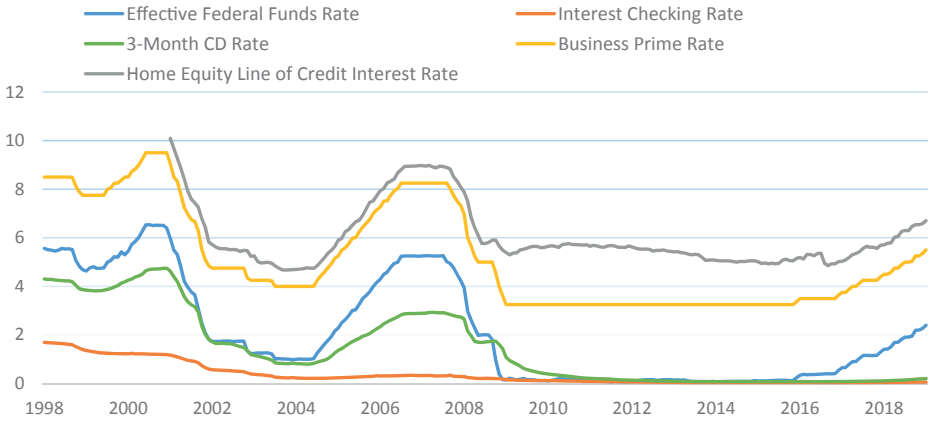
3 This is, of course, an extreme assumption but one which captures the essential idea that the CBDC would compete with the private sector for deposits.

4 Recall that the central bank's policy rate for banks can be set independently of the CBDC policy rate that applies to non-bank entities.

If the CBDC does not affect bank lending, then what does it affect? The model is very clear on this. As long as the CBDC interest rate is below a positive policy rate, the CBDC has the effect of compelling the monopoly bank to increase the deposit rate it offers its customers. The reason for this is because the profit margin on deposits is the difference between the policy rate (e.g. interest on reserves) and the deposit rate. As long as the policy rate is positive, the monopoly bank will always find it profitable to at least match the CBDC interest rate. So in reality, even if the take-up of the CBDC is small, its mere existence may be enough to encourage more attractive terms for depositors. In my model, a higher deposit rate has the effect of increasing financial inclusion – more workers are induced to substitute out of cash and into interest-bearing bank deposits, which leads to an increase in the banking sector's depositor base. Not surprisingly, the CBDC also reduces bank monopoly profits.

What of financial stability concerns? It is difficult to see how the introduction of one more risk-free, interest-bearing government security is likely to be destabilising. True, banks may witness deposit outflows, but they can choose to stem those outflows by offering depositors better terms. The capacity to do so seems evident, at least in the US, judging by the current spread between bank lending and deposit rates (see Figure 1). But even in the event of a large deposit outflow, an interest-targeting central bank should be willing to let banks borrow reserves. As with other considerations, the potential impact of a CBDC on banks and financial markets depends on the policies governments have in place (e.g. Grey forthcoming). It would be of some interest to check the sensitivity of my theoretical results by extending my model to incorporate factors that are missing but potentially important, such as bank and investment risk, moral hazard, regulatory considerations, and open economy considerations.

Figure 1 US interest rates, January 1998 to January 2019 (%)



Sources: RateWatch, Bloomberg and Federal Reserve Board.

Let me conclude with the following observation. In the US today, there exists an efficient, low-cost, real-time gross settlement payment system that transfers close to $3 trillion of funds *per day* across a set of fully insured digital accounts presently yielding 240 basis points in interest. Only depository institutions have access to this service (known as Fedwire) through the reserve accounts they hold with the US Federal Reserve. The rest of the US population must content itself with relatively slow payments, low deposit rates, high interchange fees, limited deposit insurance, or the inconvenience of cash. A significant number of Americans (over 8 million households) do not even have bank accounts. At the same time, the US Treasury permits all US persons to open online interest-bearing treasury accounts, called a TreasuryDirect account.[5] Unfortunately, the existing infrastructure does not permit TreasuryDirect accounts to be used as a convenient payment instrument. However, this is clearly just a technical detail that could be modified with an appropriate change in public policy. Ricks et al. (2018) provide a strong case for why such a change is desirable.

5 See www.treasurydirect.gov

References

Andolfatto, D (2018a), "Blockchain: What It Is, What It Does, and Why You Probably Don't Need One", *Federal Reserve Bank of St. Louis Review* 100(2): 87-95.

Andolfatto, D (2018b), "Assessing the Impact of Central Bank Digital Currency on Private Banks", Federal Reserve Bank of St. Louis Working Paper 2018-026B.

Barrdear, J and M Kumhof (2016), "The Macroeconomics of Central Bank Issued Digital Currencies", Bank of England Staff Working Paper No. 605.

Bech, M L and R Garratt (2017), "Central Bank Cryptocurrencies", *Bank for International Settlements Quarterly Review*, September: 55-70.

Berentsen, A and F Schar (2018), "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies", *Federal Reserve Bank of St. Louis Review* 100(2): 97-106.

Bordo, M D and A T Levin (2017), "Central Bank Digital Currency and the Future of Monetary Policy", NBER Working Paper No. 23711.

Broadbent, B (2016), "Central Banks and Digital Currencies", speech at the London School of Economics, 2 March 2.

Cecchetti, S G and K L Schoenholtz (2017), "Fintech, Central Banking and Digital Currency", *Money and Banking Blog*, 12 June.

Diamond, P A (1965), "National Debt in a Neoclassical Growth Model", *American Economic Review*,55(5): 1126-1150.

Engert, W and B Fung (2017), "Central Bank Digital Currency: Motivations and Implications", Bank of Canada Staff Discussion Paper 16.

Gale, D (1978), "The Core of a Monetary Economy without Trust." *Journal of Economic Theory* 19(2): 456-491.

Grey, R (forthcoming), "Banking Under a Digital Fiat Currency Regime", in G Dimitropoulos, S Eich, P Hacker, and I Lianos (eds), *Regulating Blockchain: Political and Legal Challenges*, Oxford University Press.

Kahn, C M, F Rivadeneyra and T-N Wong (2019), "Should the Central Bank Issue E-money?" Federal ReserveBank of St. Louis Working Paper 2019-003A.

Keister, T and D Sanches (2018), "Managing Aggregate Liquidity: The Role of a Central Bank Digital Currency", Working Paper.

Klein, M A (1971), "A Theory of the Banking Firm", *Journal of Money, Credit and Banking*, 3(2): 205-218.

Monti, M (1972), "Deposit, Credit and Interest Rate Determination under Alternative Bank Objective Functions", in K Shell and G P Szegö (eds), *Mathematical Methods in Investment and Finance,* Elsevier, pp. 431-454.

Ricks, M, J Crawford and L Menand (2018), "A Public Option for Bank Accounts (Or Central Banking for All)", Vanderbilt Law Research Paper 18-33 and UC Hastings Research Paper No. 287.

Author the author

David Andolfatto is a Senior Vice President in the Research Department at the Federal Reserve Bank of St. Louis. He was a professor of economics at the University of Waterloo (1991-2000) and Simon Fraser University (2000-2009), before joining the Fed in July 2009. Mr. Andolfatto has published several articles in the profession's leading economic journals, including the *American Economic Review*, the *Journal of Political Economy*, and the *Journal of Economic Theory*. In 2009, he was awarded the Bank of Canada Fellowship Award for his contributions in the area of money, banking, and monetary policy. Mr. Andolfatto is a native of Vancouver, Canada and received his Ph.D. in economics from the University of Western Ontario in 1994.

