New Economic Windows

Paolo Tasca
Tomaso Aste
Loriana Pelizzon
Nicolas Perony *Editors*

# Banking Beyond Banks and Money

## A Guide to Banking Services in the Twenty-First Century

Springer

# Banking Beyond Banks and Money

# New Economic Windows

More information about this series at http://www.springer.com/series/6901

Paolo Tasca · Tomaso Aste
Loriana Pelizzon · Nicolas Perony
Editors

# Banking Beyond Banks and Money

## A Guide to Banking Services in the Twenty-First Century

Springer

*Editors*
Paolo Tasca
Centre for Blockchain Technologies
University College London
London
UK

Tomaso Aste
Computer Science Department
University College London
London
UK

and

Systemic Risk Centre
London School of Economics
London
UK

Loriana Pelizzon
SAFE
Goethe University Frankfurt
Frankfurt am Main
Germany

and

Department of Economics
Ca' Foscari University of Venice
Venice
Italy

Nicolas Perony
ETH Zurich
Zurich
Switzerland

and

ECUREX Research
Zurich
Switzerland

ISSN 2039-411X ISSN 2039-4128 (electronic)
New Economic Windows
ISBN 978-3-319-42446-0 ISBN 978-3-319-42448-4 (eBook)
DOI 10.1007/978-3-319-42448-4

Library of Congress Control Number: 2016946295

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

# Contents

# Introduction

**Paolo Tasca, Tomaso Aste, Loriana Pelizzon and Nicolas Perony**

**Abstract** New technologies are dramatically transforming our economic systems, and our society in general. The introduction of decentralised peer-to-peer technologies makes possible to initiate a new economy that is blurring the lines between consumers and producers, this technology shift is enabling a rapid transition towards what is known as the economy of collaborative commons: a digital space where providers and users share goods and services at a marginal cost rapidly approaching nil. In this book leading scholars, entrepreneurs, policy makers and practitioners are reporting from their different perspectives the unfolding technological revolution in banking and finance.

**Keywords** Crowdfunding • Distributed Ledger Technologies • Blockchain • P2P finance - Peer to Peer finance • e-finance • Fintech

P. Tasca (✉)
Centre for Blockchain Technologies, University College London, London, UK
e-mail: p.tasca@ucl.ac.uk

T. Aste
Computer Science Department, University College London, London, UK
e-mail: t.aste@ucl.ac.uk

T. Aste
Systemic Risk Centre, London School of Economics, London, UK

L. Pelizzon
SAFE, Goethe University Frankfurt, Frankfurt am Main, DE
e-mail: pelizzon@safe.uni-frankfurt.de

L. Pelizzon
Department of Economics, Ca' Foscari University of Venice, Venice, IT

N. Perony
ETH Zurich, Zurich, CH
e-mail: perony@ecurex.com

N. Perony
ECUREX Research, Zurich, CH

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_1

This book collects the voices of leading scholars, entrepreneurs, policy makers and consultants who, through their expertise and keen analytical skills, are best positioned to picture from various angles the unfolding technological revolution in banking and finance.

We stand on the brink of a fourth industrial revolution, which will fundamentally alter the way we live, work, and relate to one another. New technologies are dramatically transforming our economic systems, and our society in general, into something very different from what we were used to think about over the last few decades. The possibilities unlocked by billions of people collectively connected by mobile devices, with unprecedented processing power, storage capacity, and access to knowledge, are vast. The introduction of distributed ledger technologies makes possible to initiate a new economy that is blurring the lines between consumers and producers, this technology shift is enabling a rapid transition towards what is known as the economy of collaborative commons: a digital space where providers and users share goods and services at a marginal cost rapidly approaching nil (Rifkin 2014). These innovations will be further multiplied by emerging technological breakthroughs in fields such as machine learning, robotics, the Internet of Things, nanotechnology, biotechnology, materials science, energy storage and quantum computing.

In this context, traditional financial instruments, institutions and markets are rapidly becoming obsolete and inadequate to serve an increasingly globally interconnected online marketplace with an accelerating number of high-frequency transactions.

As technology progressed, the advent of the Internet era at the end of the last century opened the road to new financial services and markets. In Allen et. al 2002, the word e-finance was coined by Allen et al (2002). to include mobile and digital financial services such as online banking, Internet transactions and online trading. If, during that phase, the traditional brick-and-mortar banking model was somehow still able to keep its dominant role within the financial systems, now this position is challenged by new technology advances. The evolution, and combined use of, information communication technologies, cryptography, open source computing methods, time-stamped ledgers, and peer-to-peer distributed networks now afford end users direct, anonymous, disintermediated and secure access to assets, payments and financial services without the need to rely upon banks.

In recent years, we have started to move from e-finance to peer-to-peer (P2P) finance, defined by Tasca (2015) as: “the provision of financial services and markets directly by end users to end users using technology-enabled platforms supported by computer-based and network-based information and communication technologies”. The term P2P finance encompasses cryptocurrencies and blockchain-based financial applications, decentralised markets for lending, crowdfunding and other financial services, digital assets and wallets.

These technologies are fragmenting and dismantling some of the major banking services: Lending, deposits, security, advisory services, investments, payments and currencies. These financial services, that were traditionally procured under one roof with a single point of control, can now be offered by decentralised platforms with limited or absent human interaction—one of the prerequisites and founding pillars of the brick-and-mortar banking model.

P2P finance is a new form of banking beyond banks and money, emerging as a consequence of the ongoing FinTech revolution characterized by a finance-focused trend of technology start-ups and corporations primarily focused on peripheral industries but increasingly interested in finance. A legion of technology companies in San Francisco, New York City, London, and elsewhere seized the opportunity offered by the dissatisfaction of banking customers and are now creating financial products and services that are beyond the capacity of banks to replicate. This new contingent of FinTech companies are not only capturing revenues that were traditionally banking profits (e.g., in payments or lending), but also experimenting with new data-led revenue streams for banking.

At the same time, although banks find it difficult to innovate mostly due of the burden of their legacy infrastructures, the traditional banking industry benefits from many years of experience with a large number of detailed regulations and operational procedures, providing the means to operate safely. No such framework currently exists for P2P finance which is a bottom-up phenomenon, based on fast-evolving technological advances. P2P finance is shifting the power from the traditional stakeholders to the end users, and the citizens in general, and creating new opportunities for entrepreneurs; in doing so it also introduces new risks and challenges for legal systems and risk management practices.

Similarly, in the twenty-first century we need the same banking services of the twentieth century, but the way we expect them to be delivered to us has dramatically changed, as we now leave in the digital age global communication and information sharing. In the first decade of the twenty-first century only, people connected to the Internet worldwide increased from 350 million to over 2.5 billion. The use of mobile phones increased from 750 million to over 6 billion. By 2025, if the current pace of technological innovation is maintained, most of the projected 8 billion people on Earth will be online (Schmidt and Cohen 2013). As long as the connectivity will continue to increase and become more affordable, by extending the online experience to places where people today don't even have landline phones, we envision a landscape where P2P finance will continue to invade and disrupt the financial mainstream. New forms of financial (dis)intermediations, new ubiquitous accesses to services and decentralised markets will emerge, which will fill gaps, create value and progressively substitute the traditional banking system.

This book constitutes a unique perspective on this technological and social revolution, as it is written by the people who are driving it. By presenting an overview of the new banking and money transfer models and, at the same time, addressing their challenges and threats, this collection of essays is meant to offer a guideline for the providers and the consumers of banking services in the twenty-first century.

## References

Allen, F., Andrews, J.M., Strahan, P.: E-finance: an introduction. J. Financ. Serv. Res. **22**(1–2), 5–27 (2002)

Rifkin, J.: The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism. Macmillan (2014)

Schmidt, E., Cohen, J.: The New Digital Age: Reshaping the Future of People, Nations and Business. Hachette, UK (2013)

Tasca, P.: Digital Currencies: Principles, Trends, Opportunities, and Risks. ECUREX Research WP, 7 Sept 2015

# Classification of Crowdfunding in the Financial System

**Loriana Pelizzon, Max Riedel and Paolo Tasca**

**Abstract** The emergence of crowdfunding has attracted attention from borrowers, investors, banks and regulators alike. This chapter reviews its historical development, distinguishes between different business models, and discusses its disruptive potential and future growth prospects. Focusing mainly on lending- and equity-based crowdfunding, it further presents insights related to participants' behavior on crowdfunding platforms and regulatory advancements in different countries.

**Keywords** Crowdfunding regulation · Equity-based crowdfunding · Peer-to-peer lending

## 1 Emergence of Social Financing in the Digital Age

Digital technology has become a prerequisite for, and a constant companion of, new developments in our daily life and business activity. Internet, information communications technologies, data-driven technologies, modern analytical methods and virtual infrastructures penetrate into the daily life of every single household by changing consumer and investment behavior worldwide. Nowadays, anyone with access to the Internet can participate interactively in digital spaces. Flexible and varied relationships are formed between people and their diverse identities, both in the online and offline worlds. We are already living in the so-called economy of Collaborative Commons characterized by the prevalence of sharing over ownership. This major structural

L. Pelizzon · M. Riedel (✉)
Research Center SAFE, Johann Wolfgang Goethe-University, House of Finance,
Theodor-W.-Adorno Platz 3, 60323 Frankfurt am Main, Germany
e-mail: riedel@safe.uni-frankfurt.de

L. Pelizzon
e-mail: pelizzon@safe.uni-frankfurt.de

P. Tasca
Centre for Blockchain Technologies, University College London, London, UK
e-mail: p.tasca@ucl.ac.uk

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_2

change mainly applies to products and services that can be easily standardized and automated, similar to the broad spectrum of services offered by traditional banks.

The rapid development from the early days of the Internet in the 90s to its current advancement towards the Internet of Things[1] is partly attributable to the emergence of the so-called Web 2.0. The term Web 2.0 was coined soon after the launch of the worldwide first crowdfunding platform ArtistShare in the US in 2003 and about one year before the pioneering peer-to-peer (P2P) lending platform Zopa was founded in the United Kingdom in 2005. The year 2004 became a turning point for Internet users. Being largely consumers of content in the 'old Web', users transformed into content creators. User interactivity, collaboration and the resulting content creation were the main characteristics of Web 2.0. As documented by Schwienbacher and Larralde (2010), Web 2.0 especially broadened the capabilities of small firms by allowing users' content to inflow and create value for the company. This technological advancement enabled the first P2P platforms to utilize the emerging momentum and popularity of various online social networks, while especially lending platforms took the simplicity and efficiency of credit scores to their advantage and managed to deal with loan applications at a speed that is close to real time.

The novel financing segment for consumers and small businesses grew from a niche to a sizeable market not until the 2008 Financial crisis. Many households, hit by huge financial pain, lost trust and confidence in the traditional banking sector (Gritten 2011) and withdrew from financial markets while looking for alternative sources to obtaining funds. Banks reduced their lending activity and capital stopped flowing from those who had it to those who were able to use it to grow businesses and create jobs, thus, prolonging the Great Recession. At the dawn of the emergency program loans and public bail outs, the reputation of the bankers was already significantly undermined in most of the western countries and their traditional role as credit providers has been criticized and put under spotlight of the public opinion, (Rose 2010; Stiglitz 2010). The post-crisis period was characterized by a low-yield environment such that investors became creative in identifying alternative investments and allocating their funds in new financial products.

Under this general context, the focus of both capital holders and capital seekers turned to alternative market infrastructures that were able to provide direct, disintermediated credit-lending relationships for households and businesses without the need of a single point of control (or failure).

## 2 The Many Facets of Crowdfunding

Crowdfunding refers to the process of acquiring capital for a project by collecting relatively small amounts from many investors or backers. It represents a more specific form of the more general term crowdsourcing, which is the acquisition of

[1] The Internet of Things describes the a concept where physical devices are connected to the Internet and are able to identify themselves and exchange data.

any resource (services, creative content, funds, etc.) from a large group that is typically online. The term crowdfunding was first coined in 2006 by Michael Sullivan on Fundavlog, his video blogging project.

The actors associated with crowdfunding fall into three main roles: (i) the borrower or project initiator who presents her credit request or idea/project to be funded; (ii) individuals or groups (i.e., the crowd) who support the funding request; and (iii) a moderating organization (i.e., the platform) that brings the parties together to launch the idea or support the borrowing request.

The literature distinguishes between (i) lending-based crowdfunding, which consists of loans which are repaid with interest, (ii) equity-based crowdfunding in which investors receive shares of the startup company, (iii) reward-based crowdfunding that involves rewarding funders with a product that has actual monetary value, often an early version of the product or service being funded, and (iv) donation-based crowdfunding in which backers donate funds because they believe in the cause (Cholakova and Clarysse 2015).

As pointed out by Everett (2008), lending-based crowdfunding is a technology-enabled form of social lending. Indeed, the advent of modern social lending is attributed to the English Friendly Societies of the 18th and 19th century that arose spontaneously during the Industrial Revolution as clubs that helped their members pool resources and risk. The Friendly Societies allowed members to make deposits and receive loans, and also assisted family members in the case of negative shocks such as illness. What was a locally bounded phenomenon in the past has become nowadays a spatially unbounded opportunity to connect with socially inclined or profit oriented, mostly anonymous, individuals. Besides, one of the biggest challenges, accurate risk assessment, was facilitated with technological advances. Friendly Societies had little experience in risk management and about one third of them had failed in the 19th century (Covello and Mumpower 1986). An online platform, on the other hand, is not exposed to idiosyncratic risk of its borrowers per se but it provides the necessary tools to investors for controlling their risk exposure by (a) collecting, scoring, and disseminating credit qualifications for a pool of prospective borrowers, (b) the real-time reporting supply of lending bids, allowing investors to diversify across loans and spreading borrower risk across investors, and (c) the online servicing, monitoring, and credit history reporting of loan performance.

The equity-based model is a valuable alternative source of funding for entrepreneurs as the crowd takes the role of traditional investors in startups, such as business angels and venture capitalists. The project initiatives involve equity shares, revenue, or profit sharing with the funders.

In contrast to lending- and equity-based crowdfunding, the donation- and reward-based models do not guarantee a payoff to funders. Projects of this kind tend to raise smaller amounts of capital than those with equity participation. Still, both models experienced high popularity among backers. This might seem unreasonable since financial reward is practically non-existent and one might assume that project initiators depend solely on the goodwill of potential backers. This is not necessarily true as pointed out by Schwartz (2015). Funders can be incentivised to donate by experiencing a non-financial value while doing so. Their intrinsic motivation might be driven by factors such as personal entertainment, political expression, arts patronage, altruism, being part of a community, or having a feeling of being a creator.

Despite the growing popularity of the latter two models, it is mostly P2P lending and equity-based crowdfunding that pose a potential threat to the business models of traditional financial institutions. Consequently, the focus of this survey lies especially on these two models.

## 3 Evidence of Positive Disruption to Traditional Financing

How does crowdfunding relate to the financial system? Is it complementary or disruptive? In order to answer these questions it is advisable to consider first the size of this market.

In 2015, more than 400 crowdfunding platforms were operating in more than 35 countries and more than 100 social lending platforms were running business in 25 countries. To give a dimension of the market, one should know that in 2009 the crowdfunding volume was about USD 530 million worldwide. Almost doubling every year, it reached USD 16.2 billion by the end of 2014,[2] while growth projections for the year 2020 suggest an increase to USD 150–490 billion worldwide.[3]

In the United States, the top five P2P lending platforms originated USD 3.5 billion in loans in 2013, up from USD 1.2 billion in 2012.[4] As a comparison, households in the United States had around USD 858 billion in credit card debt outstanding as of December 2013, reflecting net new borrowing of USD 12.3 billion over the prior 12 months. Under the assumption that the USD 12.3 billion figure is a rough estimate of the growth in securitized consumer lending, this suggests that a relevant share of consumer lending net growth could be captured by P2P lending.

The effects of the growing alternative financing markets on the traditional financial system were not investigated yet. Classical economic literature, though, suggests that an increase in competition, in general, improves consumers' welfare because it minimizes deadweight loss. In fact, Fraiberger and Sundararajan (2015) show that sharing economies improve overall welfare benefits. A more crowdfunding-related study was done by Agrawal et al. (2011). They observe that online platforms eliminate economic frictions related to spacial distance, enhancing credit supply to artists.

[2] Source: Crowdsourcing.org; Massolution.

[3] Source: Morgan Stanley Research.

[4] Source: Fitch Ratings. https://www.fitchratings.com/gws/en/fitchwire/fitchwirearticle/P2P-Lending's-Success?pr_id=851174.

Theoretical and empirical results show that traditional banks have little incentive for screening small borrowers and practically they invest little effort in doing this. Iyer et al. (2010) find that the screening process in P2P markets incorporates 'soft', i.e. non-standard, information. They point out that lenders are able to infer one-third of the information regarding borrowers' credit score by utilizing such information benefiting in particular small borrowers. Since traditional lenders use only 'hard', standard information on estimating creditworthiness, they argue that Prosper, a lending platform in the US, acts like a complementary lending institution that improves small borrowers' overall credit access. On the negative side, not all lenders have financial and screening expertise giving a comparative advantage to institutional investors over individual investors in selecting profitable loans. Butler et al. (2010) reports that borrowers with relatively better access to traditional bank financing are willing to borrow at a lower rate at Prosper. This suggests that P2P markets add to overall credit supply efficiency.

Morse (2015) points out that the main driver of the crowdfunding disrupting force is the increasing role of big data. Data analysis has become a crucial part in business relations and an integral component of social network businesses. Despite the fact that big data brings forth also all sorts of uncertainties such as privacy, monopoly power, or discrimination, P2P platforms might be able to offer pricing and access benefits to potential borrowers if they manage to unearth soft information not accessed or used by intermediated finance.

By considering all the above elements, if asked whether crowdfunding has the possibility to positively disrupt consumer finance, it seems that this is potentially the case. Due to the complexity of some businesses (e.g., collateralized loans requiring repossessions and foreclosures, and long maturity lending without forcing mechanisms), this will probably be not the case across all markets.

## 4 Insights on Social Behavior in P2P Lending Markets

P2P markets provide an academically interesting setting where social interaction, investment and borrowing decisions can be studied simultaneously. The following survey will provide an overview of recent behavioral and financial insights.