8 Stablecoins: The quest for a low-volatility cryptocurrency

Aleksander Berentsen and **Fabian Schär**
Center for Innovative Finance, University of Basel

The 2008 article "Bitcoin: a Peer-To-Peer Electronic Cash System" by Satoshi Nakamoto (Nakamoto 2008) is the most influential contribution to monetary economics of the last 50 years. Interestingly and perhaps tellingly, the article was published in 2008 via a mailing list for cryptography and not in a peer-reviewed scientific journal. The Bitcoin paper and the corresponding software implementation connect several technological components to create a virtual asset that is substantially different from any other asset. For the first time, ownership of virtual property is possible without the need for a central authority – a development with the potential to fundamentally change the current financial system and many areas in both the public and the private sectors (Berentsen and Schär, 2017, 2018).

The Bitcoin technology is fascinating but there are also challenges, including high price volatility. In this chapter, we discuss 'stablecoins' – cryptoassets that are developed with the aim of minimising price volatility by embedding a stability mechanism.

To understand the origins of the enormous price volatility, one needs to appreciate that Bitcoin is a fiat currency. A fiat currency's main characteristic is that it possesses no intrinsic value. Accordingly, its market value is based solely on the public's expectations about its future price, and such expectations can change quickly. Currencies such as the US dollar, the euro, or the Swiss franc are fiat assets the same as bitcoin. What distinguishes bitcoin from these fiat currencies is the absence of a stability mechanism.

The supply of bitcoins is predetermined and converges to 21 million units, after which no additional bitcoin units are produced. This rigid aggregate supply schedule meets a constantly changing aggregate demand driven by rapidly changing expectations. The

result is substantial price volatility. In contrast, all central banks in developed countries attempt to stabilise the value of their currencies. They do this by providing an 'elastic currency', in other words, they adjust the aggregate supply of money to a changing aggregate demand.

The first stablecoins emerged in 2014 (including BitShares, NuBits, and Tether), after which many more flourished. The market capitalisation of all stablecoins at the beginning of 2019 was roughly $2.7 billion (which is 2.2% of the total market capitalisation of all cryptoassets). The largest one is still Tether, with a market capitalisation of around $2 billion. The stablecoin DAI has a market capitalisation of $0.073 billion. We mention it here because of its very interesting design.

There are basically three types of stablecoin, as can be seen from Table 1. In what follows and without loss of generality, we assume that they are all pegged to the US dollar. However, our discussion also applies to stablecoins that are pegged to other currencies, to gold, or to baskets of goods. The distinguishing characteristics between the three types are the stability mechanism and the nature of the collateral.

Table 1 The three types of stablecoin

Goal	Stability mechanism	Type of collateral	Examples
USD parity	Algorithmic	None	Basis
USD parity	Collateralised	On-Chain (e.g. Ether)	DAI
USD parity	Collateralised	Off-Chain (e.g. USD)	Tether

Algorithmic stablecoins

The defining characteristic of a pure algorithmic stablecoin is the absence of collateral. The basic stability mechanism works as follows. If the demand for the stablecoin increases, the issuer will create and sell additional stablecoins in order to maintain the peg to the dollar. If the demand decreases, the issuer issues a second asset, typically a bond, and sells it against the stablecoin in order to reduce the aggregate supply. The bond is a promise to future stablecoins. That is, algorithmic stablecoins attempt to stabilise a falling price by promising to increase the stablecoin supply in the future.

The interested reader might ask why someone would buy such a bond. Our answer is that we do not know, and our recommendation is to be very sceptical. Of all the stability mechanisms that we discuss in this chapter, algorithmic stablecoins are the least convincing, and we strongly recommend against using them.

The most prominent algorithmic stablecoin is called Basis (Nader et al. 2017). It received large amounts of funding, but the project was recently closed and what is left of the funding will be returned to the investors. The official explanation was regulatory issues; however, we believe that the investors finally realised that the economics of the Basis stablecoin rest on shaky foundations.

Collateralised stablecoins: On-chain

The working of a collateralised stablecoin with on-chain collateral is best explained by the DAI stablecoin, which is pegged to the US dollar. DAI is based on a set of smart contracts on the Ethereum blockchain. Everyone can generate new DAI tokens. In order to do so, a user must send Ether – the native cryptocurrency of the Ethereum blockchain – to one of the smart contracts. These funds serve as collateral for a loan in DAI that the user can get. The interest rate is known as the stability fee and is currently very low.[1]

Since a DAI loan is backed up with ether and the price of ether is volatile, the loan has to be over-collateralised. Currently, the minimum collateral is 150%, that is, if a user holds ether to the value of $150 in the smart contract, he can obtain a DAI loan of $100. It is strongly advised to hold much more collateral than 150%. The reason is that if the collateral value falls below 150%, the collateralised debt position (CDP) of the user is automatically liquidated. That is, the ether held as collateral are automatically sold against DAI.

There are additional safeguards in place to guarantee that DAI remains stable against the dollar even under high stress. To explain all of these goes beyond the scope of this chapter, but we would like to encourage the reader to conduct his own research on this very interesting project.

1 See https://makerdao.com/en/whitepaper

Even though the economics are sound, there are a few risks. First, it is possible that the DAI smart contract is faulty and one day behaves in unexpected ways. This is the typical risk that applies to all smart contracts. Second, the DAI smart contract requires price feeds. In particular, the smart contract needs to know the ether price at any point of time. DAI has several distinct ether price feeds and uses a weighted average of these. The price feeds add some centralisation to an otherwise decentralised system and are a potential attack vector. Finally, the DAI stablecoin has kept its value during a time where the ether price lost more than 90%. Nevertheless, we still need to find out how the system would react when the ether price falls by 50% or even more in one day.

We would like to conclude with a final observation. The DAI stablecoin is generated as a result of two agents with different risk attitudes. An agent who wants to increase the risk of his portfolio can leverage his portfolio by sending ether to the DAI smart contract and then receiving a DAI loan. He can then acquire additional ether with the proceeds of the loan, thereby leveraging his position. In contrast, an agent who wants to reduce the risk in his portfolio can sell ether for the DAI stablecoin. Thus, the transfer of risk is at the origin of the demand and the supply of the DAI stablecoin.

Collateralised Stablecoins: Off-chain

By far the largest and best-known collateralised stablecoin is Tether, which was founded in 2014.[2] Tether is associated with the Hong Kong-based exchange platform Bitfinex and the company Tether is incorporated in Hong Kong. The history of the Tether stablecoin reveals the main issues that arise with off-chain collateral: transparency, censorship resistance, and profitability.

First, from its inception there has been a considerable uncertainty whether Tether has been fully backed with an adequate amount of US dollars. On the Tether webpage are statements such as “Tether is always fully transparent” and “Our reserve holdings are published daily”. Unfortunately, we could not find an independent statement of

2 See https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf

their reserve holdings (the statement on their website is from June 2018 and is not downloadable).

Second, holding reserves off-chain in a bank account is a central point of attack. Governments can simply shut down the Tether stablecoin by freezing the dollar reserves. Interestingly, the issuer of the Tether stablecoin had to move its banking relations several times across various jurisdictions for undisclosed reasons.

Third, stability requires that a stablecoin is backed up at 100% of its value and that the assets held as reserves are liquid. Unfortunately, liquid assets such as foreign exchange pay no or very low interest. The main problem for an issuer of a stablecoin is therefore profitability. Tether, for example, charges fees on withdrawals and deposits. In order to make money, an issuer of a fully off-chain stablecoin is always tempted to engage in fractional reserve banking. This is not much different from the traditional banking sector, where fractional reserve banking is the norm. The fact that transparency can only be fully achieved with expensive audits does not help profitability.

Conclusions

Stablecoins will bring many benefits to crypto-land. They can be used in atomic transactions, in smart contracts and for simple payments. For this reason, blockchain enthusiasts will keep innovating relentlessly until they find a working design. There are a few lessons that can already be drawn today.