One string of literature focuses on identifying statistical as opposed to taste-based discrimination in P2P markets. The former occurs when distinctions between demographic groups are made on the grounds of real or imagined statistical distinctions between the groups. The latter takes place when agents' personal prejudices or tastes against associating with members of a particular group affect their treatment of those individuals (Becker 1971). Pope and Sydnor (2011) observe racial discrimination through borrower pictures on Prosper. In particular, pictures of the black, the elderly and people with an unhappy facial expression are significantly discriminated against in terms of loan funding and high interest rates. Ravina (2008) observes that personal characteristics significantly affect the probability of having a loan funded. Beautiful borrowers are favored while black borrowers are relatively less likely to get a loan as opposed to white. They conclude that the way borrowers present themselves affects the likelihood of getting a loan and more favorable loan terms. Overall, beauty seems to be related to taste-based discrimination while blacks are subjected to statistical discrimination.

Successful loan funding also appears to be related to various signals of trustworthiness. Duarte et al. (2012) finds that borrowers who appear to be more trustworthy have a higher likelihood of getting loan and being charged a relatively lower interest rate. However, trustworthy-looking borrowers, in fact, default at a lower rate and have a relatively better credit rating. Freedman and Jin (2014) observe that also having a social network is beneficial for borrowers as it increases the probability of being funded and lowers the interest rate on the loan. According to Hildebrand et al. (2010), group leaders, who are rewarded for successful loan listings, have an incentive to signal borrower quality to lenders. This alleviates information asymmetries that can be mitigated if group leaders invest a substantial amount in the loans themselves.

Studies show that some investors do not process all available information optimally. Gelman (2013) finds that small investors, in particular, ignore valuable borrower information that is conveyed in a borrower's loan verification status on Lending Club. Thus, such investors show risk seeking behavior while professional investors act more rationally and in a more risk averse manner. Furthermore, Freedman and Jin (2014) find that lenders on Prosper do not understand the relation between social ties and unobserved borrower quality. Some borrowers use their social network to their advantage of getting the best deal. Lenders learn about such gaming behavior from their investment mistakes only gradually over time and adjust slowly. Contrary to this finding, Lin et al. (2009) observes that friendships of borrowers signal credit quality to lenders.

Mach et al. (2014) show that small business applications are more than twice as likely to be funded than other loans. Berger and Gleisner (2014) observe that market participants who were paid to act as intermediaries on Prosper and screen loan listings had a positive impact on lowering borrowers' credit spreads by reducing information asymmetries.

There is also presence of herding behavior among lenders. Zhang and Liu (2012), Herzenstein et al. (2011) and Ceyhan et al. (2011) observe that bids for a single loan do not occur uniformly over time. In particular, bids are concentrated at the end of a listing's lifetime and tend to be more concentrated for listings that are close to being fully funded.

From a more theoretical perspective, Paravisini et al. (2009) estimate investors' risk preference parameters and their elasticity to wealth. They find that wealthier investors exhibit lower absolute risk aversion and higher relative risk aversion and that for a given investor, the relative risk aversion increases after experiencing a negative wealth shock.

To sum up, despite some inefficiencies observed by researchers, P2P lending markets overall positively affect credit supply to individuals.

## 5 Recent Developments in Equity-Based Crowdfunding

Equity crowdfunding is a mechanism that enables individuals to collectively invest in startup companies and small businesses in return for equity.[5] In terms of funding volume, equity crowdfunding is a relatively small category. During the last years it counted only for about the 5 % of the total funds channeled via crowdfunding platforms (Wilson and Testoni 2014). The reason behind this low level lies in the fact that equity crowdfunding is heavily penalized by different legislative approaches that in general tend to protect investors from its high risk profile. Some significant evidence is that, although the US lead the overall crowdfunding, when it comes to the equity-based market, it is Europe who holds the leading position thanks to its accommodating policy environment. But the situation in US might improve because of the recent approval of Title III of the JOBS Act in 2015. In practice, this law will unlock the possibility for every US citizen to invest in equity crowdfunding. This could indeed represent a sizable positive shock for the US market.

*Difference* Compared with other types of crowdfunding, equity crowdfunding exhibits some unique characteristics along with peculiar investment attitudes. Ahlers et al. (2015) compare four types of crowdfunding (donation-based, reward-based, lending-based and equity-based) by positioning them in a two dimensional map where, on one side is the level of complexity (legislation and information asymmetries) and on the other side is the level of uncertainty. With no doubt, equity crowdfunding reaches the highest level along both dimensions. Accordingly, investors of equity crowdfunding are the least risk averse. From an incentive point of view, the investors in equity crowdfunding tend to pursue a long-term monetary return. In terms of funding scale, equity crowdfunding is in general smaller than private equity, venture capital and even angel investments. This characteristic makes equity crowdfunding a proper instrument that is able to fill the ‘equity gap’ for early stage projects. Traditionally, small businesses in seed funding raise funds from the three ‘f’ (friends, family and fools). However, friends and family financing is often an insufficient source of funds and in order to achieve scale, larger sources of risk capital are often required. During the recent years, business angels and venture capitalists—the traditional sources of risk capital after the three ‘f’, have increasingly been moving their investment activity upstream, making larger investments into more developed companies (Collins and Pierrakis 2012). To have a sense of the dimension, according to Wilson and Testoni (2014), most of the equity-based projects raise an amount of funds ranging between USD 50,000 and USD 100,000. Instead, many angels tend to consider only businesses that are looking to raise amounts larger than USD 100,000.

[5] Financial Conduct Authority (2016, April 6). The FCA’s regulatory approach to crowdfunding over the internet, and the promotion of non-readily realisable securities by other media. Retrieved from http://www.fca.org.uk/static/documents/policy-statements/ps14-04.pdf.

*Funding* From the funding side there are many factors that could influence the performance of equity crowdfunding. Compared to venture capital funding, which is lead by professional experts, the influential factors of equity crowdfunding could be detrimental when funding decisions are taken by small investors without a strong financial background. An empirical examination in this field is applied by Ahlers et al. (2015). After having investigated 104 equity crowdfunding offerings published on ASSOB (one of the largest equity-based crowdfunding platform), the authors present several key factors that could lead to an investment bias. Namely, factors that are not necessarily linked to performance but that are instead perceived as such by the investors: the quantity of the board members, the levels of members, education, their professional network, the clarification for the exit scenario (IPO, or trade sale) and the time that the firm has been in the business (experience).

*Investment* As for as investment is concerned, the valuation of a startup is the great challenge, especially when it comes to small investors. In donation-based crowdfunding, the pricing problem does not exist at all, as the motivation for donation is not based on financial return. For lending-based crowdfunding, investors could receive their interest periodically, thus the pricing model could at least refer to Discounted Cash Flow techniques. But when it comes to equity crowdfunding, there does not exist an unassailable text-book model. Usually, the valuation could be either based on the asset value, on the expected cash flow (or return) or a mix of both. In terms of asset valuation, for startups in early-stage, the most important asset is probably the intellectual property, which is intangible and therefore subjected to an arbitrary valuation. On the other hand, the forthcoming expected return could also be of great uncertainty. Indeed, it is very common to happen that no cash flow is generated in the first 5–7 years for a seed or early-stage company. If any, it would anyway be reinvested into the business again. So, investors generally do not have a sufficient set of track-records to use in order to extrapolate future cash flows or returns on investment (Wilson and Testoni 2014). And due to information asymmetries, entrepreneurs and investors probably have a different view on equity pricing because they have a different information set. In fact, the information asymmetry problem is hardly avoided especially for startups still in their seed stage. There exists a tension in equity crowdfunding (but not only) as entrepreneurs have to bear the risk to disclose more business details to the crowd but at the same time they need to protect their ideas and business strategies that could be copied easily by other companies. In this field Innovestment, a German crowdfunding platform, provides an innovative solution. In Innovestment, pricing of equity is based on auction. Investors bid for the equity of a startup according to their own internal valuation and entrepreneurs can at the end decide whether to accept or refuse the funding amount.

*Regulations* Investment in seed-stage companies is essentially a high-risk activity because, as presented above, it deserves some level of competence. Indeed, according to Zhang et al. (2014), the majority of investors are professionals or high-net-worth individuals. Thus, governments tend to be very cautious with regard to regulation of retail equity crowdfunding. Although still in evolution, in the following, we briefly present the status of the legislation for some of the biggest crowdfunding markets. In the US, for a long time equity-based crowdfunding has only been opened to accredited investors. According to the Security and Exchange Commission an accredited investor, in the context of a natural person, includes anyone who earned income in excess of USD 200,000 in each of the prior two years, or has a net worth over USD 1 million. This restriction is expected to be lifted up soon. However, in October 2015, the SEC approved the Title III of the JOBS Act, which will allow non-accredited investors to invest in equity-based crowdfunding. When the rules will come into effect, the US equity crowdfunding market will be open to all citizens. Also in UK, equity crowdfunding is considered a risky investment. It is fully monitored and regulated by the Financial Conduct Authority which considers any share in equity-based crowdfunding as a non-readily realizable security. In general, the market is only open to some qualified investors whose wealth or income has surpassed a certain pre-defined standard. According to a rule approved in 2014, retail investors and normal citizens must explicitly confirm that they will not invest more than 10 % of their net investable assets in equity crowdfunding products. In other EU countries, the investment environment is relatively loose. In July 2013, Italy, became the first country in Europe to implement a complete retail equity crowdfunding regulation. After few months, in reviewing existing rules, Italy enlarged the category of suitable crowdfunding target companies. Now, it is no longer limited only to startups but it is extended and applied to a broader definition, provided that crowdfunding companies are innovating and launching new products. In Germany equity crowdfunding has been legal for years but only limited to silent partnership, which means investors could only share the profit but have no voting rights. In France, equity crowdfunding is also allowed but the regulation places some constraints. For example, crowdfunding platforms need to maintain a minimum capital requirement of EUR 730,000.

Looking at the past, it becomes clear that regulators are willing to facilitate the flow of capital between market participants. However, most countries are still in the ongoing process of defining an appropriate legal framework for the crowdfunding segment.

## References

Agrawal, A., Catalini, C., Goldfarb, A.: Friends, family, and the at world: the geography of crowdfunding. Working paper, University of Toronto, Toronto (2011)

Ahlers, G.K.C., Cumming, D.J., Guenther, C., Schweizer, D.: Signaling in equity crowdfunding. Entrepreneurship Theory Pract. **39**(4), 955–980 (2015)

Becker, G. (1971): The economics of discrimination. Chicago [usw.] The Univ. of Chicago Pr., 2. ed. edn

Berger, S.C., Gleisner, F.: Emergence of financial intermediaries in electronic markets: the case of online P2P lending. BuR-Bus. Res. **2**(1), 39–65 (2014)

Butler, A.W., Cornaggia, J., Gurun, U.G.: Do Local Capital Market Conditions Affect Consumers' Borrowing Decisions? Social Science Research Network Working Paper Series (2010)

Ceyhan, S., Shi, X., Leskovec, J.: Dynamics of bidding in a P2P lending service: effects of herding and predicting loan success. In: Proceedings of the 20th International Conference on World Wide Web, WWW ‘11, pp. 547–556, New York, NY, USA. ACM (2011)

Cholakova, M., Clarysse, B.: Does the possibility to make equity investments in crowdfunding projects crowd out reward-based investments? Entrepreneurship Theory Pract. **39**(1), 145–172 (2015)

Collins, L., Pierrakis, Y.: The venture crowd: crowdfunding equity investments into business. NESTA (2012)

Covello, V.T., Mumpower, J.: Risk Evaluation and Managementchap. Risk Analysis and Risk Management, pp. 519–540. Springer US, Boston, MA (1986)

Duarte, J., Siegel, S., Young, L.: Trust and credit: the role of appearance in peer-to-peer lending. Rev. Financ. Stud. **25**(8), 2455–2484 (2012)

Everett, C.R.: Group Membership, Relationship Banking and Loan Default Risk: The Case of Online Social Lending. Social Science Research Network Working Paper Series (2008)

Fraiberger, S.P., Sundararajan, A.: Peer-to-Peer Rental Markets in the Sharing Economy. Social Science Research Network Working Paper Series (2015)

Freedman, S., Jin, G.Z.: The Information Value of Online Social Networks: Lessons from Peer-to-Peer Lending. Working Paper 19820, National Bureau of Economic Research (2014)

Gelman, I.A.: Show Us Your Pay Stub: Income Verification in P2P Lending. Social Science Research Network Working Paper Series (2013)

Gritten, A.: New insights into consumer confidence in financial services. Int. J. Bank Mark. **29**(2), 90–106 (2011)

Herzenstein, M., Dholakia, U.M., Andrews, R.L.: Strategic herding behavior in peer-to-peer loan auctions. J. Interact. Mark. **25**(1), 27–36 (2011)

Hildebrand, T., Puri, M., Rocholl, J.: Skin in the Game: Evidence from the Online Social Lending Market. Working paper, Duke University (2010)

Iyer, R., Khwaja, A.I., Luttmer, E.F.P., Shue, K.: Screening in New Credit Markets: Can Individual Lenders Infer Borrower Creditworthiness in Peer-to-Peer Lending?. Social Science Research Network Working Paper Series (2010)

Lin, M., Prabhala, N., Viswanathan, S.: Judging Borrowers by the Company They Keep: Friendship Networks and Information Asymmetry in Online Peer-to-Peer Lending. Social Science Research Network Working Paper Series (2009)

Mach, T., Carter, C., Slattery, C.R.: Peer-to-Peer Lending to Small Businesses. Social Science Research Network Working Paper Series (2014)

Morse, A.: Peer-to-Peer Crowdfunding: Information and the Potential for Disruption in Consumer Lending. Social Science Research Network Working Paper Series (2015)

Paravisini, D., Rappoport, V., Ravina, E.: Risk Aversion and Wealth: Evidence from Person-to-Person Lending Portfolios. Social Science Research Network Working Paper Series (2009)

Pope, D.G., Sydnor, J.R.: What’s in a picture?: Evidence of discrimination from Prosper.com. J. Human Resour. **46**(1), 53–92 (2011)

Ravina, E.: Love & Loans: The Effect of Beauty and Personal Characteristics in Credit Markets. Social Science Research Network Working Paper Series (2008)

Rose, M.H.: A Failure of Capitalism: The Crisis of ‘08 and the Descent into Depression. By Richard A. Posner. Cambridge: Harvard University Press, 2009. xviii + 346 pp. Index. Cloth, $23.95. ISBN: 9780674035140., Business History Review, 84, 137–139 (2010)

Schwartz, A.A.: The Nonfinancial Returns of Crowdfunding. Social Science Research Network Working Paper Series (2015)

Schwienbacher, A., Larralde, B.: Crowdfunding of Small Entrepreneurial Ventures. Social Science Research Network Working Paper Series (2010)

Stiglitz, J.E.: FREEFALL: America, Free Markets and the Sinking of the World Economy. WW Norton & Company (2010)

Wilson, K.E., Testoni, M.: Improving the Role of Equity Crowdfunding in Europe's Capital Markets. Social Science Research Network Working Paper Series (2014)

Zhang, J., Liu, P.: Rational herding in microloan markets. Manage. Sci. **58**(5), 892–912 (2012)

Zhang, Z., Collins, L., Baeck, P.: Understanding Alternative Finance—The UK Alternative Finance industry Report 2014. NESTA (2014)

## Author Biographies

**Loriana Pelizzon** is the Program Director of the Research Centre SAFE Systemic Risk Lab and SAFE Full Professor at Goethe University Frankfurt, Chair of Law and Finance, part-time Full Professor of Economics at the Ca' Foscari University of Venice and Research Affiliate at MIT Sloan. She graduated from the London Business School with a doctorate in Finance. She was Assistant Professor in Economics at the University of Padova from 2000 till 2004 and recently Visiting Associate Professor at MIT Sloan and NYU Stern. Her research interests are on risk measurement and management, asset allocation and household portfolios, hedge funds, financial institutions, systemic risk and financial crisis. Pelizzon has been awarded the EFA 2005 - Barclays Global Investor Award for the Best Symposium paper, FMA 2005 European Conference for the best conference paper and the Award for the Most Significant Paper published in the Journal of Financial Intermediation 2008. She teaches Systemic Risk and Sovereign Risk PhD courses at GSEFM and Money and Banking at the undergraduate program. She has been awarded the Best Teacher in 2007 and 2008 at the Ca' Foscari University of Venice. She was one of the coordinators of the European Finance Association (EFA) Doctoral Tutorial, member of the EFA Executive Committee and member of the BSI GAMMA Foundation Board. She has been involved in NBER and FDIC projects as well as EU, Europlace and Inquire Europe, EIEF, Bank of France projects and VolkswagenStifftung Europe and Global Challenges. From March 2016 she is a member of the EIOPA's Insurance and Reinsurance Stakeholder Group, Member of the EU independent expert advice team in the field of Banking Union and external Expert for the EU commission on digital currency and blockchain technology. She frequently advises banks, pension funds and government agencies on risk measurement and management strategies.

**Max Riedel** is a Ph.D. student and currently employed as a research assistant the Goethe University Frankfurt. He has been working in the quantitative portfolio management department of a fund management company based in Frankfurt. Max Riedel studied Business & Economics and Mathematics at the Goethe University. His research interests are asset pricing, banking and financial markets.

**Paolo Tasca** is a FinTech economist specialising in P2P Financial System. An advisor for different international organisations including the EU Parliament on blockchain technologies, Paolo recently joined the University College London as Director of the Centre for Blockchain Technologies. Prior to that, he has been a senior research economist at Deutsche Bundesbank working on digital currencies and P2P lending. Paolo is the co-author of the bestseller "FINTECH Book" and the co-editor of the book "Banking Beyond Banks and Money". He holds an M. A in Politics and Economics (summa cum laude) from the University of Padua and a M.Sc. in Economics and Finance from Ca' Foscari, Venice. He did his PhD studies in Business between Ca' Foscari Venice and ETH, Zürich. Other current appointments: Research Fellow at CFS, Goethe University, Research Associate at the Systemic Risk Centre of the London School of Economics, Research Associate of the Institut de Recherche Interdisciplinaire Internet et Société and Senior Advisor of the Beihang Blockchain & Digital Society Laboratory in Beijing.