- First, price stability requires collateral of at least 100%. For that reason, we discard the idea that stability can be attained solely through a fancy algorithm.
- Second, on-chain collateral has many benefits over off-chain collateral. With on-chain collateral, transparency is automatically given as demonstrated by the DAI stablecoin. Every user can verify that the collateral is effectively there. Furthermore, off-chain collateral is a single point of attack and the threat of a sudden closure by an outside entity is clearly present. When the collateral is on-chain, as for the DAI stablecoin, this threat is non-existent.

- Finally, a stablecoin with off-chain collateral typically entails severe costs (e.g. audits and banking relation) and is often issued with a profit motive. This results in a permanent desire to engage in fractional reserve banking as in the traditional banking world. Again, this desire is not present with a decentralised on-chain collateral solution à la DAI.

References

Berentsen, A and F Schär (2018), "A Short Introduction to the World of Cryptocurrencies", Federal Reserve Bank of St. Louis Review, First Quarter: 1-16.

Berentsen, A and F Schär (2017), *Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung*, Books on Demand.

Nader, A-N, J Chen and L Diao (2017), "Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank", Version 0.99.7 (first published 20 June 2017).

Nakamoto, S (2008), "Bitcoin: A Peer-to-Peer Electronic Cash System".

About the authors

Aleksander Berentsen is Professor of Economic Theory and Dean of the Faculty of Business and Economics of the University of Basel. His research interests include monetary economics and blockchain technologies. He held visiting positions at the University of California in Berkeley, the University of Pennsylvania, the University of Zurich and the Free University of Berlin. He is currently research fellow at the Federal Reserve Bank of St. Louis and used to be an external consultant for the Swiss National Bank and the Bank for International Settlements. He has published academic articles in the *American Economic Review, Review of Economic Studies*, and the *Journal of Monetary Economics.*

Fabian Schär is Professor for Distributed Ledger Technology/Fintech and the Managing Director of the Center for Innovative Finance at the University of Basel. He has a PhD in Cryptoassets and Blockchain Technology and co-authored several publications including the bestselling book, *Bitcoin, Blockchain and Cryptoassets*.

In addition, he is a board member of the Swiss Blockchain Federation, an advisor of various blockchain organizations and an invited speaker at numerous conferences, including the G20 Global Financial Stability Conference.

Part 4

Cryptocurrencies, ICOs, and regulation

9 Initial coin offerings: Fundamentally different but highly correlated

Antonio Fatás and **Beatrice Weder di Mauro**
INSEAD and CEPR

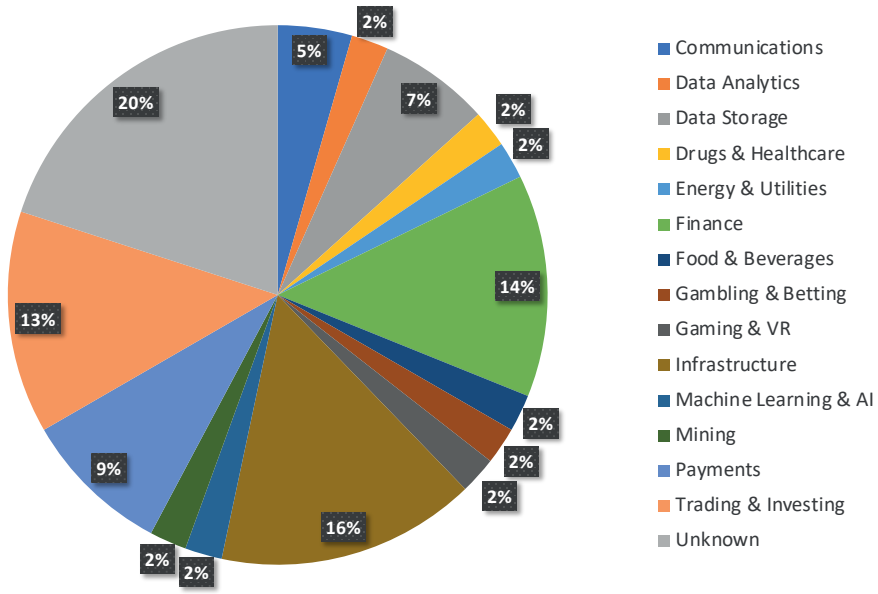
While the Bitcoin hype came under pressure in 2018 as its price collapsed, activity in initial coin offerings (ICOs) still remained significant. Over 1,000 new coins or tokens were created through ICOs in 2018, raising over US$21 billion.[1] The two largest ICOs (pre-sale) – Telegram and EOS – raised $1.7 billion and $4.2 billion, respectively, and the next largest also raised over $500 million. Investors, aspiring entrepreneurs, and also policymakers and regulators have been paying increasing attention to this new market. What are the characteristics of ICOs? What are the benefits and risks? Do ICOs represent a new model of funding or is their fate linked to the world of cryptocurrencies?

ICOs as innovative funding models

While ICOs typically rely on a similar technology to that used in cryptocurrencies (i.e. blockchain), their purpose is much wider than just facilitating payments. ICOs can be seen as a new funding model for new ventures. ICOs differ from traditional forms of funding because the founders often do not retain control of the platform after its launch, an attractive feature for those who like the idea of decentralised power. While many ICOs are in the IT space, there have also been many cases in other industries, ranging from health care, energy, and finance to infrastructure (see Figure 1).

1 Source: CoinSchedule (https://www.coinschedule.com/stats.html?year=2018).

Figure 1 Share of each sector in the 50 largest ICOs



Source: Author's calculations based on list of largest ICOs at https://www.coinist.io/monthly-ico/

ICOs involve two types of tokens: security tokens and utility tokens. Security tokens offer participation in governance and future earnings, and are thus more akin to equity. Regulators have increasingly taken the view that the issuance of such tokens should be subject to the same regulations as securities, implying high regulatory costs.

To avoid potential regulation, most recent ICOs have involved utility tokens, where no ownership or dividends are granted to token holders. Utility tokens instead promise their holders access to the venture's future services. This model works because most of the projects relate to building a platform around a community of users trading certain services (for example, Filecoin is a platform to exchange decentralised electronic storage services). As a result, the ICO not only raises the funding for the project but also puts into motion the launch of the network of future users.

The ICO funding model, like peer-to-peer lending, promises to reduce intermediation costs. But ICOs are more closely related to crowdfunding platforms, as the investment is linked to the use of the company's product in a way that helps companies and markets better gauge the potential demand for the service, and it also creates a degree

of customer commitment (Howell et al. 2018). The novelty of ICOs is that they promise 'exclusive' access to a service that is restricted to holders of a new token. For users of the platforms, tokens are the only way to purchase the service. And because demand is uncertain and possibly increases as the venture becomes successful, holders of tokens are often promised returns through increases in the value of the token.

Why is a new currency or token needed? Many ICO projects are related to platforms with strong network effects. Having investors committing to also being customers can create the necessary critical mass to make a project successful (Li and Mann 2018). This is what we observe empirically, with many ICOs are willing to underprice tokens in the initial phases in the hope of creating the necessary liquidity and critical mass (Momtaz 2018).

The limitations and risks of ICOs

While there are potential benefits to ICOs, there are also costs. The creation of separate tokens for services resembles a world in which products and services are priced in their own currency and transactions take place through barter, the equivalent to a modern "Stone Age world of the Flintstones" (Roubini 2018). This scenario runs contrary to the economic intuition that strong network effects of money of a single unit of account (i.e. one currency) always dominate a tokenised economy.

In addition, selling tokens to access future services and products requires a strong and verifiable commitment regarding the number of tokens or the price of the service (both of them related).[2] The lack of a credible commitment technology could reduce the potential additional funding that the business might need and undermine the value of the ICO (Catalini and Gans 2018).

From the point of view of the investor, there can also be concerns about token values. Many early investors are betting on the popularity of the service associated with the

2 Many ICOs explain the logic of token pricing via an equation that resembles the quantitative theory of money. If the value of transactions (measured in US dollars) increases over time, given the limited supply of tokens, the value of each of these tokens (in US dollars) will have to increase to satisfy the demand.

token increasing so that the value of the token increases and delivers a return. But there can be a contradiction here – returns can only be realised when tokens are used, but tokens are only bought by investors speculating on a return.

The final potential risk is that ICOs do not have any inherent economic advantage, but are attractive simply because they offer a way of avoiding the regulatory costs related to securities laws and investor protection. In the worst-case scenario, they allow fraudulent projects to lure in small-time investors. The large number of ICOs that have failed provide support to these concerns.

The performance of ICOs as a funding vehicle

Because of the novelty of ICOs it is difficult to establish at this stage whether the potential benefits outweigh the risks and costs. Howell et al. (2018) provide evidence that successful ICOs have characteristics that are similar to successful projects that raise funds using alternative methods, reporting that "liquidity and trading volume are higher when issuers offer voluntary disclosure, credibly commit to the project, and signal quality". On the other hand, Fisch (2018), using a similar methodology, finds mixed results.

Given the strong connection between ICOs and the world of cryptocurrencies, one of the fears has been that investors have bought ICO tokens because they were seen as a quick source of high returns. We now investigate whether ICO prices reflect this behaviour.

Our assumption is that there will be a positive correlation with returns on other cryptocurrencies because ICOs tend to rely on a similar infrastructure (many ICOs rely on Ethereum, for example). At the same time, the correlation cannot be too high given that the business model of Bitcoin or Ethereum, as alternative payment systems or token platforms, is quite different from the business models of most ICOs. As we have shown before, we find ICOs in a variety of sectors.

We study this correlation empirically by collecting data on the pricing of the largest 50 ICOs and test whether the behaviour of ICO returns are correlated to the returns of Bitcoin and Ethereum. If ICOs are truly pricing their unique business models, we would expect their returns to be idiosyncratic with low correlations. If, on the other

hand, they are simply seen as an investment vehicle to generate excess returns based on a 'cryptocurrency bubble', we would expect them to be highly correlated to prices of the major cryptocurrencies.[3]

We calculate the daily correlation between the daily return of the top 50 ICOSs with the return of Bitcoin and Ethereum using a 30-day rolling window.[4] The results are shown in Figures 2 and 3, where we plot the evolution of the price of the two cryptocurrencies in the same charts to understand whether the correlation has changed over time as the sentiment towards these currencies has changed.

Figure 2 Correlation of daily ICO returns with Bitcoin returns

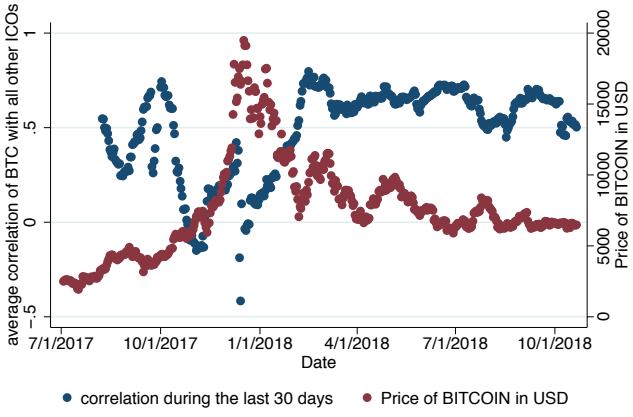
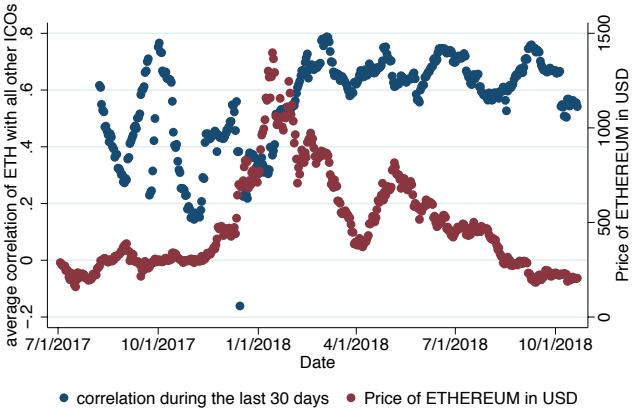


Figure 3 Correlation of daily ICO returns with Ethereum returns



3 Hu et al. (2018) also provide an analysis of the behavior of returns of cryptocurrencies and ICOs.

4 Price data from https://coinmarketcap.com

Correlations remained positive but low while the cryptocurrency phenomenon was taking off and Bitcoin and Ethereum prices were increasing. However, once the price of the two cryptocurrencies starts falling, correlations increase and reach a very high level, signalling that daily news on the future of Bitcoin and Ethereum seema to be moving the price of all ICO tokens. It seems that as the 'cryptocurrency bubble' bursts, the price-discovery mechanism of ICOs collapses and all their prices just track the value of Bitcoin or Ethereum.

Conclusions

ICOs are seen as funding vehicles and have been used to finance thousands of ventures in many different industries. We should not expect a high correlation between tokens and the price of Bitcoin or Ethereum given that they have very different business cases. This seems to have been the case during 2017, but the moment the Bitcoin/Ethereum bubble burst, the correlation with ICOs increased and remained very high even when prices had stabilised.

There are two interpretations of this pattern. The benign one is that the ICO market is still in its infancy and will need to mature. When ICOs grow up, we might expect them to be seen as very distant relatives of Bitcoin or Ethereum and to be priced according to their own merit. The alternative is that ICOs were just one of the children of the hype and are likely to share the fate of major cryptocurrencies.

References

Catalini, C and J S Gans (2018), "Initial Coin Offerings and the Value of Crypto Tokens", SSRN Scholarly Paper.

Fisch, C (2018), "Initial Coin Offerings (ICOs) to Finance New Ventures: An Exploratory Study", SSRN Scholarly Paper.

Howell, S T, M Niessner and D Yermack (2018), "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales", NBER Working Paper 24774.

Hu, A, C A Parlour and U Rajan (2018), "Cryptocurrencies: Stylized Facts on a New Investible Instrument",

Li, J and W Mann (2018), "Initial Coin Offering and Platform Building", SSRN Scholarly Paper.

Momtaz, P P (2018), "Initial Coin Offerings", SSRN Scholarly Paper.

Roubini, N (2018), "Initial Coin Scams", Project Syndicate, 10 May.

About the authors

Antonio Fatas is the Portuguese Council Chaired Professor of Economics at INSEAD, an international business school with campuses in Fontainebleau (France) and Singapore. During the 2008-09 academic year he was on a sabbatical from INSEAD as a Research Fellow in Residence at the Center for Business and Public Policy at the McDonough School of Business (Georgetown University). He received a Masters and Ph.D. in Economics from Harvard University (Cambridge, MA, USA). He has also worked as an External Consultant at the International Monetary Fund, the World Bank, the OECD and the European Commission. He was the Dean of the MBA programme at INSEAD from September 2004 to August 2008. His research covers areas such as the macroeconomic effects of fiscal policy, the connections between business cycles and growth and the effects of institutions on macroeconomic policy and has been published in academic journals such as *Quarterly Journal of Economics, Journal of Monetary Economics, Journal of Economic Growth, Journal of Money, Banking and Credit*, and *Economic Policy*.