# Crowdfunding and Bank Stress

**Daniel Blaseg and Michael Koetter**

**Abstract** Bank instability may induce borrowers to use crowdfunding as a source of external finance. A range of stress indicators help identify banks with potential credit supply constraints, which then can be linked to a unique, manually constructed sample of 157 new ventures seeking equity crowdfunding, for comparison with 200 ventures that do not use crowdfunding. The sample comprises projects from all major German equity crowdfunding platforms since 2011, augmented with controls for venture, manager, and bank characteristics. Crowdfunding is significantly more likely for new ventures that interact with stressed banks. Innovative funding sources are thus particularly relevant in times of stress among conventional financiers. But crowdfunded ventures are generally also more opaque and risky than new ventures that do not use crowdfunding.

**Keywords** Crowdfunding • Bank stress • Funding alternative • New ventures • Credit crunch

## 1 Introduction

Akerlof's (1970) seminal lemons problem epitomizes the key challenge faced by any investor: how to select projects from a pool of opaque applicants. Traditionally, banks help resolve the information asymmetry between savers and investors by developing screening competences and acting as delegated monitors (Diamond 1984). But dramatically reduced transaction and information acquisition costs, together with historically low interest rates, impede banks' incentives to engage in

D. Blaseg
Goethe-University Frankfurt, Theodor-W.-Adorno-Platz 4, 60323 Frankfurt, Germany
e-mail: blaseg@wiwi.uni-frankfurt.de

M. Koetter (✉)
Frankfurt School of Finance and Management, Deutsche Bundesbank,
and IWH, Sonnemannstr. 9-11, 60314 Frankfurt, Germany
e-mail: m.koetter@fs.de

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_3

costly information generation, which can lead to the contraction of credit (Puri et al. 2011; Jiménez et al. 2012) or misallocated funding to too risky projects (Dell'Ariccia and Marquez 2004; Jiménez et al. 2014). Against this backdrop, recent studies by Belleflamme et al. (2013) and Mollick (2014) hypothesize that crowdfunding may rival bank finance and connect even small savers with risky new ventures that face traditionally tighter financing constraints (e.g., Cassar 2004; Robb and Robinson 2014).

We test whether the wisdom-of-the-(investor)crowd becomes a more likely substitute for bank credit as a major source of funding for new ventures if young ventures' banks are shocked. We construct a novel, hand-collected data set of ventures' uses of equity crowdfunding in Germany, their relationships with banks, and various venture traits since 2011. By observing venture-bank relationships, we can identify if ventures connected to shocked banks are more likely to use crowdfunding in an attempt to substitute for contracting bank credit supply. In so doing, we move beyond the important descriptive evidence in this nascent strand of literature, which does not permit inferences about the causal effects of the determinants of crowdfunding.[1]

We also control for observable management and venture traits to determine if more opaque ventures with greater information asymmetries are more likely to use crowdfunding as an alternative source of financing. Greater information asymmetries increase capital costs, which implies a well-known pecking order of capital structure: Internal funds are preferred over debt, and equity is a last resort of funding (Jensen and Meckling 1976; Myers and Majluf 1984). To mitigate information asymmetries and facilitate the efficient allocation of financial resources, from savers to productive investors, financial intermediaries can generate private information by establishing close and long-term relationships (Rajan 1992; Uchida et al. 2012). But relationship lending is costly, so banks may turn down funding requests by promising, yet hard-to-assess projects such as new ventures if they cannot confidently cover the costs associated with producing necessary private information (Rajan 1992; Petersen and Rajan 1994, 2002). In this setting, we investigate if ventures tied to banks that struggle to cover the costs of private information generation are more likely to tap a potentially less-than-wise crowd as a funding source.

The financial crisis of 2008 amplified the generally prevalent challenges that young and small ventures confront when trying to raise external finance. In the aftermath of the great financial crisis, the number and volume of equity financing rounds from venture capital sources declined significantly (Block et al. 2010), credit supply tightened in the Eurozone (Hempell and Kok 2010), and in Germany, even local lenders reduced their loans (Puri et al. 2011). Gorman and Sahlman (1989) and Cassar (2004) caution that credit supply shocks are especially important for new ventures. However, most existing empirical evidence is geared toward venture capitalist

[1] Recent policy (e.g., De Buysere et al. 2014), and academic (e.g., Mollick 2014; Schwienbacher 2013; Hornuf and Schwienbacher 2014), light on the potential role of crowdfunding and vividly illustrate the broadening interest in this new form of financing ventures. We instead seek to provide empirical evidence about the causal effects of bank credit crunches.

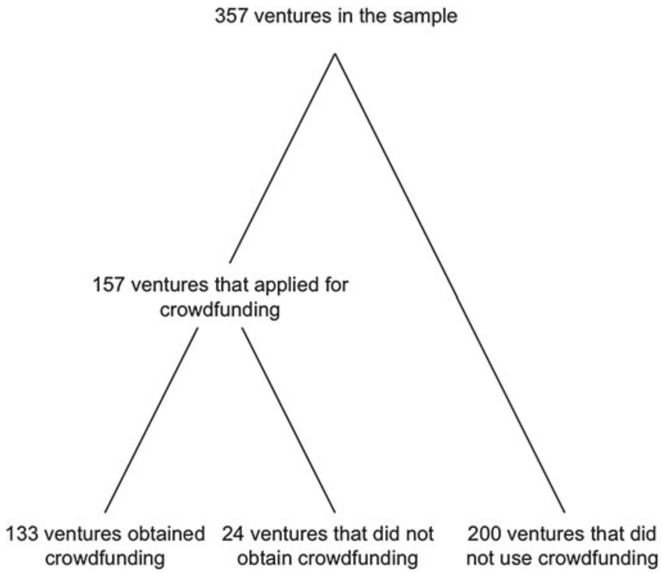

357 ventures in the sample
157 ventures that applied for crowdfunding
133 ventures obtained crowdfunding
24 ventures that did not obtain crowdfunding
200 ventures that did not use crowdfunding

**Fig. 1** Sample of new ventures that apply for crowdfunding or not. *Notes* This figure shows the sample of ventures that applied successfully to one of the six largest equity crowdfunding platforms in Germany for funds between 2011 and 2014. Out of 157 applicants, 133 ventures successfully completed their funding request by obtaining the requested minimum amount, 24 applying ventures were not successfully in terms of raising the the requested minimum amount, and 200 ventures did not apply at all. Some ventures applied multiple times for funding. The data on non-applicants is obtained from the German Federal Association of Startups. The data about crowdfunding applicants were collected from observing applicant data directly in the online platforms maintained by Bankless24, Berfuerst, Companisto, Fundsters, Innovestment, Mashup Finance, Seedmatch, and others

funding (for an overview, see Gompers and Lerner 2001). The ability of crowdfunding to substitute for bank credit or other sources of external finance, due to its significantly lower transaction costs in the Internet age, in particular remains unclear.

This research gap exists primarily because of the absence of data. We hand-collected a sample of all the ventures that applied for funds on major German equity crowdfunding platforms since 2011. That is, among 357 new ventures for which we have data, 157 applied for equity crowdfunding at one of the six major German online platforms between November 2011 and June 2014, which cover 95 % of the total market in terms of offerings and 99 % in terms of volume. Figure 1 illustrates the structure of the sample and the main specifications that explain the odds that a venture apply for external funding on a crowdfunding platform conditional on its bank relationship and venture and management traits.

We manually gathered the data for the crowdfunding ventures from each platform webpage and database. For the 200 ventures that did not use crowdfunding, we obtained the venture and management variables from the membership database of the Federal Association of Startups. Thus, in contrast with previous research into crowdfunding (e.g., Belleflamme et al. 2013; Mollick 2014), we can estimate the probability of tapping the "wisdom of the crowd''Trust and Reputation, conditional on venture and managerial traits, relative to a relevant comparison group of comparable young ventures that face similar financing constraints.

Another challenge that plagues empirical literature pertaining to the role of crowdfunding is the notorious unobservability of the arguably most important competing source of external finance: bank credit. Because we collect information about each ventures' bank relationship, we can exploit the heterogeneity in bank distress in the aftermath of the financial crisis and identify credit supply shocks to ventures, according to the health of their main external financier. To our knowledge, this article is the first to seek to identify the effect of bank stress on alternative forms of external finance directly.

In total, we identify 82 banks connected to the new ventures in our sample and specify five alternative indicators of stressed relationship lenders. The main indicator is whether a bank received capital support from the German Special Fund for Financial Market Stabilization ("SoFFin"), which came into effect as of 2008. With an alternative approach, we also classify banks as stressed if they report an existing restructuring plan, according to the comprehensive assessment conducted by the European Banking Authority (EBA) in November 2014, and whether a regional savings bank belongs to a stressed Landesbank in 2008 (see Puri et al. 2011).

The main results show that ties to a bank bailed out by the SoFFin increase the probability that the venture taps a crowdfunding platforms by 18 %. The probability of successfully completing a crowdfunding request increases by 22 % tough, so the successful completion of a crowdfunding request (the left branch in Fig. 1) does not appear to depend on the indicators of bank distress. That is, credit supply shocks determine the choice to seek alternative funding forms, but they do not necessarily discriminate between projects that can or cannot convince the crowd. The positive effect of crunched banks the use of crowdfunding remains statistically and economically significant, even when we control directly for bank financial profiles. Alternative indicators of bank distress, and especially the existence of restructuring plans shared with the EBA, yield qualitatively similar results, though with weaker statistical significance. Regarding other venture and management traits, we find that the likelihood of using crowdfunding is significantly larger for ventures that exhibit lower ratings, are smaller, and have fewer tangible assets. This result may indicate that ventures with greater information asymmetry suffer the most from a credit supply shock, and therefore seek crowdfunding as an alternative. Whether these projects are more likely to be lemons or gems that have been neglected by banks is an important question for further research.

The remainder of this article is organized as follows: Sect. 2 relates our study to prior literature and provides an institutional background of equity crowdfunding in Germany. In Sect. 3, we present and discuss crowdfunding data, as well as our identification strategy for bank-venture relationships. We discuss the empirical findings in Sect. 4 and conclude in Sect. 5.

## 2 Literature and Background

### 2.1 Bank Funding and Crowdfunding

Banks are vital to resolve information asymmetries, especially those that plague small and medium enterprises (e.g., Petersen and Rajan 1994, 2002; Berger and Udell 1998). The quality of opaque new ventures is difficult for investors to evaluate and information asymmetries always exist during external, early stage financing (see Jensen and Meckling 1976; Stiglitz and Weiss 1981; de Meza and Webb 1987). Information asymmetries between ventures and possible investors result in the well-known pecking order of capital (Myers and Majluf 1984), such that ventures prefer to finance new projects with retained earnings or other internal cash flows, because external funds are more expensive. External debt financing is favored over equity, because the latter dilutes the ownership of the entrepreneur. Robb and Robinson (2014) use the Kauffman Firm Surveys to document the important role of debt at the beginning of a venture's life and suggest that the largest part of total capital comes from outside debt, followed by owners' equity, then insider debt, outside equity, and finally owner debt. Brown et al. (2012) also note the important role for bank debt as a source of funding for new ventures in Germany.

The financial crisis aggravated the financing challenges faced by young ventures during and after 2008 (e.g., Popov and Udell 2012; Jiménez et al. 2012). Puri et al. (2011) document a credit supply crunch among German local lenders and Hempell and Kok (2010) identify a significant bank lending contraction in Germany from the ECB lending survey. Considering the important role of debt use in entrepreneurial financing, we conjecture that banks transmitting a credit shock may cause the young ventures connected to them to grow more inclined to find new sources of funding, especially if small financing volumes imply high relative transaction costs that are unattractive to large-scale investors (Titman and Wessels 1988; Robb and Robinson 2014).

A novel way to reduce transaction costs in entrepreneurial financing is crowdfunding. Schwienbacher and Larralde (2010) provide an overview of nascent equity crowdfunding literature in relation to entrepreneurial finance, in which they discuss why founders choose this source of funding. Hornuf and Schwienbacher (2014) and Mollick (2013) compare crowdfunding to different entrepreneurial financing options. Hemer (2011) emphasizes that the funding process itself is the decisive difference, because "entrepreneurs make an open call for funding on a crowdfunding platform, and investors make their decisions based on the information provided therein. Moreover, the crowdfunding platform facilitates the transaction by providing a standardized investment contract and settling the payments." Bradford (2012) defines equity crowdfunding as a scenario in which supporters or investors receive a stake in the ventures they fund, in the form of profit participation or straight equity. We similarly define equity crowdfunding as a source of funds, obtained when an entrepreneur sells equity shares of a company to a group of (small) investors through an open call for funding on Internet-based platforms.

## 2.2 Institutional Background

Equity crowdfunding platforms are non-bank financial institutions that provide intermediation services for the offering and sale of stocks and similar securities to the general public. These services include the provision of standardized contracts, technology infrastructure for the transactions, and investor relations. To reduce investors' transaction costs, they also provide standardized information, such as pitch decks, financials, and valuations sourced from the venture, without guaranteeing their correctness though. Most equity crowdfunding platforms do not act as open marketplaces but instead serve as network orchestrators, curating the offerings placed on the platform after a cross-check of formal criteria, such as limited liability and available documentation.

Where as some platforms allow the direct acquisition of securities in the venture, others act as nominated agents and pool funds. Because they facilitate the sale of equity-like instruments without voting rights, the platforms fall outside legal brokerage framework, though rapidly growing crowdfunding markets worldwide have prompted some countries (e.g., Italy, the United Kingdom, France, Germany, Spain) to develop specific crowdfunding regulations, with the goal of protecting unprofessional investors and increasing the transparency of offers in the shadow banking market.

German crowdfunding platforms use financial instruments and equity-like mezzanine capital, such as silent partnerships (*Stille Beteiligungen*) and participation rights (*Genussrechte*). More common debt-like mezzanine instruments take the form of subordinated loans (*Partiarische Nachrangdarlehen*), which are less regulated. The offerings of a venture based on equity-like securities in Germany are limited to EUR 100,000 per year without an official prospectus, which is accepted by the *Bundesanstalt fuer Finanzdienstleistungsaufsicht* (BaFin) as long as there are more than 20 investors or the offering is aimed at unprofessional investors with a share price of less than EUR 50,000. Subordinated loans skirt this problem and allow offerings with higher volumes.

As an intermediary between investors and the ventures looking for funding, the platforms are not directly involved in the financial activity and take on very limited responsibility. Revenue is mostly generated from the success fees for offerings that exceed their minimum requested amount, which range between 5 and 10 % of the amount raised. Few platforms operate as full banks, which means they cannot handle the payments on their own and instead must engage an authorized payment service provider or bank, which incurs additional costs of 1–3 % for the funded venture. Expenses to produce a video, often a core element in an offering, together with the costs of preparing and running the campaign and maintaining the investor relations afterwards, also must have to be taken into account by the venture.

Table 1 provides an overview of the German crowdfunding market. The first six projects were funded at the end of November 2011 on the Innovestment and Seedmatch platforms. As of December 2014, 14 active crowdfunding platforms were facilitating equity crowdfunding or revenue-sharing models in Germany. Nine more platforms started operations but closed before their first offering. The total

**Table 1** German crowdfunding market overview

| Year<br>Platform | 2011 | 2012 | 2013 | 2014 | Total |
|---|---|---|---|---|---|
| Bankless24 | – | – | 0.18 (2) | 0.37 (4) | 0.55 (6) |
| Bergfuerst | – | – | 3.0 (1) | 1.1 (1) | 4.1 (2) |
| Companisto | – | 0.55 (6) | 2.65 (15) | 3.9 (9) | 7.1 (30) |
| Fundsters | – | – | 0.56 (5) | 0.48 (6) | 1.04 (11) |
| Innovestment | 0.1 (2) | 1.0 (13/8) | 0.85 (11/4) | 0.3 (7) | 2.25 (33/12) |
| Mashup finance | – | 0.1 (1) | 0.11 (1) | – | 0.21 (2) |
| Seedmatch | 0.35 (4) | 2.2 (22) | 7.32 (22/1) | 9.17 (20) | 19.04 (68/1) |
| Others | – | 0.0 (1) | 0.55 (11) | 0.45 (7) | 1.0 (19) |
| Total | 0.45 (6) | 3.85 (43/8) | 15.22 (68/5) | 15.77 (54) | 35.29 (171/13) |

*Notes* This table presents the volume raised in the German equity crowdfunding market with successful campaigns, in millions of EUR, during the period 2011–2014. The number of (successful/unsuccessful) offerings appear in brackets. *Source* Own elicitation

funding volume of equity crowdfunding platforms in Germany in 2011 was around EUR 0.45 million, but it rose to EUR 35.3 million by the end of 2014. Seven of the 14 active platforms had one or no offerings during this period, and 95 % of the total volume was raised on five platforms: Seedmatch (approximately EUR 19 million), Innovestment (EUR 2.3 million), Bergfuerst (EUR 4.1 million), Fundsters (EUR 1 million), and Companisto (EUR 7.1 million). In total, 171 offerings by the end of 2014 came from 165 different ventures. Thirteen offerings were unsuccessful in that the minimum amount the venture requested by the company was not raised during the funding process.

# 3 Sampling and Identification

## *3.1 Sampling*

To identify the differential effect of a credit supply shock on the inclination of ventures to seek crowdfunding, we sample new ventures that use or that do not use crowdfunding, as shown in Fig. 1. We begin with the members of the Federal Association of Startups in Germany (*Bundesverband Deutsche Startups*). It had 264 members by the end of 2014, of which 64 used crowdfunding. The formal prerequisites to be listed on a German crowdfunding platform are very similar to those required for a membership in the association. We thus identified 93 crowdfunding offerings with available information that applied for funding through the German crowdfunding platforms Bankless24, Bergfuerst, Companisto, Fundsters, Innovestment, Mashup Finance, or Seedmatch between November 2011 and December 2014. The resulting sample included 157 ventures that used crowdfunding (Group 1) and 200 ventures that did not (Group 2). Figure 1 also indicates which of these ventures completed the funding request. The comparison of their descriptive statistics confirms that we compare very similar ventures.

We obtain the data by continuously pulling information from each crowdfunding platform's webpage. The dependent variable is an indicator equal to "1" if the venture attempted to obtain external finance through crowdfunding and "0" otherwise. Of all 157 offerings, 85 % were successful, and the ventures raised about EUR 200,000 from 280 investors on average. With an average company valuation of approximately EUR 1.95 m, the investors acquired about 10 % of a venture. Before turning to the ventures' characteristics, we explain how we collected the data about the venture-bank relationships that we used to identify the effects of bank stress on the odds of using crowdfunding.

### 3.2 *Identification Through Bank Bailouts*

To assess the role of equity crowdfunding as a way to mitigate credit constraints of young ventures, we seek to compare the conditional likelihood that new ventures seek crowdfunding, according to whether they are tied to healthy banks or stressed banks.

To this end, we collect bank-venture relationships for all 357 ventures from the Creditreform database. For each company, it provides a unique bank identification number that indicates the financial institutions with which it has a major credit relationship. We combine these data with the BaFin database to control for consolidation and obtain complete bank names. In total, we identify 82 banks (see Table 9), which we categorize as stressed or healthy, according to the five alternative criteria illustrated in Fig. 2.

For the 82 banks, our base-line identification defines stressed banks as those that received equity support from the SoFFin. In October 2008, the German Federal government founded the *Special Fund for Financial Market Stabilization* (SoFFin) in response to the turmoil in the aftermath of the collapse of Lehman Brothers. The fund was designed to strengthen the capital base of German banks that were hit by taking over problematic positions and providing other guarantees. It had supported a total of 10 German banks since its inception, with a total volume of outstanding equity and guarantees of 192 billion Euros in 2009. By the end of 2014, the SoFFin remained exposed to three German banks with share and hybrid capital equivalent to a total volume of about EUR 17 bn.

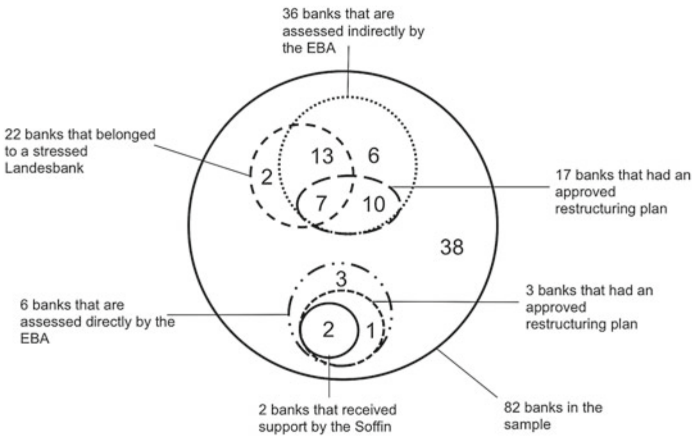

36 banks that are assessed indirectly by the EBA
22 banks that belonged to a stressed Landesbank
17 banks that had an approved restructuring plan
13
6
2
7
10
38
3
6 banks that are assessed directly by the EBA
3 banks that had an approved restructuring plan
2
1
2 banks that received support by the Soffin
82 banks in the sample

**Fig. 2** Definitions of stressed Banks. *Notes* This figure presents the 82 banks in the sample listed in Table 9 that are connected to the 357 ventures shown in Fig. 1. The link between ventures and banks is collected from the Creditreform database. The base line identification defines stressed banks as those that received equity support from the SoFFin. Next, we also define banks as stressed if they had, according to the comprehensive assessment by the European Banking Authority (EBA) of 2014, a restructuring plan in place since before 2013. We distinguish between banks assessed directly by the EBA (6) and those that were connected to a bank holding company that was assessed. Finally, we consider all those regional savings banks that were connected to a Landesbank distressed, because their responsible bank holding company was exposed to the U.S. subprime market shock (Puri et al. 2011)

We matched the bank names from the Creditreform database with public information about which banks were supported by the SoFFin. However, ventures may self-select into bank relationships depending on the health of that bank. For example, participating in the SoFFin support program may induce certain entrepreneurs to avoid seeking credit from such a bank.

Therefore, we also define stressed banks by using the comprehensive assessment by the European Banking Authority (EBA) that took place in November 2014, which is *after* we observe the crowdfunding choices of new ventures in this sample. The assessment by the EBA cannot by itself indicate credit supply strain; rather, it offers a testimony of systemic relevance. Our used EBA based measure of stress is therefore whether a bank had a restructuring plan in place before 2013. As illustrated in Fig. 2, we distinguish generally between banks assessed directly by the EBA and those connected to a bank holding company that was assessed. Finally, we consider any regional savings banks connected to a Landesbank distressed, because their responsible bank holding company was exposed to the US subprime market shock (Puri et al. 2011).

We also follow Berger and Udell (2004) and calculate CAMEL (i.e., capital, asset quality, management quality, and liquidity) covariates for every bank, which we use as proxies for its financial health. Table 2 offers an overview of the

**Table 2** Descriptive statistics: bank characteristics by stress indicator

| *Soffin* | | | | | | | | | *Total* | | | | *Difference* | *Equal variances* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No | | | | Yes | | | | | | | | | |
| | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | | |
| Capital | 0.074 | 0.041 | 0.033 | 0.097 | 0.036 | 0.009 | 0.008 | 0.097 | 0.073 | 0.041 | 0.032 | 0.096 | 0.038 | Yes |
| Asset quality | 0.002 | 0.016 | 0.009 | 0.059 | 0.005 | 0.004 | 0.029 | 0.008 | 0.003 | 0.015 | 0.007 | 0.008 | −0.003 | Yes |
| Management | 0.726 | 0.488 | 0.546 | 0.801 | 0.954 | 0.310 | 0.734 | 1.17 | 0.731 | 0.484 | 0.553 | 0.805 | −0.228 | Yes |
| Earnings | 0.036 | 0.026 | 0.006 | 0.069 | −0.110 | 0.125 | 0.199 | 0.022 | 0.032 | 0.037 | 0.003 | 0.068 | 0.146 | No |
| Liquidity | 0.191 | 0.197 | 0.097 | 0.571 | 0.268 | 0.225 | 0.109 | 0.428 | 0.193 | 0.197 | 0.043 | 0.518 | −0.077 | Yes |
| Sec./ear. assets | 0.273 | 0.123 | 0.131 | 0.502 | 0.418 | 0.160 | 0.305 | 0.531 | 0.276 | 0.125 | 0.134 | 0.506 | −0.146 | Yes |
| Fees/interest | 0.307 | 0.165 | 0.159 | 0.472 | 0.237 | 0.397 | 0.044 | 0.517 | 0.305 | 0.169 | 0.142 | 0.473 | 0.070 | No |
| Observations | 80 | | | | 2 | | | | 82 | | | | | |
| *Landesbanken* | | | | | | | | | *Total* | | | | *Difference* | |
| | No | | | | Yes | | | | | | | | | |
| | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | | |
| Capital | 0.072 | 0.047 | 0.095 | 0.095 | 0.075 | 0.021 | 0.041 | 0.098 | 0.073 | 0.041 | 0.032 | 0.096 | −0.003 | Yes |
| Asset quality | 0.004 | 0.018 | 0.007 | 0.009 | −0.001 | 0.004 | 0.028 | 0.005 | 0.003 | 0.015 | 0.007 | 0.008 | 0.005* | No |
| Management | 0.762 | 0.563 | 0.546 | 0.824 | 0.647 | 0.066 | 0.559 | 0.722 | 0.731 | 0.484 | 0.553 | 0.805 | 0.116 | Yes |
| Earnings | 0.034 | 0.042 | 0.096 | 0.069 | 0.027 | 0.016 | 0.004 | 0.051 | 0.032 | 0.037 | 0.003 | 0.068 | 0.007 | Yes |

(continued)

**Table 2** (continued)

| *Landesbanken* | | | | | | | | | *Total* | | | | *Difference* | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No | | | | Yes | | | | | | | | | |
| | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | | |
| Liquidity | 0.221 | 0.216 | 0.055 | 0.73 | 0.118 | 0.097 | 0.041 | 0.373 | 0.193 | 0.197 | 0.043 | 0.518 | $0.103^{***}$ | No |
| Sec./ear. assets | 0.290 | 0.134 | 0.127 | 0.54 | 0.238 | 0.085 | 0.138 | 0.37 | 0.276 | 0.125 | 0.134 | 0.506 | $0.052^{**}$ | No |
| Fees/interest | 0.316 | 0.194 | 0.051 | 0.598 | 0.274 | 0.049 | 0.19 | 0.365 | 0.305 | 0.169 | 0.142 | 0.473 | $0.042^{*}$ | No |
| Observations | 46 | | | | 36 | | | | 82 | | | | | |

| *Resturcturing plan* | | | | | | | | | *Total* | | | | *Difference* | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No | | | | Yes | | | | | | | | | |
| | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | Mean | SD | p5 | p95 | | |
| Capital | 0.066 | 0.024 | 0.043 | 0.012 | 0.069 | 0.021 | 0.072 | 0.11 | 0.073 | 0.041 | 0.032 | 0.096 | −0.003 | Yes |
| Asset Quality | 0.000 | 0.004 | 0.005 | 0.005 | −0.001 | 0.006 | 0.010 | 0.009 | 0.003 | 0.015 | 0.007 | 0.008 | 0.001 | Yes |
| Management | 0.675 | 0.082 | 0.559 | 0.797 | 0.693 | 0.133 | 0.559 | 0.989 | 0.782 | 0.484 | 0.553 | 0.805 | −0.018 | Yes |
| Earnings | 0.031 | 0.019 | 0.004 | 0.068 | 0.010 | 0.053 | 0.113 | 0.022 | 0.032 | 0.037 | 0.003 | 0.068 | $0.021^{*}$ | Yes |
| Liquidity | 0.169 | 0.186 | 0.043 | 0.518 | 0.164 | 0.143 | 0.034 | 0.525 | 0.193 | 0.197 | 0.043 | 0.518 | 0.005 | Yes |
| Sec./ear. assets | 0.260 | 0.142 | 0.134 | 0.479 | 0.278 | 0.130 | 0.132 | 0.54 | 0.276 | 0.125 | 0.134 | 0.506 | −0.018 | Yes |
| Fees/interest | 0.299 | 0.110 | 0.218 | 0.469 | 0.248 | 0.099 | 0.008 | 0.411 | 0.305 | 0.169 | 0.142 | 0.473 | 0.051 | Yes |
| Observations | 22 | | | | 20 | | | | 42 | | | | | |

*Notes* Descriptive statistics for the characteristics of the banks in the full sample (82 banks, 357 relationships), as well as separately for the different stress indicators. For each variable, this table presents the mean, standard deviation, 5th percentile, 95th percentile, and difference-in-means descriptive statistics of the CAMEL covariates, separated by the different stress indicators.

Banks that are supported by the SoFFin or have an affiliation with a stressed Landesbank exhibit worse CAMEL profiles than non-supported or unaffiliated banks. Of the 82 banks in the sample, 6 were assessed directly by the EBA in their EU-wide stress tests. The parents of another 36 banks were assessed indirectly. Half of the directly assessed banks had a restructuring plan before 2013. The indirectly tested banks also exhibited similar traits.

## 3.3 Venture and Crowdfunding Traits

Table 3 provides an overview of the crowdfunding offerings of the ventures in the sample that had no missing values. Horizontally, we distinguish three panels. The first depicts the traits of firms that use and do not use crowdfunding, such as firm size and other factors motivated by venture capital literature and discussed more extensively in the Results section. Within each panel, we depict the descriptive statistics for ventures with a relationship to a bank that is supported by the SoFFin, which is our main indicator of bank distress.

Regarding venture characteristics, we find that crowdfunding users with ties to stressed bankers tend to exhibit higher asset tangibility, are significantly less often located in cities, and have better credit ratings. Yet the ventures do not differ in terms of size, female board participation, the number of board members, or receipt of a supporting scholarship from the federal government. The right-hand panel also clearly illustrates that none of the differences between firms tied to stressed versus healthy banks are significantly different when we compare crowdfunders with non-crowdfunders. Thus, we need a statistical approach to identify the factors that predict which type of ventures use crowdfunding.

The second panel shows the crowdfunding characteristics. New ventures did not differ significantly in terms of crowdfunding volumes, the number of investors, or firm valuations in the comparison of firms tied to stressed banks versus those connected to non-SoFFin banks. The only significant difference is the lower success rate of obtaining the aimed volume when the bank of a venture is stressed. Finally, the third panel shows that our indicator of bank government support in 2008, SoFFin, effectively gauges the significant difference in financial profiles, reflected by the so-called CAMEL profiles of banks. We discuss the individual effects of these variables subsequently; here, we limit ourselves to noting the upshot of this result: Banks supported by the SoFFin differ significantly, and these differences should help predict, which firms use crowdfunding as a substitute for bank finance.

**Table 3** Descriptive statistics of ventures, crowdfunding projects, and associated banks

| Crowdfunding | *Yes* | | | | | | *No* | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SoFFin | *Yes* | | *No* | | | | *Yes* | | *No* | | | | |
| | Mean | SD | Mean | SD | Difference in means | Equal variances | Mean | SD | Mean | SD | Difference in means | Equal variances | Diff-in-Diff |
| *Venture characteristics* | | | | | | | | | | | | | |
| Credit | 2.043 | 0.629 | 2.143 | 0.692 | −0.099 | Yes | 1.661 | 0.524 | 1.810 | 0.750 | −0.148 | No | −0.049 |
| Size | 10.866 | 1.576 | 11.226 | 1.315 | −0.360 | Yes | 12.317 | 1.826 | 12.513 | 1.586 | −0.196 | Yes | 0.165 |
| Tangibility | 0.123 | 0.137 | 0.069 | 0.089 | 0.054$^{**}$ | No | 0.184 | 0.212 | 0.216 | 0.204 | −0.033 | Yes | −0.087 |
| Gender | 1.449 | 0.777 | 1.286 | 0.667 | 0.164 | Yes | 1.081 | 0.351 | 1.000 | 0.000 | 0.081$^{**}$ | No | −0.083 |
| City | 0.638 | 0.484 | 0.857 | 0.355 | −0.219$^{**}$ | No | 0.742 | 0.439 | 0.810 | 0.402 | −0.068 | Yes | 0.152 |
| Heads | 1.464 | 0.655 | 1.629 | 0.843 | −0.165 | Yes | 1.653 | 0.722 | 1.667 | 0.796 | −0.013 | Yes | 0.151 |
| Rating | 3.275 | 1.235 | 2.486 | 1.337 | 0.790$^{*}$ | Yes | 3.419 | 1.362 | 3.381 | 1.396 | 0.038 | Yes | −0.751$^{*}$ |
| Scholarship | 0.203 | 0.405 | 0.200 | 0.406 | 0.003 | Yes | 0.218 | 0.414 | 0.143 | 0.359 | 0.075 | Yes | 0.072 |
| *Crowdfunding characteristics* | | | | | | | | | | | | | |
| CF min. amount | 69,936 | 116,214 | 53,164 | 20,022 | 16,771 | Yes | | | | | | | |
| CF max. amount | 271,052 | 434,322 | 272,857 | 495,471 | −1,805.0 | Yes | | | | | | | |
| CF realized amount | 216,295 | 385,257 | 233,773 | 498,250 | −17,478.1 | Yes | | | | | | | |
| CF Success | 0.797 | 0.405 | 0.914 | 0.284 | −0.117$^{*}$ | No | | | | | | | |
| Number of CF investors | 289.672 | 328.759 | 315.000 | 337.048 | −25.33 | Yes | | | | | | | |
| Firm valuation before CF | 2,253,699 | 2,719,899 | 1,907,944 | 1,131,583 | 345,754 | No | | | | | | | |

(continued)

**Table 3** (continued)

| Crowdfunding | *Yes* | | | | | | *No* | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SoFFin | *Yes* | | *No* | | | | *Yes* | | *No* | | | | |
| | Mean | SD | Mean | SD | Difference in means | Equal variances | Mean | SD | Mean | SD | Difference in means | Equal variances | Diff-in-Diff |
| *Bank characteristics* | | | | | | | | | | | | | |
| Capital | 0.049 | 0.023 | 0.030 | 0.002 | 0.019*** | No | 0.051 | 0.040 | 0.029 | 0.000 | 0.0216*** | No | 0.003 |
| Asset quality | 0.002 | 0.004 | 0.008 | 0.001 | −0.006*** | No | 0.004 | 0.012 | 0.008 | 0.000 | −0.004 | Yes | 0.001 |
| Management | 0.726 | 0.085 | 0.747 | 0.074 | −0.021 | Yes | 0.772 | 0.387 | 0.734 | 0.000 | 0.038 | Yes | 0.058 |
| Earnings | 0.047 | 0.025 | −0.027 | 0.030 | 0.074*** | Yes | 0.044 | 0.021 | −0.022 | 0.000 | 0.066*** | No | −0.009 |
| Liquidity | 0.386 | 0.326 | 0.418 | 0.054 | −0.032 | No | 0.427 | 0.340 | 0.428 | 0.000 | −0.001 | No | 0.031 |
| Sec./ear. assets | 0.427 | 0.204 | 0.525 | 0.038 | −0.097*** | No | 0.414 | 0.213 | 0.531 | 0.000 | −0.117*** | No | −0.020 |
| Fees/interest | 0.414 | 0.210 | 0.501 | 0.095 | −0.087*** | No | 0.425 | 0.218 | 0.517 | 0.000 | −0.093*** | No | −0.005 |
| Observations | 69 | | 35 | | | | 124 | | 21 | | | | |

*Notes* Descriptive statistics for the outcome of the equity crowdfunding offerings, characteristics of the ventures, and bank characteristics over the period 2011−2014 in Germany on the venture level, separated by the SoFFin indicator. The sample includes all ventures with no missing values. For each variable, the table presents the mean, standard deviation, 5th percentile, 95th percentile, difference-in-means, and difference-in-differences. A offering is successful when the realized amount is larger than the minimum amount requested. Monetary variables are in thousands of EUR

# 4 Model and Results

## *4.1 Specification and Baseline Results*

Table 4 contains the descriptive statistics for our main test variable, an indicator variable (*soffin*) that takes a value of “1” if the bank is supported and “0” otherwise. In total, 24 % of all ventures in the sample have a relationship to a bank supported by the SoFFin. However, the share of companies whose bank is supported by the SoFFin is 37 % among the group of ventures that used crowdfunding—more than twice the share of the group of ventures that did not use crowdfunding (15 %). A venture facing larger credit constraints thus appeared more likely to apply for crowdfunding, after we control for several venture traits, as we discuss shortly.

We predict the likelihood that a venture $i$ applies successfully for crowdfunding $y_i = 1$, conditional on venture traits $x_i$ and whether it is tied to a bank that was bailed out by the $soffin_i$. We use a logit model as a baseline specification and estimate[2]:

$$\Pr(y = 1|x) = \frac{\exp(\alpha + \beta x)}{1 + \exp(\alpha + \beta x)} \tag{1}$$

In addition to our main variable to test for SoFFin support, we added the covariates described in Table 10 and summarized in Table 3 step-by-step. Table 5 contains the marginal effects of the baseline logit regression model to explain crowdfunding.