Beatrice Weder di Mauro is Professor of International Economics at the Graduate Institute of Geneva and Distinguished Fellow at the INSEAD Emerging Markets Institute, Singapore. Since July 2018, she has served as President of CEPR. From 2001 to 2018, she held the Chair of International Macroeconomics at the University of Mainz, Germany, and from 2004 to 2012 she served on the German Council of Economic Experts. She was Assistant Professor at the University of Basel and Economist at the International Monetary Fund. She has held visiting positions at Harvard University, the National Bureau of Economic Research and the United Nations University in Tokyo.She

has also served as consultant to governments, international organizations and central banks (European Commission, International Monetary Fund, World Bank, European Central Bank, Deutsche Bundesbank, OECD, among others). She has published widely in leading academic journals, including the *American Economic Review, Journal of International Economics, Brookings Papers on Economic Activity, Journal of Public Economics, Journal of Development Economics* and *Review of Finance*. She is an independent director on the board of Bombardier, UBS and Bosch, a senior fellow at the Asian Bureau of Finance and Economics Research (ABFER), a member of the ETH Foundation, the International Advisory Board of Bocconi and a member of the Bellagio Group.

10 Cryptocurrencies: Why not (to) regulate?

Raphael Auer and **Stijn Claessens**[1]
Bank for International Settlements and CEPR

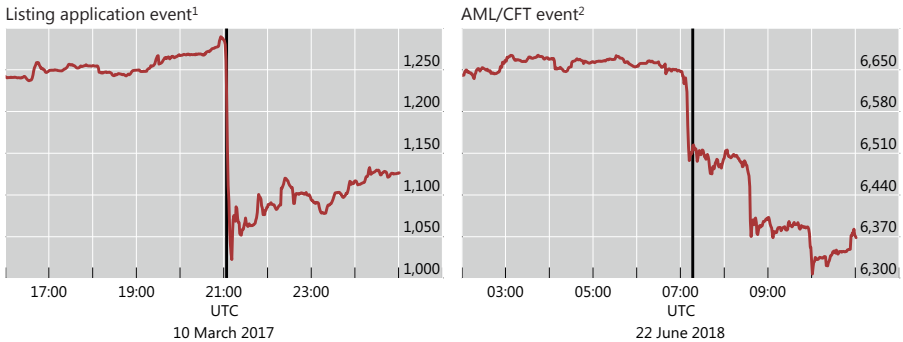
Cryptocurrencies such as Bitcoin or Ethereum have attracted much attention, because of both meteoric price swings and their advocates' claim that they represent a new model of decentralised trust. Many are analysing the validity of such claims and the economics of the underlying technology (e.g. Auer 2019, Biais et al 2018, Morris and Shin 2018, Huberman et al. 2018). Concurrently, many national authorities and international bodies have expressed concerns about market integrity and consumer protection issues, as well as the scope opened up for illicit activities such as money laundering and terrorist financing (e.g. CPMI 2015, G20 Finance Ministers and Central Bank Governors 2018, Bank for International Settlements 2018, Carstens 2018a,b, Financial Stability Board 2018, Carney 2018).

Cryptocurrencies are often thought to operate beyond the reach of individual national authorities, as they can function without institutional backing and are inherently borderless. Yet, a number of jurisdictions have announced at various points in the last year that they are considering whether and how to respond, and some have already responded. In Auer and Claessens (2018a), we examine whether and how regulatory actions and communications about such actions have affected cryptocurrency markets. We do so using an event study approach, i.e. we use the market reactions to these regulatory statements and decisions to assess the anticipated effects on cryptocurrency markets.

1 We thank Giulio Cornelli for superb assistance in the development of the dataset and the analysis. The views expressed here are those of the authors and should not be attributed to the Bank for International Settlements. This chapter is partly based on Auer and Claessens (2018b).

To illustrate our methodology, consider two events. One is the decision by the United States Securities and Exchange Commission (SEC) in March 2017 to turn down a proposal to alter stock exchange rules so as to allow the creation of an exchange-traded fund (ETF) for bitcoin. In the five minutes around the announcement, the price of bitcoin dropped by 16% (Figure 1, left-hand panel).[2] Another event is the Japanese Financial Services Agency (FSA) ordering six cryptocurrency exchanges to improve their money laundering procedures (June 2018). Again, prices tanked – although it seems to have taken several hours, until the start of the US trading day, for this measure to have its full effect (right-hand panel).[3]

Figure 1 Bitcoin intraday price reaction to two news events (US dollars)



Notes: 1 The vertical line indicates 21:04 on 10 March 2017 (news headline: "US SEC rejects application to list Bitcoin ETF"). 2 The vertical line indicates 07:17 on 22 June 2018 (news headline: "RPT – Japan FSA says ordered 6 cryptocurrency exchanges to improve business, over lax money laundering measures").

Source: Auer and Claessens (2018a).

We then proceed to assemble a systematic database of regulatory news events, which can be accessed here along with replication material, and classify news events into three categories: legal status, anti-money laundering/combating the financing of terrorism (AML/CFT) and interoperability, and unspecific general warnings.

- **Legal status news.** Figure 2 examines returns surrounding four specific categories of legal news. News pointing to an outright ban and non-recognition of the instruments as currencies is associated with negative returns, and strongly so for

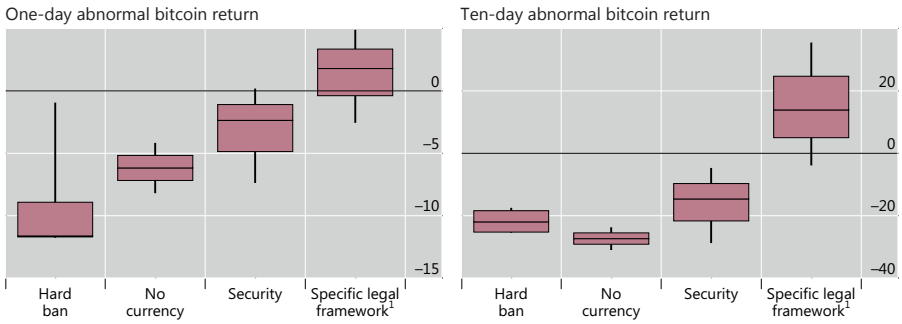
2 Relatedly, the SEC's reconfirmation of the denial of a bitcoin ETF fund listing on 26 July 2018 sent the price of bitcoin tumbling from $8,220 to $7,920 (–3.7%) within a short period.

3 This event may have had a particularly profound effect as it contrasted with the previously held belief that the FSA was sympathetic towards cryptocurrencies compared with other financial supervisors.

bans. News suggesting that cryptocurrencies could be treated as securities also leads to negative returns, probably reflecting the expectation that cryptocurrencies would be regulated more stringently. In contrast, the introduction of a specific, non-security legal framework generates positive returns, most likely as those frameworks generally come with oversight rules that are milder than those under securities law.

- These effects are large and persist over time. The responses are qualitatively consistent between the one-day (left-hand panel) and the 10-day impact (right-hand panel), with the latter generally more pronounced. We also examine the response to other news events.

Figure 2 Legal status news and bitcoin returns (%)



Notes: The box plots show minimum, lower quartile, median, upper quartile and maximum. 1 Other than a security legal framework.

Source: Auer and Claessens (2018a).