A range of goodness-of-fit indicators, the Pseudo $R^2$, and Nagelkerke’s $R^2$ support the good discriminatory power of the model, despite the relatively low sample size (Hosmer and Lemeshow 2012). We also compare the predicted probabilities against a moving average of the proportion of cases using a locally weighted scatterplot smoothing graph, which confirms the fit of the model. Likewise, the area under the receiver operating characteristic curve (“AURROC”) of 0.84 for Column 7 in Table 5 strongly indicates that the probability of using crowdfunding is explained quite well by the covariates.

The comparison of the coefficients across ordinary least squares, logit, and probit models tells a qualitatively similar story about the impact of a regressor on the probability of crowdfunding. Robust estimation procedures are qualitatively similar, mitigating potential misspecification concerns. Henceforth, we report the results from the logit regressions.

The marginal effect of the main variable of interest shows that the likelihood of applying for crowdfunding increases when a venture’s bank is supported by the SoFFin. The marginal effect is positive and statistically significant in all models.

[2] We also tested the robustness of all reported results towards using a linear probability model using OLS, which confirms all reported results.

**Table 4** Descriptive statistics: stress indicators

| Crowdfunding | | | | | | | | | | | Total | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | No | | | | | Yes | | | | | | | | | |
| | Obs. | Mean | SD | p5 | p95 | Obs. | Mean | SD | p5 | p95 | Obs. | Mean | SD | p5 | p95 |
| SoFFin | 200 | 0.145 | 0.353 | 0 | 1 | 157 | 0.369 | 0.484 | 0 | 1 | 357 | 0.244 | 0.430 | 0 | 1 |
| Landesbanken | 200 | 0.100 | 0.301 | 0 | 1 | 157 | 0.115 | 0.320 | 0 | 1 | 357 | 0.106 | 0.309 | 0 | 1 |
| Restructuring plan | 153 | 0.307 | 0.463 | 0 | 1 | 129 | 0.566 | 0.498 | 0 | 1 | 282 | 0.426 | 0.495 | 0 | 1 |

*Notes* These descriptive statistics reflects the characteristics of the stress indicators in the full sample. Statistics are presented for all ventures in the full sample (357 ventures) and separately for ventures that used crowdfunding (157 ventures) over the period 2011–2014 and ventures that not use crowdfunding (200 ventures). For each variable, the table presents the mean, standard deviation, 5th percentile, and 95th percentile

**Table 5** Marginal effects for the use of crowdfunding

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) |
|---|---|---|---|---|---|---|---|
| SoFFin | 0.285*** (0.052) | 0.253*** (0.052) | 0.263*** (0.048) | 0.270*** (0.049) | 0.188*** (0.059) | 0.189*** (0.062) | 0.175*** (0.058) |
| Credit fair | | 0.137** (0.058) | 0.090 (0.058) | 0.084 (0.058) | 0.048 (0.063) | 0.095 (0.065) | 0.046 (0.062) |
| Bad | | 0.487*** (0.082) | 0.427*** (0.086) | 0.416*** (0.087) | 0.334*** (0.100) | 0.381*** (0.102) | 0.312*** (0.100) |
| Gender mixed | | | 0.323** (0.118) | 0.337** (0.117) | 0.334** (0.121) | 0.218 (0.137) | 0.284** (0.126) |
| Female | | | 0.393*** (0.079) | 0.399*** (0.078) | 0.401*** (0.101) | 0.457*** (0.093) | 0.409*** (0.103) |
| City | | | | −0.050 (0.053) | −0.003 (0.059) | −0.059 (0.061) | −0.014 (0.058) |
| Heads | | | | −0.008 (0.032) | −0.011 (0.037) | −0.025 (0.038) | −0.005 (0.036) |
| Rating | | | | −0.017 (0.016) | −0.019 (0.018) | −0.024 (0.019) | −0.023 (0.017) |
| Scholarship | | | | 0.068 (0.058) | 0.015 (0.064) | 0.037 (0.066) | 0.016 (0.062) |
| Size | | | | | −0.086*** (0.014) | | −0.078*** (0.014) |
| Tangibility | | | | | | −0.006*** (0.002) | −0.004** (0.002) |
| Observations | 357 | 357 | 357 | 357 | 249 | 249 | 249 |
| Pseudo $R^2$ | 0.049 | 0.107 | 0.157 | 0.164 | 0.260 | 0.202 | 0.280 |
| Nagelkerke's pseudo $R^2$ | 0.087 | 0.182 | 0.260 | 0.270 | 0.401 | 0.323 | 0.426 |
| AUC | 0.612 | 0.705 | 0.749 | 0.763 | 0.828 | 0.777 | 0.837 |

*Notes* This table presents the average marginal effects from logit regression, where the dependent variable is the use of crowdfunding. The sample consists of the 157 ventures that used crowdfunding and 200 ventures that did not use crowdfunding. The variable definitions are provided in the Appendix. Standard errors appear in brackets. Significance levels are as follows: * = 10 %, ** = 5 %, *** = 1 %

Economically, the effect in column (7) is also important. If a new venture is connected to a bank supported by the SoFFin, the probability that it applies for crowdfunding increases by 17.5 %. Against the backdrop of an unconditional probability to apply for funds of 43.9 % (=157/357), this effect is large.

These results support the hypothesis that young ventures are more likely to tap innovative, alternative sources of external funding, especially then when their conventional providers of credit are stressed. To assess whether this result is driven by observable traits related to the degree of information asymmetries and the quality of the venture, we discuss individual control variables next.

### 4.1.1 Credit Scores

Credit scores are a common tool that banks use to evaluate ventures' loan applications, but it is unclear if these ratings affect the availability of debt for young ventures. Robb and Robinson (2014) explore this question with U.S. data from the Kauffman Survey, and observe that information about the ventures' past payment behavior can have a negative effect on access to finance among young ventures. Brown et al. (2012) confirm this view and suggest that information provided by an external credit agency can affect the availability of financing for young ventures; ventures with a good rating have better chances of obtaining a loan, whereas ventures with bad ratings face difficulties getting a loan. In line with prior literature, we expect that ventures with bad credit scores are more likely to use crowdfunding.

External credit ratings provided by Buergel range from A (good) to C (bad). The underlying variable (*credit*) is coded accordingly, such that rating class A takes a value of "1", indicating that the business relation is approved; rating class B is coded "2", which covers approvable business relations and class C is coded with "3", or a bad rating, which means that the business relation is a matter of trust or discretion. Buergel is one of the largest databases on German companies, with more than 3.9 million entries. With BoniCheck, a product of Euler Hermes, it offers an instrument for assessing ventures' solvency. From the Buergel database, we deduced whether an external credit rating, in the form of the BoniCheck indicator, was provided for each venture and, if so, what that rating was. Similar to the credit scores provided by Creditreform or Dun and Bradstreet, the BoniCheck relies on past payment behavior, relative to trade credit from utilities and suppliers. This information is complemented by Buergel's subjective assessment of the ventures' future ability to fulfill credit obligations, derived from information about the ventures' order situation or industry (Brown et al. 2012).

The distribution of good, fair, and bad credit scores is comparable within both groups, exhibiting a total mean of 1.88, or a fair score on average. The estimated marginal effect of credit ratings is significantly positive in all models. A bad credit rating increases the probability of using crowdfunding by 31.2 % compared with ventures that have a fair rating.

### 4.1.2 Size

The decision to finance a venture is based on many factors. Larger ventures can use economies of scale to reduce information asymmetries, but they also have access with different sources of financing, because their risk exposure and the scale of transaction costs differ. They often own more pledgeable collateral and have more diverse cash flows. Small ventures instead are informationally more opaque. Thus, size is an important choice factor when it comes to financing young ventures (Berger and Udell 1998). Small ventures often struggle to resolve informational asymmetries with investors and lenders at acceptable costs, and they therefore are exposed to higher charges for smaller amounts of capital. Transaction costs also influence funding methods. Small amounts often incur relatively high transaction costs, which is why some available sources for certain kinds of ventures are not relevant (Titman and Wessels 1988). For example, the public issues of equity shares during an initial public offering requires a scale that most small companies cannot reach in their early stages, so small ventures are excluded from this type of financing (Cassar 2004).

In summary, smaller ventures often face problems obtaining traditional sources of outside financing, which could influence their use of crowdfunding. Empirical studies generally propose a positive link between venture size and outside financing, leverage, and bank financing (Coleman 2000; Cosh et al. 2009). Therefore, we expect that smaller ventures are more likely to use crowdfunding than large ones.

The mean size (log of total assets) of the sample ventures is 11.78. Ventures that made no use of crowdfunding are larger in terms of total assets, with a log of 12.35 (≈EUR 230.000), than ventures that use of crowdfunding, whose logged size was 10.99 (≈EUR 60.000). We specify the log of assets to measure *size* so that we can mitigate the influence of outliers in the skewed size distribution.[3]

The coefficient for *size* is negative and statistically significant in all models. In line with the expected effect, the coefficient estimate indicates that smaller ventures are more likely to use crowdfunding; a greater size, in terms of logged total assets, decreases the probability per unit change by 8 %.

### 4.1.3 Tangibility

Another trait related to financing, particularly for young ventures, is the structure of their assets (Cassar 2004). In case a bankruptcy occurs, the financial loss for investors can be reduced if the assets are more tangible and generic (Harris and Raviv 1991; Titman and Wessels 1988). Moreover, the adverse selection and moral hazard costs should decrease when ventures pledge assets as collateral or charges get fixed on the tangible assets. Tangible assets increase liquidation value, so companies with a higher share of tangible assets should gain access to traditional sources of finance more easily. The lower costs of financing then tend to result in a higher degree of leverage in the capital structure of these ventures. Empirical evidence suggests that banks base their financing decision, to a certain degree on whether they can hedge the loan with tangible assets (Berger and Udell 1998; Storey 1994). Considering the substantial information asymmetries at the beginning of a venture's life cycle and the information needed to forecast future development, investors have relatively few ways to reduce their risk exposure, other than relationship banking. The asset structure, in terms of the share of tangible assets, often serves as a screening tool for banks, such that it has significant effects on financing at the beginning of a venture (Cassar 2004). Consistent with theoretical predictions, some authors suggest a positive relationship between the share of tangible assets

[3] Alternative treatments of the outliers, such as winsorizing, did not alter our results qualitatively.

and leverage for large ventures, but research pertaining to small ventures is rare, with a just a little evidence of a relationship between the asset structure and the use of debt (e.g. Michaelas et al. 1999). Nevertheless, we expect that the lower the share of tangible assets of a venture, the higher the likelihood of using crowdfunding.

To calculate the asset structure of each venture for every year since its foundation, we divided the non-current assets by total assets, then take the average of these values to define the variable (*tangibility*), ranging from "0" to "1". For the entire sample, tangible assets constitute around 15 % of the total assets of the ventures, but among ventures that did not use crowdfunding, the average tangible assets were greater 18% than it was for ventures that used crowdfunding (10 %).

The coefficients for the *tangibility* variable also were negative in all models and significantly different from zero. Therefore, ventures with a lower share of tangible assets appear to have a higher probability of using crowdfunding. A 1% decrease in the share of tangible assets increases the probability of using crowdfunding by about 0.4 %.

### 4.1.4 Characteristics of the Management Team and Venture

Financial ratios and external ratings alone cannot explain the financing decisions of new ventures. Regarding young ventures in particular, many investors include the owner or management team in their assessment, because their importance during the first years of operations cannot be underestimated (Cassar 2004). For example, due to credit discrimination or the risk aversion of some financiers, the gender composition of the management team can influence the capital structure (Coleman 2000). Arenius and Autio (2006) provide evidence that female-owned businesses are often financed differently than male-owned businesses. Other authors suggest that female-owned ventures have worse initial economic conditions, with a lower capital base (Verheul and Thurik 2001), and they face the problem of being less likely to obtain external funding (Coleman 2000). Furthermore, they usually use different sources to finance their business than do male-owned ventures (Neider 1987; Lerner et al. 1997) and face particular difficulties applying for and securing bank loans (Riding and Swift 1990; Coleman 2000; Anna et al. 2000). Ventures with mixed gender or purely female teams thus may be more likely to use crowdfunding than ventures with a male management team.

The number of members in the management team also can affect the chances of obtaining external capital. Chandler and Hanks (1998) show that ventures founded and led by a team often are more successful than those founded and led by single person. Beckman et al. (2007) find that the number of team members and the team composition have positive effects on the likelihood of ventures attracting external financing. Therefore, we posit that ventures with smaller management teams are more likely to use crowdfunding.

To control for management team characteristics, we add the number of management team members (*heads*) and the gender composition of the management team. The latter is specified as an ordinal variable (*gender*), with "1" indicating a male-only team, “2” a mixed team, and “3” a female-only team. Most of the management teams in the sample were purely male, as the 1.21 mean for the gender composition shows. Ventures that used crowdfunding included slightly more women in their teams (1.38) than ventures that did not use crowdfunding (1.1). With respect to the number of heads in the management team, the groups were comparable, with a total average of 1.59 persons, though the ventures that did not use crowdfunding were slightly larger on average.

The scholarship variable indicated whether the venture received support from the Federal Ministry of Economics and Energy (“Bundesministerium für Wirtschaft und Energie”, BMWi), in the form of an EXIST founder scholarship, a nationwide funding program, which supports innovative businesses that started in universities and research institutions during their early phases, such that it could be interpreted as a signal of quality. Approximately 20 % of the ventures in the sample received this kind of support, with similar distributions across ventures that used and did not use crowdfunding.

Most financiers invest only within a close geographic scope (Gupta and Sapienza 1992), and rural areas are often characterized by worse access to financing (Strotmann 2006). Therefore, ventures from rural areas should exhibit a higher likelihood of using crowdfunding than ventures from urban areas. The dichotomous variable (*city*) equals “1” if the headquarters is located in a city with more than 500,000 (urban) inhabitants and “0” otherwise (rural). Of all ventures, 73 % are located in cities with more than 500,000 inhabitants, though ventures that did not use crowdfunding were slightly more often located in urban areas (74 %) than ventures that used crowdfunding (73 %).

The hypothesis for the city variable predicted that ventures in rural areas should have a higher likelihood of using crowdfunding, because they have less access to finance. The coefficient for this variable was not statistically significant though, the negative sign indicated that ventures in rural areas are more likely to use crowdfunding.

In the last model in Table 5, the variables capturing the number of management heads and the location of the headquarters are both negative but not significant. The existence of a scholarship seems to increase the probability of using crowdfunding but is also not different from zero. The gender composition also has an important role, with a positive effect of using crowdfunding when the management team is female. Compared with solely male teams, the probability of using crowdfunding increases significantly by 28 % when there are male and female heads and by about 42 % when the management team is purely female.

### 4.1.5 Rating of Sophisticated Investors

A business plan is one of the most important steps to take when launching a venture. In addition to providing economic efficiency, it exists mainly to raise funds to start or expand a project. Mason and Harrison (1996) thus assert that the business plan is the minimum requirement for any financing application, because more than three-quarters of business angels base their investment decision on this document. Different studies investigate the decision-making process adopted by venture capital companies and suggest that the owner, the business strategy, and financial issues are not the only determinants of investment decisions (Zacharakis and Meyer 1998; Hall and Hofer 1993). Many investors focus on product potential, industry-specific outlooks, and growth opportunities. Sweeting (1991) shows that equity investors typically spend less than 10 min on the first screening, and Hall and Hofer (1993) indicate that they spend less than six minutes. Business angels typically devote up to nine minutes to the screening process (Mason and Rogers 1997). As an emergent and therefore rather unusual tool for financing a venture due to possible legal uncertainties, crowdfunding likely represents a second choice, such that ventures likely tried to obtain funds through traditional sources of capital first. Therefore, we expect that ventures that do not provoke detailed investigation or consideration by sophisticated investors are more likely to use crowdfunding.

The funding decision is often modeled as a stepwise process (Haines et al. 2003), with three different phases: the initial screening, the detailed investigation, and the negotiation and deal closing. The information provided on the ventures' websites provides a way to imitate the screening process and obtain ratings from different, sophisticated investors about the quality of the ventures in the data sample, as well as whether they would move on to the second step of the process, the detailed investigation, or would decide not to pursue them after the first screening. To gather this measure, we presented all the ventures to seven different equity investors from Germany, who indicated if they would further investigate investing in each venture. To avoid bias, the selected investors differed in their characteristics, such as deal volume, industry focus, type, and location. The variable (*rating*) is the sum of the single ratings, which provide a dummy variable equal to "1" for interesting follow-up investment opportunities and "0" for ventures that the investors would not take into consideration. The average rating was almost identical for both groups. On average, about 50 % of the investors would take a venture from the sample into consideration for further investigation, and the difference between the groups was small. This last explanatory variable controls for whether the ventures used crowdfunding because they were not considered for detailed investigation by sophisticated investors. Although the negative coefficient of the rating variable indicated that ventures classified as non-qualified for further investigation by investors had a higher probability of using crowdfunding than companies that were considered by more investors, the coefficient was not significantly different from zero.

## *4.2 Bank Characteristics*

A possible concern in our analysis is that our results could be driven by unobservable bank characteristics that may be correlated with the SoFFin indicator and subsequent lending and risk taking. The SoFFin indicator could therefore could merely confound unobserved traits with credit supply crunch effects.

To mitigate this concern, we specified bank-level control variables in a next step, measured as the average over the period 2009–2014. We included the same control variables described previously to gauge the financial health of banks measured according to the CAMEL supervisory ratings system (i.e., capital, asset quality, management quality, and liquidity). Table 6 reports the results of the baseline model with a stepwise integration of CAMEL covariates.

The positive effect of crunched banks on the use of crowdsourced finance indicated by support from the SoFFin, remained statistically and economically significant even when we controlled directly for financial bank profiles. The concern that the SoFFin indicator merely confounded unobserved traits as credit supply shocks thus was invalidated by the intact, significant SoFFin effect. The absence of any significant bank-covariate effect, in turn, most likely reflects the limited information contained by an averaged cross-section of bank data to which we are constrained given the lack of panel firm data. Future research extending the information about firms to longitudinal data is therefore important.

## *4.3 Alternative Bank Stress Indicators*

Some of the ventures were founded after the capital injections by the SoFFin, so that our results could driven by the ventures' choice of a bank supported by the SoFFin, rather than a non-supported bank. Table 7 shows the effect of the alternative bank stress indicators illustrated in Fig. 2.

Column (1) replicates the baseline results with bank-specific controls. The alternative bank stress indicators in column (2) refer to the connection of one of the local savings banks with a stressed Landesbank, as in Puri et al. (2011). These authors show that local savings banks restricted loan supply when they were connected to a Landesbanken with substantial subprime exposure. We similarly include an indicator of whether a regional savings bank in our sample belonged to a stressed Landesbank. Although the marginal effect of the Landesbanken variable was positive, indicating a higher probability of using crowdfunding when the respective bank of a venture belonged to a stressed Landesbank, the coefficient was very small and not significant.

Next, we included the results of the EU-wide bank stress test by the EBA, published in November 2014, because it gauges information that was not available to ventures that might have selected banks on quality.

In column (3), we specify a more direct measure of the health of the banks tested (direct and indirectly). Financial institutions reported, during the comprehensive assessment in November 2014, whether they had a restructuring plan in place before December 2013. The new ventures, sampled between 2011 and 2014, are unlikely to have had full knowledge of such restructuring initiatives when choosing whether to apply for crowdfunding, conditional on their existing bank relationships.

**Table 6** Marginal effects: use of crowdfunding with bank characteristics

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|---|---|---|
| *Treatment effect* | | | | | | | | |
| SoFFin | 0.172$^{***}$<br>(0.061) | 0.224$^{***}$<br>(0.068) | 0.175$^{***}$<br>(0.058) | 0.207$^{**}$<br>(0.099) | 0.174$^{***}$<br>(0.058) | 0.169$^{***}$<br>(0.059) | 0.174$^{***}$<br>(0.059) | 0.279$^{**}$<br>(0.138) |
| *Venture characteristics* | | | | | | | | |
| Credit fair | 0.046<br>(0.063) | 0.039<br>(0.063) | 0.046<br>(0.063) | 0.046<br>(0.062) | 0.045<br>(0.062) | 0.046<br>(0.062) | 0.046<br>(0.063) | 0.027<br>(0.062) |
| Bad | 0.311$^{***}$<br>(0.100) | 0.314$^{***}$<br>(0.099) | 0.311$^{***}$<br>(0.100) | 0.310$^{***}$<br>(0.100) | 0.313$^{***}$<br>(0.100) | 0.306$^{***}$<br>(0.100) | 0.312$^{***}$<br>(0.100) | 0.294$^{***}$<br>(0.099) |
| Gender mixed | 0.283$^{**}$<br>(0.126) | 0.290$^{**}$<br>(0.124) | 0.283$^{**}$<br>(0.126) | 0.282$^{**}$<br>(0.126) | 0.290$^{**}$<br>(0.126) | 0.278$^{**}$<br>(0.127) | 0.283$^{**}$<br>(0.126) | 0.310$^{**}$<br>(0.125) |
| Female | 0.408$^{***}$<br>(0.103) | 0.404$^{***}$<br>(0.103) | 0.408$^{***}$<br>(0.103) | 0.404$^{***}$<br>(0.104) | 0.408$^{***}$<br>(0.104) | 0.409$^{***}$<br>(0.102) | 0.410$^{***}$<br>(0.102) | 0.391$^{***}$<br>(0.105) |
| City | −0.017<br>(0.061) | 0.003<br>(0.059) | −0.012<br>(0.059) | −0.018<br>(0.059) | −0.009<br>(0.060) | −0.024<br>(0.061) | −0.016<br>(0.060) | −0.023<br>(0.064) |
| Heads | −0.006<br>(0.036) | −0.006<br>(0.036) | −0.006<br>(0.036) | −0.006<br>(0.036) | −0.006<br>(0.036) | −0.005<br>(0.036) | −0.005<br>(0.036) | 0.002<br>(0.036) |
| Rating | −0.023<br>(0.017) | −0.020<br>(0.017) | −0.023<br>(0.017) | −0.023<br>(0.017) | −0.022<br>(0.017) | −0.023<br>(0.017) | −0.023<br>(0.017) | −0.020<br>(0.017) |
| Scholarship | 0.016<br>(0.062) | 0.015<br>(0.062) | 0.016<br>(0.062) | 0.016<br>(0.062) | 0.015<br>(0.063) | 0.017<br>(0.062) | 0.016<br>(0.062) | 0.010<br>(0.061) |
| Size | −0.078$^{***}$<br>(0.014) | −0.079$^{***}$<br>(0.014) | −0.077$^{***}$<br>(0.014) | −0.078$^{***}$<br>(0.014) | −0.077$^{***}$<br>(0.014) | −0.078$^{***}$<br>(0.014) | −0.078$^{***}$<br>(0.014) | −0.081$^{***}$<br>(0.014) |
| Tangibility | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) | −0.004$^{**}$<br>(0.002) |

(continued)

**Table 6** (continued)

| | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
|---|---|---|---|---|---|---|---|---|
| *Bank characteristics* | | | | | | | | |
| Capital | −0.002<br>(0.010) | | | | | | | 0.011<br>(0.016) |
| Asset quality | | −0.100<br>(0.073) | | | | | | −0.137$^{*}$<br>(0.079) |
| Management | | | −0.000<br>(0.002) | | | | | 0.004<br>(0.003) |
| Earnings | | | | 0.004<br>(0.011) | | | | 0.010<br>(0.014) |
| Liquidity | | | | | −0.000<br>(0.001) | | | −0.003<br>(0.002) |
| Sec/ear. assets | | | | | | 0.001<br>(0.001) | | 0.007<br>(0.004) |
| Fees/interest | | | | | | | 0.000<br>(0.001) | −0.002<br>(0.003) |
| Observations | 249 | 249 | 249 | 249 | 249 | 249 | 249 | 249 |
| Pseudo $R^2$ | 0.280 | 0.286 | 0.280 | 0.281 | 0.280 | 0.281 | 0.280 | 0.299 |
| Nagelkerke's pseudo $R^2$ | 0.426 | 0.434 | 0.426 | 0.427 | 0.426 | 0.427 | 0.426 | 0.450 |
| AUC | 0.837 | 0.838 | 0.836 | 0.837 | 0.837 | 0.838 | 0.837 | 0.847 |

*Notes* This table presents the average marginal effects from a logit regression, where the dependent variable is the use of crowdfunding. Independent variables include venture characteristics and characteristics of the respective banks as CAMEL covariates. The sample consists of the 157 ventures that used crowdfunding and 200 ventures that did not use crowdfunding. The variable definitions are provided in the Appendix. Standard errors appear in brackets. Significance levels are as follows: * = 10 %, ** = 5 %, *** = 1 %

**Table 7** Marginal effects with alternative treatment effects

| | (1) | (2) | (3) |
|---|---|---|---|
| SoFFin | $0.187^{***}$<br>(0.057) | | |
| Landesbanken | | 0.006<br>(0.081) | |
| Restructuring plan | | | $0.169^{***}$<br>(0.054) |
| Control variables included? | Yes | Yes | Yes |
| Observations | 249 | 249 | 196 |
| Pseudo $R^2$ | 0.270 | 0.242 | 0.296 |
| Nagelkerke's pseudo $R^2$ | 0.414 | 0.378 | 0.447 |
| AUC | 0.832 | 0.823 | 0.846 |

*Notes* This table presents the average marginal effects from a logit regression, where the dependent variable is the use of crowdfunding. Independent variables include venture characteristics and characteristics of the respective banks as CAMEL covariates. The sample consists of the 157 ventures that used crowdfunding and 200 ventures that did not use crowdfunding. The variable definitions are provided in the Appendix. Standard errors appear in brackets. Significance levels are as follows: * = 10 %, ** = 5 %, *** = 1 %

For the restructuring plan variable, the marginal affirmed indeed that the probability of using crowdfunding increased by 17 %.

In summary, for the existence of restructuring plans shared with the EBA, we found results that were qualitatively similar to those we obtained with the SoFFin indicator.

## *4.4 Using Versus Successfully Completing Crowdfunding*

The previous analysis indicates that ventures are more likely to use crowdfunding when their bank is stressed. But applying for crowdfunding does not automatically imply tthe successful completion of the funding request. Only 85 % of the ventures in our sample were able to convince the crowd and collect the minimum requested funding volume. Thus, the wisdom of the crowd may be just as skilled as conventional intermediaries in selecting lemons out of the pool of applicants.

To test this conjecture, we differentiated between ventures that applied for crowdfunding and those that successfully obtained crowdfunding financing as a function of stressed versus healthy bank relationships. With this information, we provide more direct evidence of whether the wisdom of the (investor)crowd can substitute for bank credit as a major funding source of new ventures if banks are shocked.

In Table 8, we compare (1) the probability of applying for crowdfunding with (2) the probability of successfully completing a crowdfunding request in the full

**Table 8** Marginal effects: use and outcome of crowdfunding

| | (1) Use of crowdfunding (full sample) | (2) Successful use of crowdfunding (full sample) | (3) Successful use of crowdfunding (only ventures that used crowdfunding) |
|---|---|---|---|
| SoFFin | $0.175^{***}$<br>(0.058) | $0.216^{***}$<br>(0.058) | 0.077<br>(0.087) |
| Credit fair | 0.046<br>(0.062) | $0.135^{**}$<br>(0.064) | $0.224^{**}$<br>(0.110) |
| Bad | $0.312^{***}$<br>(0.100) | $0.203^{**}$<br>(0.098) | 0.152<br>(0.124) |
| Gender mixed | $0.284^{**}$<br>(0.126) | $0.318^{**}$<br>(0.134) | 0.000 |
| Female | $0.409^{***}$<br>(0.103) | $0.333^{***}$<br>(0.109) | 0.027<br>(0.091) |
| City | −0.014<br>(0.058) | 0.019<br>(0.061) | 0.033<br>(0.071) |
| Heads | −0.005<br>(0.036) | 0.035<br>(0.038) | $0.178^{**}$<br>(0.085) |
| Rating | −0.023<br>(0.017) | −0.017<br>(0.018) | 0.015<br>(0.022) |
| Scholarship | 0.016<br>(0.062) | 0.050<br>(0.066) | 0.135<br>(0.100) |
| Size | $-0.078^{***}$<br>(0.014) | $-0.041^{***}$<br>(0.015) | $0.083^{***}$<br>(0.024) |
| Tangibility | $-0.004^{**}$<br>(0.002) | $-0.004^{**}$<br>(0.002) | −0.003<br>(0.003) |
| Observations | 249 | 249 | 95 |
| Pseudo $R^2$ | 0.280 | 0.193 | 0.370 |
| Nagelkerke's pseudo $R^2$ | 0.426 | 0.305 | 0.482 |
| AUC | 0.837 | 0.786 | 0.886 |

*Notes* This table presents the average marginal effects from a logit regression where the dependent variable is the use of crowdfunding for the full sample (Column (1)), the successful use of crowdfunding (realized amount > requested amount) for the full sample (Column (2)), or the successful use of crowdfunding for the sample of ventures that used crowdfunding (Column (3)). The variable definitions are provided in the appendix. Standard errors appear in brackets. Significance levels are as follows: * = 10 %, ** = 5 %, *** = 1 %

sample and (3) the probability of successfully completing a crowdfunding request among ventures that applied for crowdfunding. The relationship with a stressed bank increased the probability of using crowdfunding in the baseline model by 17 %, and the same variable explained an increase of 22 % in the probability of successfully completing a crowdfunding request. The successful completion of a crowdfunding request among the 157 ventures only did not depend on indicators of bank distress. Thus, credit supply shocks appear to determine the choice to seek alternative funding forms, but do not necessarily discriminate between projects that can or cannot convince the crowd.

## 5 Conclusion

Financing is a key component of entrepreneurial activities. By observing, which ventures cooperated with banks that had to be bailed out by the German government, we identify an effect of an exogenous credit supply shock on the likelihood of using equity crowd funding. To this end, we manually collected a unique data set that provided information about the financing decisions of young ventures in Germany. Specifically, we used data from 357 young ventures to test how certain characteristics, in terms of bank relationship, size, asset structure, and other factors, affect the probability that the venture will use crowdfunding.

Our results show that a relationship of a venture with a bailed out bank increases the probability that a venture uses crowdfunding by 18 %. This effect is both economically and statistically significant. The analysis also shows that bad credit scores increase the probability that a venture uses crowdfunding by 31 %. Supply-side restrictions move banks to handle their lending more restrictively, and ventures that cannot demonstrate their creditworthiness are not financed. This result suggests that among opaque new ventures, riskier projects tend to tap equity crowdfunding instead of bank financing.

We also find that smaller ventures and ventures with fewer tangible assets are more likely to use crowdfunding. The small amounts obtained in a crowdfunding offering makes this finding plausible. Larger ventures often need greater volumes and have access to other or cheaper sources of capital, such as initial public offerings. However, management team characteristics have no statistically significant effect. Likewise, the rating of the venture's quality by experts, the location of the headquarters, the receive of a scholarship, and the number of heads all showed no significant influence on a venture's use of crowdfunding. That is, the use of crowdfunding is not a question of management or other organizational factors. This result also supports the hypothesis that quality differences are not crucial.

Perhaps the most important finding though is that ventures are more likely to use crowdfunding when their bank is affected by a credit crunch. Equity crowdfunding thus seems to be of particular importance for entrepreneurial finance, as a critical source of capital in stressful times for banks.

## Appendix

See Tables 9 and 10.

**Table 9** Bank overview

| BvD ID | Bank name | Bank-venture observations | Category | SoFFin | Landesbank | EBA direct | EBA indirect |
|---|---|---|---|---|---|---|---|
| 13046 | Bank fuer Sozialwirtschaft | 2 | Cooperative | | | | |
| 13047 | ING-DiBa | 1 | Private | | | | |
| 13124 | Volksbank Potsdam | 13 | Cooperative | | | | |
| 13190 | Commerzbank | 84 | Private | X | | X | |
| 13192 | Donner and Reuschel | 2 | Private | | | | |
| 13216 | Deutsche Bank | 77 | Private | | | X | |
| 13263 | Frankfurter Sparkasse Sprendlingen | 2 | Savings | | | | X |
| 13264 | Frankfurter Volksbank | 1 | Cooperative | | | | |
| 13296 | Heidelberger Volksbank eG | 1 | Cooperative | | | | |
| 13319 | IKB Deutsche Industriebank AG | 3 | Private | X | | X | |
| 13326 | Koelner Bank | 1 | Cooperative | | | | |
| 13331 | Sparkasse Dachau | 1 | Savings | | Bayern LB | | X |
| 13366 | Kreissparkasse Ahrweiler | 1 | Savings | | | | |
| 13379 | Sparkasse Zollernalb | 1 | Savings | | | | X |
| 13380 | Sparkasse Bamberg | 2 | Savings | | Bayern LB | | X |
| 13400 | Sparkasse Dueren | 1 | Savings | | West LB | | X |
| 13418 | Kreissparkasse Gross-Gerau | 2 | Savings | | | | X |
| 13437 | Kreissparkasse Koeln | 2 | Savings | | West LB | | X |
| 13444 | Kreissparkasse Ludwigsburg | 1 | Savings | | | | X |
| 13498 | Kreissparkasse Waiblingen | 1 | Savings | | | | X |
| 13570 | Nassauische Sparkasse | 1 | Savings | | | | X |
| 13655 | Sparkasse Bochum | 1 | Savings | | West LB | | X |
| 13724 | Sparkasse Karlsruhe Ettlingen | 2 | Savings | | | | X |

(continued)

**Table 9** (continued)

| BvD ID | Bank name | Bank-venture observations | Category | SoFFin | Landesbank | EBA direct | EBA indirect |
|---|---|---|---|---|---|---|---|
| 13727 | Sparkasse Koblenz | 2 | Savings | | | | |
| 13732 | Sparkasse Landshut | 1 | Savings | | Bayern LB | | X |
| 13740 | Sparkasse Mainz | 2 | Savings | | | | |
| 13742 | Sparkasse Markgraeflerland | 1 | Savings | | | | X |
| 13762 | Sparkasse Passau | 1 | Savings | | Bayern LB | | X |
| 13803 | Stadt- und Kreis-Sparkasse Darmstadt | 1 | Savings | | | | X |
| 13804 | Stadt- und Kreissparkasse Erlangen | 3 | Savings | | Bayern LB | | X |
| 13839 | Sparkasse Aachen | 1 | Savings | | West LB | | X |
| 13842 | Stadtsparkasse Augsburg | 1 | Savings | | Bayern LB | | X |
| 13858 | Sparkasse Harburg-Buxtehude | 1 | Savings | | | | X |
| 13866 | Stadtsparkasse Duesseldorf | 3 | Savings | | West LB | | X |
| 13869 | Verbundsparkasse Emsdetten Ochtrup | 1 | Savings | | West LB | | X |
| 13885 | Sparkasse Hannover | 4 | Savings | | | | X |
| 13894 | Kreissparkasse Kaiserslautern | 2 | Savings | | | | |
| 13896 | Kasseler Sparkasse | 1 | Savings | | | | X |
| 13912 | Stadtsparkasse Muenchen | 7 | Savings | | Bayern LB | | X |
| 13937 | Stadtsparkasse Schwerte | 1 | Savings | | West LB | | X |
| 14008 | Volksbank Ludwigsburg eG | 1 | Cooperative | | | | |
| 14011 | Volksbank Paderborn-Hoexter-Detmold | 1 | Cooperative | | | | |
| 14037 | Sparkasse Hoexter | 1 | Savings | | West LB | | X |
| 14067 | Volksbank Stuttgart | 2 | Cooperative | | | | |
| 14090 | Sparkasse Muelheim an der Ruhr | 1 | Savings | | West LB | | X |
| 14104 | Berliner Sparkasse | 31 | Savings | | | X | |

(continued)