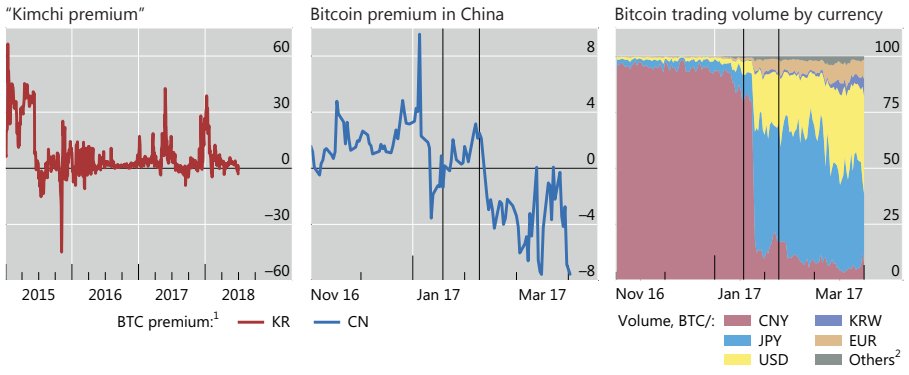
- **AML/CFT and interoperability.** We find that regulatory news regarding AML/CFT measures and limits on the interoperability of cryptocurrencies with the regulated financial system adversely impacts cryptocurrency markets.
- **General warnings.** In contrast, general warnings about cryptocurrencies, including about the risk of loss, have little discernible effect on prices. In this sense, moral suasion alone does not seem to work in stemming speculative markets.

Why do news events about national regulations have such an impact on cryptoassets that have no formal legal homes and are traded internationally? Part of our interpretation is that cryptocurrencies rely on regulated institutions to convert regular currency into and out of cryptocurrencies. After all, it is the price of cryptocurrencies in terms of conventional money that hogs the headlines and generates speculative activity. Their cumbersome setup also means that many consumers hold and transact

in cryptocurrencies through interfaces, such as online crypto-wallets, that are often regulated or can be regulated in principle. And international arbitrage is still limited. Agents cannot easily access cryptocurrency markets offshore – because they may need to have a bank account in the foreign jurisdiction. Factors such as these create market segmentation and fragmentation, which currently make national regulatory actions bind to some degree.[4]

One example of likely market segmentation is the 'Kimchi premium' – i.e. the fact that the price of bitcoin in Korea regularly exceeds that in the US, at times by over 50% (Figure 3, left-hand panel). This suggests limits to cross-border arbitrage. Similarly, news about cryptocurrency regulation by authorities in China has led at times to price differentials compared with the US market (Figure 3, centre panel).

Figure 3 Premia and trading volume (%)



Notes: The vertical lines in the centre and right-hand panels indicate 19 January 2017 ("MEDIA-PBOC branch finds 'hidden risks' in bitcoin exchange BTCC-EID") and 9 February 2017 ("China central bank says warned bitcoin exchanges of closure risk on rule violations"). 1 Premium of local BTC price (in USD) compared with BTC price in the United States. 2 AUD, CHF, CAD, GBP, HKD, ILS, INR, PHP and SGD.

Source: Auer and Claessens (2018a).

While arbitrage is imperfect, the markets are obviously interconnected. Accordingly, we find that national regulatory measures do spill across borders. For example, when China hinted at the possibility of strict regulation of Bitcoin around the end of January

4 Another channel would be the reputation effect: the possibility that a decision by one government could encourage other governments to adopt an 'anti-crypto' mind-set.

2017, bitcoin trading shifted massively towards other Asian currencies (Figure 3, right-hand panel).

Overall, our analysis suggests that there is scope for national financial authorities to apply some existing and new regulations to cryptocurrencies, in the sense if they choose to do so, even unilateral actions have an impact. This does not answer the much more difficult question as to whether there is some value in passing regulatory frameworks specific to cryptocurrencies. Here several considerations arise.

For one, such rules risk giving credibility to cryptocurrencies. It would require establishing the case that cryptocurrencies are economically useful, including as a means of payments. This has surely not yet been established (Bank for International Settlements 2018). A particular point of importance regards the limitations of proof-of-work security and the uncertain outlook regarding alternative technologies (Auer 2019).

The alternative, the option of 'benign neglect,' however, cannot be a solution either. Cryptocurrencies are the payment means of choice in the 'darknet' – the global marketplace for drugs, weapons and other illegal objects. In fact, their use is so pervasive that cryptocurrency prices collapsed when the FBI shut down one major darknet marketplace – Silkroad – in 2013. The technology is also being used for the financing of other illicit activities.[5]

The lack of clarity does not mean no regulatory actions are needed. The likely most important near-term response concerns effective global, risk-based actions to reduce the AML/CFT risks associated with cryptocurrencies and other virtual assets. This is

5 The ongoing investigation into the use of BTC to manipulate the 2016 US presidential election provides one example. The US Department of Justice charged that to hack "into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election and releasing the stolen documents—the Defendants conspired to launder the equivalent of more than $95,000 through a web of transactions structured to capitalize on the perceived anonymity of cryptocurrencies such as bitcoin" (US Department of Justice 2018).

also singled out by a recent communique by the Financial Action Task Force.[6] Once the AML/CFT concerns are addressed, – i.e. there is a level the playing field for cryptocurrencies compared to other payment means – one can assess the true economic use case for the technology and accordingly their proper regulation.

References

Auer, R (2019), "Beyond the doomsday economics of proof-of-work in cryptocurrencies", BIS working papers No. 765.

Auer, R and S Claessens (2018a), "Regulating cryptocurrencies: assessing market reactions", *BIS Quarterly Review*, September: 51-65.

Auer, R and S Claessens (2018b), "Regulating cryptocurrencies: Assessing market reactions, VoxEU.org, 9 October.

Bank for International Settlements (2018), *Annual Economic Report 2018*, June.

Biais, B, C Bisière, M Bouvard and C Casamatta (2017), "The blockchain folk theorem", TSE Working Papers no 17–817.

Carney, M (2018), FSB Chair's letter to G20 finance ministers and central bank Governors, 13 March.

Carstens, A (2018a), "Money in the digital age: what role for central banks?", lecture at the House of Finance, Goethe University, Frankfurt, 6 February.

Carstens, A (2018b), "Technology is no substitute for trust", Börsen-Zeitung, 23 May.

Carstens, A (2018c), "Money in a digital age: 10 thoughts", speech on 15 November.

6 It makes clear that jurisdictions should ensure that virtual asset service providers are subject to AML/CFT regulations, for example conducting, customer due diligence including ongoing monitoring, record-keeping, and reporting of suspicious transactions. It asks that all service providers in this industry – crypto exchanges, wallet providers, and providers of financial services for Initial Coin Offerings – should be licensed or registered and subject to monitoring to ensure compliance.

Committee on Payments and Market Infrastructures (2015), *Digital currencies*, November.

Financial Stability Board (2018), *Crypto-assets: report to the G20 on the work of the FSB and standard-setting bodies*.

Financial Activity Taskforce (2018), Regulation of virtual assets, FATF Recommendations, 19 October.

G20 Finance Ministers and Central Bank Governors (2018), Buenos Aires Summit communiqué, 19–20 March.

Huberman, G, J Leshno and C Moallemi (2017), "Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", Columbia Business School Research Papers no 17–92.

Landau, J-P and A Genais (2018), *Les crypto-monnaies, rapport au Ministre de l'Économie et des Finances*, 4 July.

Morris, S and H S Shin (2018), "Distributed ledger technology and large value payments: a global game approach", mimeo, Princeton University, November.

US Department of Justice (2018), "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election", 13 July.

About the authors

Raphael A. Auer is Principal Economist in the Monetary and Economic Department of the Bank for International Settlements (BIS). He is also a CEPR Research Affiliate and president of the Central Bank Research Association. Prior to joining the BIS, he was Senior Economist, Deputy Head of International Trade and Capital Flows, Economic Advisor and Member of the Directorate at the Swiss National Bank; as well as an associated research professor at the Konjunkturforschungsstelle (KOF) of the Swiss Federal Institute of Technology (ETH). During 2009-10, he was a Globalization and Governance Fellow at Princeton University. He holds a PhD in economics from MIT.

Stijn Claessens represents the BIS externally in senior groups, including the Financial Stability Board, the Basel Committee on Banking Supervision and the G20. Within the BIS, he leads policy-based analyses of financial sector issues and oversees the work of the Committee on the Global Financial System and other committee secretariats. Between 1987 and 2006, he worked at the World Bank in various positions. From 2007 to 2014, he was Assistant Director in the Research Department of the International Monetary Fund. From 2015 to early 2017, he was Senior Adviser in the Division of International Finance of the Federal Reserve Board. He holds a PhD in business economics from the Wharton School of the University of Pennsylvania and a master's degree from Erasmus University, Rotterdam. He taught at the New York University business school and the University of Amsterdam.

11 Regulating fintech: Ignore, duck type, or code

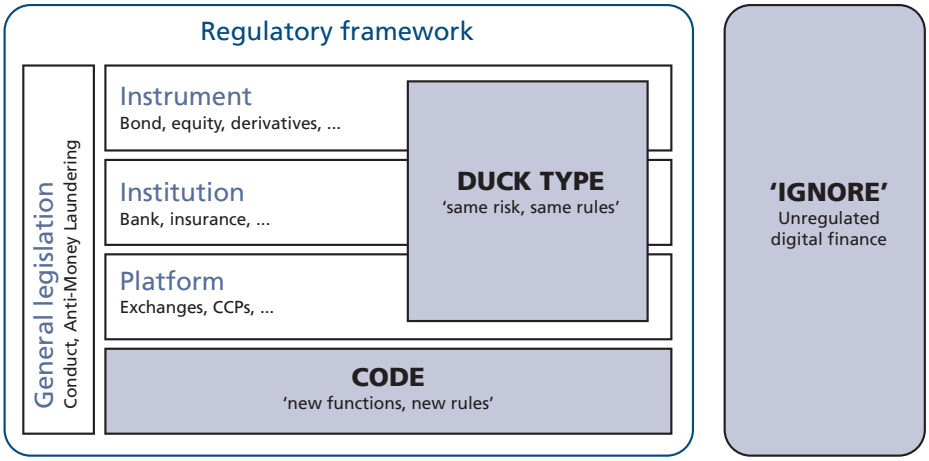
Marlene Amstad[1]
The Chinese University of Hong Kong, Shenzhen

Two events have shaped the financial system over the past ten years: the global financial crisis and the rise of the crypto-finance ecosystem, broadly labelled 'fintech'. Both of these events have raised questions about the appropriate regulatory response. The lessons learned after the crisis have been widely discussed and the regulatory response broadly agreed upon – even though it is not yet fully implemented – in the Basel III framework by the Financial Stability Board (FSB). However, the answer as to whether and how to regulate fintech is still in its early stages and is a topic of an ongoing policy debate.

In the current traditional regulatory framework, a few aspects – such as conduct and money laundering – apply to the full financial universe. However, in most aspects, the regulatory framework differs by instrument, institution, and platform (see Figure 1). Where does fintech fit into this landscape? The answer is not trivial as fintech encapsulates a broad spectrum of activities. A one-size-fits-all regulatory approach seems to risk stifling innovation and discouraging new market entrants. Accordingly, Claessens et al. (2018) focus on fintech credit and Kaal (2018) focuses on ICOs, both finding that the current regulatory responses differ widely across types of fintech activities and jurisdictions. In this chapter, I argue that despite these disparate differences regulators essentially have three options in this regard: ignore, duck type, or code (Amstad 2019).

1 Marlene Amstad serves as Vice Chair of the Board at Swiss Financial Market Supervisory Authority (FINMA). The views expressed in this chapter are those of the author and do not necessarily represent those of FINMA.

Figure 1 Regulating digital finance



Source: Amstad (2019).

Ignore — 'keep it unregulated'

The first option is to leave fintech largely unregulated. A precondition for good regulation is clarity about the need for, and goals of, regulation. The finance literature commonly gives three forms of market failure as a basis for the justification of regulation: information asymmetry, moral hazard, and monopoly power. From these elements, objectives such as investor protection, financial stability, and market integrity take shape. These likely can also provide appropriate guidance as to whether or not to regulate fintech.

In the early days of fintech, regulators in most jurisdictions chose 'wait and see'. Some fintech companies felt hampered in their activities as they could not benefit from the legal certainty of regulation – a criticism that contrasts with the sometimes anti-governmental approach of at least some fintech activities. However, implementing new regulations or even licensing may be misinterpreted as endorsement by supervisory authorities, or even as an implicit guarantee.

The aggregate market capitalisation of cryptoassets skyrocketed from $30 billion to peak at over $800 billion in early January 2018, before falling back to around $200 billion (Rauchs et al. 2018). With increased fintech-era volumes, levels of fraud,

inappropriate market practices, and Ponzi schemes increased. Hesitant to over-regulate but increasingly seeing the need for a regulatory response to ensure investor protection and market integrity, several jurisdictions resorted to issuing warnings to the market. In detailing the case of initial coin offerings (ICOs), Zetzsche et al. (2018) document the issuance of warnings as the least interventionistic of all regulatory options.

In terms of financial stability, the Committee on the Global Financial System and the Financial Stability Board, among others, concluded that at this stage, the size of fintech-era credit in many jurisdictions was still small enough to limit any systemic impact (CGFS and FSB 2017). At the same time, a range of benefits and risks were identified in cases where fintech might grow further. If regulation seems appropriate, the fundamental question arises as to whether fintech's risks and rewards can be integrated into the existing framework, or whether a new regulatory paradigm is required.

Duck type — 'same risk, same rules'

The second option is to 'duck type'[2] fintech rules into the existing regulation. Some fintech models are essentially digital or crypto representations of an instrument, an institution, or a platform. A straightforward approach to regulating these fintech models is to focus on their economic function or, more specifically, their underlying risk. This strategy refers to the famous Howey test,[3] and is often simplified as the 'duck test' that says, "if it looks like a duck, swims like a duck, and quacks like a duck, then it probably is a duck."

Duck typing regulation applies two widely used regulatory principles: it is 'principles-based' as it regulates the same risk with the same rule, and it is 'technology-neutral' as it focuses on the economic function. An example is the ICO guidelines by Swiss Financial Market Supervisory Authority: "In assessing ICOs, FINMA will focus on the economic function and purpose of the tokens (i.e., the blockchain-based units) issued by the ICO organizer" (FINMA 2018). Accordingly, ICOs are classified into payment, utility, and

2 I borrow the term 'duck typing' from computer programming.

3 It goes back to a case in the Supreme Court in 1946, which created a test that looks at an investment's substance, rather than its form, as the determining factor for whether it is a security

asset tokens. Compliance with respective existing regulations and in all cases with anti-money-laundering legislation is required. Duck-typing regulates the function rather than the instrument, institution, or platform. However, fintech innovations may also lead to new functionality. Regulators need to identify these new functions and, if need be, code them into new regulations that specifically address fintech issues.

Code – 'new functionality, new rules'

The third option is to code fintech using regulations that are specifically tailored to new functionality made possible through technological innovation.

Duck typing regulation works as long as fintech operates in the same way as traditional finance. Despite technological change, the underlying core risks in financial markets, such as market, credit, liquidity, and operational risks, have remained largely the same. However, with ongoing financial innovation, new combinations of risks might emerge. Alternatively, the core risks might show up in forms only made possible through using new technology. Both scenarios might need additional specific regulations. Similarly, new risks stemming from interconnected financial markets were brought to the forefront during the global financial crisis. While underlying risks would stay the same, it became clear that safeguarding individual financial institutions is insufficient and a separate additional macroprudential layer is necessary.