**Table 9** (continued)

| BvD ID | Bank name | Bank-venture observations | Category | SoFFin | Landesbank | EBA direct | EBA indirect |
|---|---|---|---|---|---|---|---|
| 14123 | Herner Sparkasse | 1 | Savings |  | West LB |  | X |
| 14133 | Postbank | 18 | Private |  |  |  | X |
| 14166 | Volksbank Mittelhessen | 1 | Cooperative |  |  |  |  |
| 14199 | Sparkasse Leipzig | 1 | Savings |  | Sachsen LB |  |  |
| 14469 | Ostsaechsische Sparkasse Dresden | 2 | Savings |  | Sachsen LB |  |  |
| 14530 | Volksbank Karlsruhe | 1 | Cooperative |  |  |  |  |
| 14654 | Deutsche Kontor Privatbank AG | 1 | Private |  |  |  |  |
| 15415 | Raiffeisenbank Gundelfingen | 2 | Cooperative |  |  |  |  |
| 27737 | National Bank | 1 | Private |  |  |  |  |
| 29867 | Sparkasse KoelnBonn | 4 | Savings |  | West LB |  | X |
| 40293 | Hamburger Sparkasse | 10 | Savings |  |  | X |  |
| 40583 | GLS Gemeinschaftsbank | 5 | Cooperative |  |  |  |  |
| 40867 | Sparkasse Westmuensterland | 1 | Savings |  | West LB |  | X |
| 41395 | VR-Bank Rhein-Sieg | 1 | Cooperative |  |  |  |  |
| 42705 | Volksbank Rhein-Nahe-Hunsrueck | 1 | Cooperative |  |  |  |  |
| 42771 | Sparkasse Oder-Spree | 1 | Savings |  |  |  |  |
| 43024 | Volksbank Neckartal | 1 | Cooperative |  |  |  |  |
| 43128 | Volksbank Erft | 1 | Cooperative |  |  |  |  |
| 43289 | Nordthueringer Volksbank | 1 | Cooperative |  |  |  |  |
| 43393 | Stadtsparkasse Magdeburg | 2 | Savings |  |  |  | X |
| 43617 | VR-Bank Starnberg-Herrsching-Landsberg | 1 | Cooperative |  |  |  |  |
| 43968 | Volksbank St. Blasien | 1 | Cooperative |  |  |  |  |
| 44034 | Sparkasse Maerkisch-Oderland | 1 | Savings |  |  |  |  |

(continued)

**Table 9** (continued)

| BvD ID | Bank name | Bank-venture observations | Category | SoFFin | Landesbank | EBA direct | EBA indirect |
|---|---|---|---|---|---|---|---|
| 44155 | VR-Bank Passau | 1 | Cooperative | | | | |
| 44562 | Sparkasse Bremen | 1 | Savings | | | | X |
| 45341 | Raiffeisenbank Heinsberg | 1 | Cooperative | | | | |
| 45375 | Sparkasse Herford | 1 | Savings | | West LB | | X |
| 45877 | Raiffeisenbank Parsberg-Velburg | 1 | Cooperative | | | | |
| 46123 | Volksbank Welzheim | 2 | Cooperative | | | | |
| 46801 | HypoVereinsbank | 11 | Private | | | | |
| 47101 | VR Bank Muenchen Land | 1 | Cooperative | | | | |
| 47634 | Volksbank Brilon-Baeren-Salzkotten | 1 | Cooperative | | | | |
| 47699 | Vereinigte Volksbank Maingau | 1 | Cooperative | | | | |
| 47734 | LBBW | 2 | Landesbank | | | X | |
| 49769 | Sparkasse Schaumburg | 1 | Savings | | | | X |
| 49838 | Volksbank Sauerland | 1 | Cooperative | | | | |
| | Total Bank Observations | 82 (357) | | 2 (87) | 22 (38) | 6 (207) | 36 (75) |
| | Thereof cooperative banks | 27 (47) | | | | | |
| | Thereof landesbanken | 1 (2) | | | | | |
| | Thereof private banks | 9 (198) | | | | | |
| | Thereof savings banks | 45 (110) | | | | | |

*Notes* These descriptive statistics detail the banks in the full sample. The number of bank-venture observations appear in brackets

**Table 10** Definition of variables

| Variable name | Source | Description | Measurement unit |
|---|---|---|---|
| *Crowdfunding characteristics* | | | |
| Crowdfunding | Crowdfunding platforms | Dummy variable equal to one if the venture used crowdfunding | Binary |
| CF min. amount | Crowdfunding platforms | Minimum amount of the respective crowdfunding offering | EUR |
| CF max. amount | Crowdfunding platforms | Maximum amount of the respective crowdfunding offering | EUR |
| CF realized amount | Crowdfunding platforms | Realized amount of the respective crowdfunding offering | EUR |
| CF success | Crowdfunding platforms | Dummy variable equal to one if the venture used successfully crowdfunding (realized amount > minimum amount) | Binary |
| Number of CF investors | Crowdfunding platforms | Number of investors in the respective crowdfunding offering | # |
| Valuation of venture before CF | Crowdfunding platforms | Valuation of Venture before the crowdfunding offering, which is done by the platform | EUR |
| *Venture characteristics* | | | |
| Size | Bundesanzeiger | Log of total assets as average since foundation | Log of EUR |
| Tangibility | Bundesanzeiger | Percentage of tangible assets as average since foundation | % |
| Heads | Creditreform | Number of heads in the management team | # |
| Gender | Creditreform | Gender composition of the management team (male/mixed/female) | Categorical |
| Credit | Buergel | Credit rating of the venture (good/fair/bad) | Categorical |
| Rating | | Rating of seven sophisticated investors if they would further investigate an investment for each venture (0/1) | Categorical |
| City | Creditreform | Dummy variable equal to one if the location of headquarter of the venture is based in a city with more than 500,000 inhabitants | Binary |
| Scholarship | BMWi | Dummy variable equal to one if the venture received the EXIST scholarship by the BMWi | Binary |
| *Treatments* | | | |
| SoFFin | BMFS | Dummy variable equal to one if the bank of the venture received funds from the SoFFin | Binary |

(continued)

**Table 10** (continued)

| Variable name | Source | Description | Measurement unit |
|---|---|---|---|
| Landesbanken | Sparkassen-Verband | Dummy variable equal to one if the bank of the venture is a savings bank that owns holdings in one of the affected Landesbanken (Bayern LB, Sachsen LB, West LB) | Binary |
| EBA | European Banking Authority | Dummy variable equal to one if the bank of the venture is directly or indirectly included in the 2014 EU-wide stress test conducted by the European Banking Authority (EBA) | Binary |
| EBA direct | European Banking Authority | Dummy variable equal to one if the bank of the venture is directly included in the 2014 EU-wide stress test conducted by the European Banking Authority (EBA) | Binary |
| EBA indirect | European Banking Authority | Dummy variable equal to one if the bank of the venture is indirectly over holdings included in the 2014 EU-wide stress test conducted by the European Banking Authority (EBA) | Binary |
| CET1 16 | European Banking Authority | Fully loaded Common Equity Tier 1 (CET1) ratio in the adverse scenario 2016 | % |
| CET1 16—CET1 13 | European Banking Authority | Difference between the CET1 ratio starting 2013 and the fully loaded CET1 ratio in the adverse scenario 2016 | % |
| CET1 16 < 8 % | European Banking Authority | Dummy variable equal to one if the CET1 ratio of the tested bank is lower than 8 % in the adverse scenario 2016 | Binary |
| Restructuring plan | European Banking Authority | Dummy variable equal to one if the bank of the venture had an restructuring plan before 2013 | Binary |
| *Bank characteristics* | | | |
| Capital | Bankscope | Proxy for capital adequacy of a venture's bank measured as the ratio of total equity to total assets | % |
| Asset quality | Bankscope | Proxy for asset quality of a venture's bank measured as the ratio of loan loss provisions to total gross loans | % |
| Management | Bankscope | Proxy for managerial quality of a venture's bank measured as the ratio of total costs to total income | % |

(continued)

**Table 10** (continued)

| Variable name | Source | Description | Measurement unit |
|---|---|---|---|
| Earnings | Bankscope | Proxy for earnings of a venture's bank measured as the return on average equity | % |
| Liquidity | Bankscope | Proxy for liquidity of a venture's bank measured as liquid assets to deposits and short-term funding | % |
| Sec./ear. assets | Bankscope | Proxy for liquidity of a venture's bank measured as securities to total earning assets | % |
| Fees/interest | Bankscope | Non-interest income divided by net interest income | % |

## References

Akerlof, G.A.: The market for lemons: Quality uncertainty and the market mechanism. Q. J. Econ. **84**(3), 488–500 (1970)

Anna, A.L., Chandler, G.N., Jansen, E., Mero, N.P.: Women business owners in traditional and non-traditional industries. J. Bus. Ventur. **15**(3), 279–303 (2000). doi:10.1016/S0883-9026(98)00012-3

Arenius, P., Autio, E.: Financing of small businesses: are Mars and Venus more alike than different? Ventur. Capital **8**(2), 93–107 (2006). doi:10.1080/13691060500433793

Beckman, C.M., Burton, M.D., O'Reilly, C.: Early teams: the impact of team demography on VC financing and going public. J. Bus. Ventur. **22**(2), 147–173 (2007). doi:10.1016/j.jbusvent.2006.02.001

Belleflamme, P., Lambert, T., Schwienbacher, A.: Crowdfunding: tapping the right crowd. J. Bus. Ventur. **29**(5), 585–609 (2013). doi:10.1016/j.jbusvent.2013.07.003

Berger, A., Udell, G.: The institutional memory hypothesis and the pro-cyclicality of bank lending behavior. J. Financ. Intermediation **13**, 458–495 (2004)

Berger, A.N., Udell, G.F.: The economics of small business finance: the roles of private equity and debt markets in the financial growth cycle. J. Bank. Finance **22**(6–8), 613–673 (1998)

Block, J., Sandner, P., De Vries, G.: Venture capital and the financial crisis: an empirical study across industries and countries. In: Cumming, D. (ed.) The Oxford Handbook of Venture Capital. Oxford University Press, Oxford (2010). Chap. 3

Bradford, C.S.: Crowdfunding and the federal securities law. Columbia Bus. Law Rev. **2012**(1), 1–150 (2012). ISBN 1000142405274. doi:1916184

Brown, M., Degryse, H., Hower, D., Penas, M.F.: How do banks screen innovative firms? Evidence from start-up panel data. ZEW Discuss. Pap. **12–032**, 1–37 (2012)

Cassar, G.: The financing of business start-ups. J. Bus. Ventur. **19**(2), 261–283 (2004)

Chandler, G.N., Hanks, S.H.: An examination of the substitutability of founders human and financial capital in emerging business ventures. J. Bus. Ventur. **13**(5), 353–369 (1998). doi:10.1016/S0883-9026(97)00034-7

Coleman, S.: Access to capital and terms of credit: A comparison of men- and women-owned small businesses. J. Small Bus. Manage. **38**(3), 37 (2000)

Cosh, A., Cumming, D., Hughes, A.: Outside entrepreneurial capital. Econ. J. **119**(1), 494–533 (2009)

De Buysere, K., Gajda, O., Kleverlaan, R., Marom, D.: A Framework for European Crowdfunding, Technical report, European Crowdfunding Network (2014)

de Meza, D., Webb, D.C.: Too much investment: a problem of asymmetric information. Q. J. Econ. **102**(2), 281–292 (1987)

Dell'Ariccia, G., Marquez, R.: Information and bank credit allocation. J. Financ. Econ. **72**, 185–214 (2004)

Diamond, D.W.: Financial intermediation and delegated monitoring. Rev. Econ. Stud. **51**(3), 393–414 (1984)

Gompers, P., Lerner, J.: The venture capital revolution. J. Econ. Perspect. **15**(2), 145–168 (2001)

Gorman, M., Sahlman, W.: What do venture capitalists do? J. Bus. Ventur. **4**(4), 231–248 (1989). doi:10.1016/0883-9026(89)90014-1

Gupta, A.K., Sapienza, H.J.: Determinants of venture capital firms' preferences regarding the industry diversity and geographic scope of their investments. J. Bus. Ventur. **7**(5), 347–362 (1992). ISBN 08839026. doi:10.1016/0883- 9026(92)90012-G

Haines, G.H., Madill, J.J., Riding, A.L.: Informal investment in Canada: financing small business growth. J. Small Bus. Entrepreneurship **16**(3–4), 13–40 (2003). doi:10.1080/08276331.2003.10593306

Hall, J., Hofer, C.W.: Venture capitalists' decision criteria in new venture evaluation. J. Bus. Ventur. **8**(1), 25–42 (1993). ISBN 08839026. doi:10.1016/0883-9026(93)90009-T

Harris, M., Raviv, A.: The theory of capital structure. J. Finance **46**(1), 297–355 (1991). ISBN 00221082. doi:10.2307/2328697

Hemer, J.: A snapshot on crowdfunding. Working Paper Series: Firms and Region—Fraunhofer ISI No. 2 (2011)

Hempell, H.S., Kok, C.: The impact of supply constraints on bank lending in the euro area—crisis induced crunching? European Central Bank Working Paper Series No. 1262 (2010)

Hornuf, L., Schwienbacher, A.: Crowdinvesting—Angel investing for the masses? In: Handbook of Research on Venture Capital, vol. 3. Business Angels. Edward Elgar Publishing Ltd., Cheltenham (2014)

Hosmer, D.W., Lemeshow, S.: Applied Logistic Regression, 3rd edn. Wiley, Hobo-ken, NJ (2012). ISBN 9780471654025

Jensen, M.C., Meckling, W.H.: Theory of the firm: managerial behavior, agency costs and ownership structure. J. Financ. Econ. **3**(4), 305–360 (1976). doi:10.1016/0304-405X(76)90026-X

Jiménez, G., Ongena, S., Saurina, J., Peydró, J.-L.: Credit supply and monetary policy: identifying the bank balance-sheet channel with loan applications. Am. Econ. Rev. **102**(5), 2301–2326 (2012)

Jiménez, G., Ongena, S., Saurina, J., Peydró, J.-L.: Hazardous times for monetary policy: what do twenty-three million bank loans say about the effects of monetary policy on credit risk? Econometrica **82**(2), 463–505 (2014)

Lerner, M., Brush, C., Hisrich, R.: Israeli women entrepreneurs: an examination of factors affecting performance. J. Bus. Ventur. **12**(4), 315–339 (1997). ISBN 0883-9026. doi:10.1016/S0883-9026(96)00061-4

Mason, C., Harrison, R.: Why 'business angels' say no: a case study of opportunities rejected by an informal investor syndicate. Int. Small Bus. J. **14**(2), 35–51 (1996). ISBN 9781845424794. doi:10.1177/0266242696142003

Mason, C., Rogers, A.: What do investors look for in a business plan? An exploratory analysis. In: Deakins, D., Jennongs, P., Mason, C. (eds.) Entrepreneurship in the 1990s, pp. 29–46. Paul Chapman Publishing, London (1997)

Michaelas, N., Chittenden, F., Poutziouris, P.: Financial policy and capital structure choice in U.K. SMEs: empirical evidence from company panel data. Small Bus. Econ. **12**(2), 113–130 (1999). doi:10.1023/A:1008010724051

Mollick, E.: The dynamics of crowdfunding: an exploratory study. J. Bus. Ventur. **29**(1), 1–16 (2014). doi:10.1016/j.jbusvent.2013.06.005

Mollick, E.R.: Swept away by the crowd? Crowdfunding, venture capital, and the selection of entrepreneurs. SSRN Electr. J. (2013)

Myers, S.C., Majluf, N.S.: Corporate financing and investment decisions when firms have information that investors do not have. J. Financ. Econ. **13**(2), 187–221 (1984). doi:10.1016/0304-405X(84)90023-0

Neider, L.: A preliminary investigation of female entrepreneurs in Florida. J. Small Bus. Manage. **25**, 22–29 (1987)

Petersen, M.A., Rajan, R.G.: The benefits of lending relationships: Evidence from small business data. J. Finance **49**(1), 3–37 (1994)

Petersen, M.A., Rajan, R.G.: Does distance still matter: the information revolution in small business lending. J. Finance **57**, 2533–2570 (2002)

Popov, A., Udell, G.F.: Cross-border banking, credit access, and the financial crisis. J. Int. Econ. **87**(1), 147–161 (2012). doi:10.1016/j.jinteco.2012.01.008

Puri, M., Rocholl, J., Steffen, S.: Global retail lending in the aftermath of the US financial crisis: distinguishing between supply and demand effects. J. Financ. Econ. **100**, 556–578 (2011)

Rajan, R.G.: Insiders and outsiders: the choice between informed and arm's-length debt. J. Finance **47**, 1367–1400 (1992)

Riding, A.L., Swift, C.S.: Women business owners and terms of credit: Some empirical findings of the Canadian experience. J. Bus. Ventur. **5**(5), 327–340 (1990). doi:10.1016/0883-9026(90)90009-I

Robb, A.M., Robinson, D.T.: The capital structure decisions of new firms. Rev. Financ. Stud. **27**(1), 153–179 (2014)

Schwienbacher, A.: Financing the business. In: Baker, T., Welter, F. (eds.) The Routledge Companion to En-trepreneurship. Routledge, London (2013)

Schwienbacher, A., Larralde, B.: Crowdfunding of small entrepreneurial ventures. In: Handbook of Entrepreneurial Finance. Oxford University Press (2010). ISBN forthcoming. doi:10.2139/ssrn.1699183

Stiglitz, J.E., Weiss, A.: Credit rationing in markets with imperfect information. Am. Econ. Rev. **71**(3), 393–410 (1981)

Storey, D.J.: New firm growth and bank financing. Small Bus. Econ. **6**(2), 139–150 (1994)

Strotmann, H.: Entrepreneurial survival. Small Bus. Econ. **28**(1), 87–104 (2006). doi:10.1007/s11187-005-8859-z

Sweeting, R.: UK venture capital funds and the funding of new technology-based businesses: Process and relationships. J. Manage. Stud. **6**(November), 601–622 (1991). ISBN 0022-2380. doi:10.1111/j.1467-6486.1991.tb00982.x

Titman, S., Wessels, R.: The determinants of capital structure choice. J. Finance **43**(1), 1–19 (1988). ISBN 00221082. doi:10.1111/j.1540-6261.1988.tb02585.x

Uchida, H., Udell, G.F., Yamori, N.: Loan officers and relationship lending to SMEs. J. Financ. Intermediation **21**(1), 97–112 (2012)

Verheul, I., Thurik, R.: Start-up capital: "Does gender matter?". Small Bus. Econ. **16**(4), 329–346 (2001). ISBN 10.1023/A:1011178629240. doi:10.1023/A:1011178629240

Zacharakis, A.L., Meyer, G.D.: A lack of insight: ao venture capitalists really understand their own decision process? J. Bus. Ventur. **13**(1), 57–76 (1998). ISBN 0883-9026. doi:10.1016/S0883-9026(97)00004-9

## Author Biographies

**Daniel Blaseg** is expert for startup financing and crowdfunding. Responsible for the business development and venture capital section of mayerhöfer and co, he consulted and executed different financing rounds and exits in the area of FinTech, eCommerce and eMobility over the last years. Moreover, Daniel is CFO of Innovestment, one of the oldest and most successful German crowdfunding platforms. After graduating at the Frankfurt School of Finance and Management (Master of Finance), he is now a doctoral student at Goethe-University Frankfurt in the marketing department with Prof. Dr. Bernd Skiera.