Indeed, current research suggests that fintech might lead to new functionality based, among other elements, on: (a) the specific features of blockchain technology, (b) the new combination of business models, and (c) new digital operational challenges. In the following we provide examples for each characteristic.

(a) Blockchain technology. Cong and He (2018) demonstrated that blockchains have profound economic implications on consensus generation, industrial organisation, smart contract design, and anti-trust policy. Specifically, in the traditional system – largely due to contract incompleteness – sellers cannot offer prices contingent on the success of delivering the goods. In contrast, blockchains, via decentralized consensus, enable agents to contract based on service outcomes and to automate contingent transfers. They conclude that this new functionality can deliver higher social welfare

and consumer surplus through enhanced entry and competition, yet it may also lead to greater collusion. Consequently, they suggest an oft-neglected regulatory solution to separate usage and consensus generation on blockchains, so that sellers cannot use the consensus-generating information for the purpose of sustaining collusion.

Another example for functionality made possible through blockchain is the 'fork', as an either accidental or intentional change in protocol. Biais et al. (2017) illustrated that forks might be an integral part of blockchain applications, leading to orphaned blocks and persistent divergence between chains.[4] Again, it is not straightforward to see a direct analogy to a fork in the non-digital world and therefore how to mirror it using current regulations, at least taking into consideration whether dedicated regulations are needed.

New functionality might also arise from decentralisation, which, for example, allows for greater ease in benefitting from regulatory arbitrage. Makarov and Schoar (2018) found that price movements in cryptocurrencies are largely driven not by transactions costs or differential governance risk, but rather by avoiding regulation.

(b) New combination (of business models and jurisdictions). Fintech is characterised by a strong and increasing cross-segment expansion instead of limiting itself to the value chain of a classic bank or insurance company. Rauchs et al. (2018) found that 57% of cryptoasset service providers were operating across at least two market segments to provide integrated services for their customers. This led some to declare fintech a new asset class. Findings by Hu et al. (2018) support this view, showing that cryptocurrencies are highly correlated among each other – likely driven by Bitcoin serving as vehicle currency in the cryptocurrency space – but are largely orthogonal to traditional assets. It is still too early to tell whether cryptocurrencies' distinct behaviour is a testament to the rise of a new asset class justifying its own regulation.

(c) New digital operational risks can appear across the digital financial services and market value chain. Digital technology also enables the generation and analysis of vast

4 They also show how forks can be generated by information delays and software upgrades.

amounts of customer and transaction data (i.e. 'big data'), which introduces its own set of benefits and risks that should be managed (G20 2018).

An additional need for dedicated regulation may arise from the fact that digital blockchain records must be *enforced* in the physical world. "While blockchains can keep track of transfer of ownership, proper enforcement of possession rights is still needed, except in the case of (fiat) cryptocurrencies" (Abadi and Brunnermeier 2019). The enforcement of rights and duties in fintech may differ from those found in traditional assets. Cohney et al. (2018) found, for example, that ICO codes and ICO disclosures often do not match, opening a potential need for ensuring legal certainty by regulating the link between the legal framework and the code.

Conclusion

As with previous regulation, regulating fintech needs to be justified by either investor protection, market integrity, or safeguarding financial stability. Ignore or wait-and-see approaches – at least in the beginning— can therefore be prudent approaches to avoid stifling innovation. In cases where regulation seems appropriate, however, similar activities should be treated in similar ways in an attempt to limit incentives for regulatory arbitrage. At the same time, regulators would be well-advised to remain alert to the limits of duck typing. An open dialogue among regulators, the fintech industry and academia may help to identify early on new functionalities that may require conceptually distinct regulation of technology-enabled finance.

References

Abadi, J, and M K Brunnermeier (2019), "Blockchain Economics", working paper.

Amstad, M (2019), "Regulating Fintech: Objectives, Principles and Practices", forthcoming in M Amstad, B Huang, P Morgan, and S Shirai (eds), *Fintech in Asia,* ADBI press.

Biais, B, C Bisière, M Bouvard and C Casamatta (2018), "The blockchain fork theorem", Toulouse School of Economics Working Paper No 17-817.

Committee on the Global Financial System and Financial Stability Board (CGFS and FSB) (2017), "FinTech credit: market structure, business models and financial stability implications", CGFS Papers, May.

Claessens, S, J Frost, G Turner and F Zhu (2018), "Fintech credit markets around the world: size, drivers and policy issues", *BIS Quarterly Review*, September.

Cohney, S, D Hoffman, J Sklaroff and D Wishnick (2018), "Coin-Operated Capitalism", *Columbia Law Review* (forthcoming).

Cong, W and Z He (2018), "Blockchain Disruption and Smart Contracts", *Review of Financial Studies* (forthcoming).

FINMA (2018), "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)".

G20 (2016), "High-Level Principles for Digital Financial Inclusion".

Hu, A S, C A Parlour and U Rajan (2018), "Cryptocurrencies: Stylized Facts on a New Investible Instrument", working paper.

Kaal, W (2018), "Initial Coin Offerings: The Top 25 Jurisdictions and their Comparative Regulatory Responses", working paper, University of St. Thomas School of Law.

Makarov, I and A Schoar (2018), "Trading and Arbitrage in Cryptocurrency Markets", working paper.

Rauchs, M, A Blandin, K Klein, G Pieters, M Recanatini and B Zhang (2018), "2nd Global Cryptoassets benchmarking study", Cambridge Centre for Alternative Finance, University of Cambridge.

Zetzsche, D A, R P Buckley, D W Arner and L Föhr (2018), "The ICO Gold Rush: It's a scam, it's a bubble, it's a super challenge for regulators", EBI Working Paper Series no. 18.

About the author

Marlene Amstad is Professor of Practice in Economics at the Chinese University of Hong Kong, Shenzhen and Co-Director of the Center for Financial Technology and Social Finance at the Shenzhen Finance Institute (SFI). She serves as Vice Chair of the Board of Directors at the Swiss Financial Market Supervisory Authority (FINMA) and is a fellow of the Asian Bureau of Finance and Economic Research (ABFER). She was Deputy Director at the Swiss National Bank and their Head of Investment Strategy and Financial Market Analysis, Regional Advisor at Bank for International Settlements (BIS) in Hong Kong, research fellow at the Bank of Japan and the Federal Reserve Bank of New York. She taught at University of Bern and Tsinghua University.

The explosion of cryptocurrencies such as Bitcoin, as well as an array of new technologies in financial markets (fintech), has attracted the interest of investors, financial institutions, the media as well as policymakers. The promise of radical changes has been met with excitement but also a good dose of scepticism. This eBook brings together eleven contributions from members of CEPR's Research and Policy Network on Fintech and Digital Currencies on some of the key areas where these changes are becoming more visible. The book covers four main topics.

- **Technology and governance.** Can these new technologies be compatible with the strict requirements of financial markets? Can decentralised systems replace the traditional financial market that relies on intermediaries and a central authority?
- **The economics of blockchain.** Is blockchain technology and its decentralised consensus mechanism viable in financial markets?
- **Private and public digital currencies.** Can private digital currencies such as Bitcoin compete with traditional currencies? Do digital currencies (including those issued by a central bank) make the financial system more robust and efficient?
- **Regulation of cryptocurrencies and ICOs.** How should regulation approach new assets such as cryptocurrencies and initial coin offerings (ICOs)? Should we ignore them or regulate them like traditional securities, or do we need new rules to deal with their digital nature?

Centre for Economic Policy Research
33 Great Sutton Street
London EC1V 0DX
Tel: +44 (0)20 7183 8801
Email: cepr@cepr.org www.cepr.org

ISBN 978-1-912179-18-3

CEPR Press