**Michael Koetter** is a Professor of Banking and Finance at Frankfurt School of Finance and Management since 2012 and director of the Research Centre “Financial Intermediaries and the Real Economy (FIRE)”. Before joining Frankfurt School, Michael held positions at the University of Groningen and the Boston Consulting Group and visited business schools in the US, France, and Mexico. He is or was a guest researcher at Deutsche Bundesbank, Sveriges Riksbank, and the ECB, and served as the acting head of the Financial Markets department at the Institute for Economic Research (IWH) in Halle until January 2016. His current research concerns the consequences of unorthodox monetary policy, Finance 4.0, risk taking and competition, and international banking. His research was funded by the Netherlands Organization of Scientific Research (NWO), the Leibniz Gesellschaft, and science foundations of the financial industry. It appeared in both general interest and field journal and he is regularly commenting in the media.

# How Peer to Peer Lending and Crowdfunding Drive the FinTech Revolution in the UK

**Susanne Chishti**

**Abstract** An overview of the booming alternative finance sector in the UK which generated more than £3.2 billion in investments and loans in 2015, an increase of more than 80 % over 2014. Susanne Chishti, CEO of FINTECH Circle describes the business models and drivers behind the industry's success and highlights UK's leading peer to peer lending and crowdfunding platforms.

**Keywords** Alternative Finance · Alternative Lending · Peer to Peer - P2P · FinTech · Crowdfunding · UK P2P Platforms

## 1 Overview of the Alternative Finance Sector in the UK

Currently the largest industry in alternative finance, peer to peer lending has experienced both headlining successes and serious challenges during its early development. The last five years have seen most of the main players in the UK launch their investment platforms with a sustained customer uptake moving alternative finance further towards the mainstream. In 2015 the volume of P2P business lending reached a record £1,490 m.[1] It is not uncommon for P2P platforms to offer returns of over 10 % to savers looking for better returns than are currently offered by high street banks[2] after years of record-breaking low interest rates. Borrowers looking for loans are now able to find new avenues and affordable rates through P2P lending platforms.

[1] http://www.nesta.org.uk/sites/default/files/pushing_boundaries_0.pdf.

[2] http://www.thisismoney.co.uk/money/diyinvesting/article-3062370/The-investment-trusts-backing-lending-platforms-10-return.html.

S. Chishti (✉)
FINTECH Circle, London, UK
e-mail: info@FINTECHCircle.com

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_4

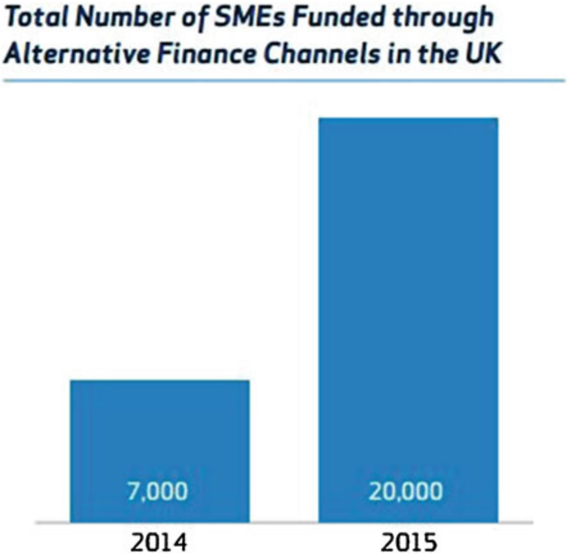
Although accounting for a smaller percentage of the market, equity crowdfunding platforms have become one of the first options for many startups looking to raise funds from individual investors in exchange for shares. With new raises frequently being reported by the media crowdfunding is also experiencing high growth. Peer to peer lending is competing with banks by matching up lenders with borrowers without the cost of branches or the dependency on old legacy systems. By using the web they cut out the middleman and can offer better rates to both sides. In response to an increasing demand for better financial services, FinTech has continued to provide cost effective platforms as an alternative to traditional banking. Driven by innovative technology, alternative finance in the UK is experiencing some of the highest growth rates in the world.

With a broad range of business ventures successfully financed crowdfunding continues to make the headlines with companies and individuals who would have otherwise struggled to find investment. The type of companies found on these platforms range from worthwhile causes to commercially driven startups and SMEs. Crowdfunding websites have created a platform where equity can be offered to larger groups of investors who share the financial risk. The opportunities driven by the crowd model mean that the availability of smaller investments open up the market to a broader range of individuals wanting to buy shares whilst at the same time providing the companies with both a public funding route and potentially a new customer based (if new shareholders turn into customers as well (especially relevant for Business to Consumer (B2C)) propositions).

Although peer to peer lending and crowdfunding continue to offer critical support to the 5.4 million UK based SMEs[3] there has been limited awareness about these new options available to them. Most small businesses look for finance from the ‘big four’ banks, HSBC, Barclays, Lloyds Banking Group and RBS Group and are not always able to find the best deals. Borrowers try to negotiate their way through a labyrinth of hidden fees and are regularly unsuccessful with their applications. The Small Business, Enterprise and Employment Act included a banking referral legislation in the UK where details of businesses declined for bank loans will be recommended to alternative finance platforms. In the light of this RBS and Santander have already started referring borrowers to P2P platforms.

FinTech has taken central stage in the UK as a world leader of financial innovation proving itself to be effective in unbundling bank services by providing better

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/467443/bpe_2015_statistical_release.pdf.



value and a better customer experience. Preferable rates and increased access are not the only factors to be taken into account when looking at previous growth figures. The ease in which interested parties can interact with these platforms, the transparency of the deals available and the speed at which things can be achieved are all considerations that are attracting individuals and institutions to this sector. FinTech companies have cherry picked and developed these core banking services and as a result lending, borrowing and investing have recently seen some of the most significant changes in living memory. Central to alternative finance, the continued performance of P2P lending and crowdfunding will determine the future of this sector.

As both of these platforms adapt to the rapidly changing landscape of finance a wider FinTech ecosystem is developing around them. For those who can meet the challenges ahead to support the demand for continued growth, advanced credit scoring abilities will provide new opportunities for those who are able to assess a wider proportion of potential borrowers. Rather than only relying on traditional credit scoring calculations, FinTech companies are harnessing an abundance of new information by using software developed for big data and their ability to develop improved algorithms to automatically match lenders with borrowers. Newly developed credit scoring models and a high level of borrower vetting have kept Zopa and RateSetter defaults at some of the lowest rates in the lending industry, though unlike a bank savings account there is no FSCS coverage which insures most UK savings accounts up to £85,000.[4]

[4] http://www.fscs.org.uk/what-we-cover/products/banks-building-societies/.

Since 2015 the FCA has regulated P2P lending sites to ensure transparency and that they have the funds to dampen risk exposure to lenders. Zopa has a Safeguard fund to repay investors in the event of a borrower defaulting on their loan. Their fund is in a trust held by a not-for-profit organisation. RateSetter was the first to provide a 'provision fund' and their website states that no investor has lost a penny since their launch in 2010. With an investment spread across multiple borrowers, defaults at these rates become manageable with repayment funds in place. However both of these young industries have only been operating during times of ultra low inflation which can be seen as giving them favourable terms in comparison to their main competitors. The limitations of the P2P industry will continue to be tested. Lending Club in the USA has seen their CEO stand down over questionable sales practices[5] highlighting the potential dangers of a burgeoning industry driven by investor demand for high-yielding fixed income assets, while the difficulties of forecasting its performance during times of higher interest rates and inflation becomes a crucial issue for the future.

## 2 UK's Leading P2P and Crowdfunding Platforms

*UK's top six platforms are briefly portrayed below:*

### 2.1 Funding Circle

P2P lender Funding Circle has been reported to be trebling its loan volumes to SMEs every year.[6] Founded in 2010 by Samir Dasai, Funding Circle has lent to small businesses globally: $2 billion to more than 15,000 businesses.[7] Their business model includes the option for investors and borrowers to trade parts of an existing loan and Funding Circle takes a 0.25 % fee on each sale.[8] They were the first peer to peer lending site in the country to focus solely on loans to businesses and are currently the fifth largest net lender to small businesses.[9]

[5] http://www.ft.com/cms/s/0/22559850-15d9-11e6-b197-a4af20d5575e.html#axzz48MJxuygb.

[6] http://www.standard.co.uk/business/markets/funding-circles-samir-desai-after-the-banking-cowboys-here-comes-the-new-wave-loan-arranger-9082657.html.

[7] https://www.fundingcircle.com/us/about/press/.

[8] https://www.fundingcircle.com/lenders/terms.

[9] https://www.fundingcircle.com/blog/press/.

## 2.2 Zopa

Launched in 2005 Zopa was the first peer to peer lending site founded five years before most of its competitors. Founded in the UK it has a strong international presence and is now Europe's largest and oldest P2P lending organisation.[10] Originally a consumer loans company Zopa have now teamed up with UBER to create a market for drivers who would like to buy their own car. Challenger bank Metro have also partnered with Zopa to enter into the P2P market by using the platform to lend to customers. This could be seen as a signal to institutional lenders and investors that alternative finance is here to stay.

## 2.3 RateSetter

Launched in 2010 RateSetter co-founders Peter Behrens and Rhydian Lewis have lent over £1b to date.[11] Now partnered with the British Business Bank (BBB) they lend through RateSetter to those needing loans for business purposes. They are seen as one of the lowest risk P2P lenders with a strict vetting policy for borrowers. RateSetters provision fund currently stands at over £17,993,000[12] and lenders can start with as little as £10. Also typical of FinTech platforms RateSetter is a great example of a website design and functionality that gives the user an experience matched with the ease and simplicity of their business model.

## 2.4 Crowdcube

Darren Westlake and Luke Lang established the world's first equity crowdfunding platform in 2011. As a platform it aims to enable anyone to buy equity in unlisted UK registered businesses, investing as little as £10. If the business fails to raise the set target then no funds are taken from investors. In the beginning their average raise for a business was a little over £100,000 in their first two years, though the average now is around £500,000.[13]

[10] https://en.wikipedia.org/wiki/Zopa.

[11] http://www.crowdfundinsider.com/2016/01/80641-ratesetter-tops-1-billion-claims-record-pace-for-uk-marketplace-lending/.

[12] https://www.ratesetter.com/invest/everyday-account/protection.

[13] http://www.wired.co.uk/news/archive/2015-07/08/crowdcube-darren-westlake-wired-money-2015.

### 2.5 Seedrs

Seedrs was founded in 2012 by Jeff Lynn and Carlos Silva as part of an MBA project which soon went on to raise £1.3 million.[14] Also based on the "all or nothing" equity crowdfunding business model, Seedrs acts as single legal shareholder on behalf of all investors in a deal (via a nominee structure). In 2015 the combined forces of the alternative finances sector came together with the lending site Assetz who raised £3 million by equity fundraising with Seedrs.[15]

### 2.6 SyndicateRoom

SyndicateRoom requires that businesses wanting to raise funds have already secured investment from experienced sources. Founded by Gonçalo de Vasconcelos and Tom Britton and launched in 2013 they are the first to crowdfund an IPO. Raising over £10,000,000 of investment for companies in the UK during their first year[16] they have helped over 30 businesses raise on average over £600,000.[17]

## 3 Business Models and Drivers Behind the Success of Peers to Peer Lending

P2P lending accounts for around 90 % of the alternative finance market.[18] With the world's first company launching in the UK, London has continued to play a central role with eye opening growth rates over the last 5 years. The HM Treasury's ongoing efforts to create more competition for the banking sector has included tax breaks and regulation favouring new entrants into the alternative finance market who are now able to challenge the incumbents. The most successful models

[14] http://www.crowdfundinsider.com/2013/12/29179-seedrs-closes-2013-high-note-3-million-raised-december/.

[15] http://www.crowdfundinsider.com/2015/04/66388-seedrs-leads-the-way-in-raising-capital-for-other-crowdfunding-platforms/.

[16] https://en.wikipedia.org/wiki/SyndicateRoom.

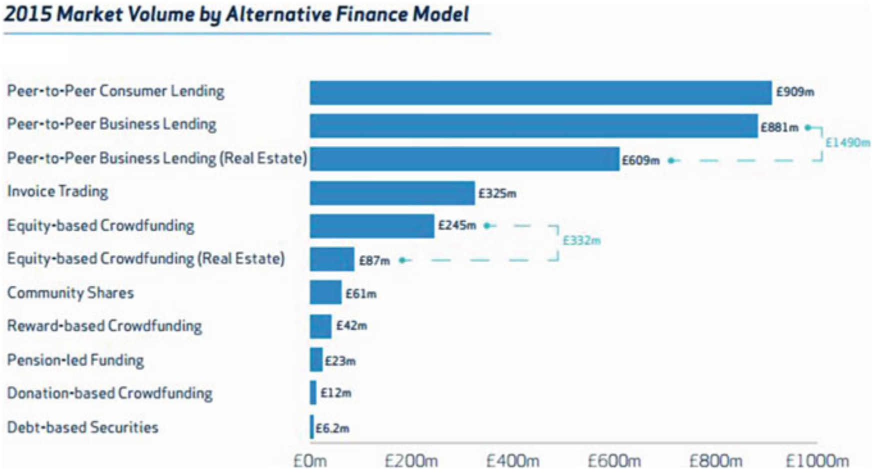
[17] http://www.businessweekly.co.uk/tech-trail/funders/businesses-can-now-bank-diverse-range-funding-options.

[18] http://www.4thway.co.uk/news/uk-leading-the-way-on-p2p-lending/.

developed in the P2P lending space have produced the ‘Big Three’ - Zopa, Funding Circle and RateSetter. Their new title coined by the industries press is reminiscent of the ‘Big Four’ and although maybe tongue in cheek it is a reminder of where P2P lending is potentially heading.

The options on offer to lenders have diversified over recent years. Most commonly a lender is able to choose who they lend to and at a fixed rate set on a borrowers request for a loan. Also there is the option to lend via a reverse auction for a loan where the investor offering the lowest rates to a borrower is successful. It is also possible that borrowers can be vetted by the lender for each individual loan. P2P lending sites can operate a marketplace lending model where lenders are offered basic information about the loans on offer that are underwritten by the platform itself and are then given the rate already agreed by the borrower. Similarly the platform can package interest products from existing loans with annual rates and the returns being paid at the end of each year rather than on a monthly basis. An environment in which loans can be packaged, bought and sold enables a market where lenders can cash in early but only if they can find a buyer or are willing to pay an early withdrawal/exit fee.

P2P lending first became popular with unsecured consumer loans and now includes business lending with the option to be secured by the borrower’s property. Whether secured or unsecured, this offers SME lending more flexibility to both investor and borrower. Previously SMEs attempting to find deals from a high street bank were up against a lack of transparency with hidden borrowing fees to uncover and understand, often being unexpectedly charged even after committed due diligence. The peer to peer technology based lending model has harnessed data in ways the legacy systems of banks have not been able to deliver. As a result P2P loan applications are processed at higher speeds and with more clarity on the agreements. With this increased access to finance SME lending has reached a pivotal moment in banking history as P2P platforms have claimed their stake in the lending market and now institutions notorious for being slow moving are starting to take notice.



The foundation of P2P lending was originally built on the principle of facilitating large groups of individuals (peers). Site owners have started to market this concept less as new products become available that make the peer to peer title less relevant, though this is one of the key values that separates them from their main competitors. The technology that makes P2P lending work serves as a platform where investors and businesses can interact on a scale that offers the advantages of choice and diversity. This has driven the widely publicised success of this model and peer to peer loans are now accepted as an asset class of their own. Institutions have had the experience with positive results in raising funds, investing and even launching their own P2P lending platforms. The endorsement and cash flow provided by institutional investment has been of great benefit to this developing industry but it could be possible that if the large amount of small investors who are still driving this phenomenal growth are overshadowed by the power of institutional shareholders, P2P lending could potentially move towards the old models it has successfully disrupted.

In April 2016 peer to peer investments became eligible for individual Savings Accounts (ISAs), tax free savings vehicles for UK residents. After a consultation that looked at potential concerns such as problems that could arise from P2P platforms not legally owning the loans they originate, the majority of the contributors did not recognise any undue risk and now peer to peer lenders will be able to act as ISA managers. There have been well documented issues in recent years about loan originators not having the same interests as direct lender/borrower relationships. In the case of peer to peer lending the lifeblood of these facilitators depend on their valued transparency and brand reputation which some argue holds their main interests firmly with their customers. Also Zopa and Funding Circle are both institutionally funded at about 30 %,[19] the up side to this being the level of scrutiny they provide for other investors to follow can inspire confidence that reliable due diligence will have been done on the loan originations.

With peer to peer loan origination the principle risk is passed on from borrower to lender which also leaves the lender with exposure to agency risk from the P2P platform. With provision funds and a healthy default track record there can be a common misconception by inexperienced lenders that taking their savings from a bank to a peer to peer investment with a higher rate will not be without higher risks. Without a substantial track record lenders can be challenged to assess agency risk on 5 year commitments when the industry itself has not been in existence for much longer. Since 2010 interest rates have remained consistently low which has favoured alternative finance against the banks. This is something that will inevitably change at some point. It will be interesting to observe the impact of rising interest rates on the P2P sector.

[19] http://www.altfi.com/article/1140_key_talking_points_from_p2p_ceo_breakfast.

Alternative finance paired with London's FinTech sector has followed in the footsteps of the UK's centuries old global financial industry. Between 2012 and 2014, P2P lending in the UK has accounted for approximately 90 % of the alternative finance market while Europe's peer to peer lending industry made up 59 % of the market according to a Cambridge Judge Business School report released in 2015.[20] Collectively the European alternative finance industry increased its transaction volumes by six times in this three year period, though during 2015 alone the UK market is expected to grow over five times than is forecast for the rest of Europe.[21] With a thriving FinTech industry and a strong financial heritage the UK is set to carry on its leading position within Europe into the foreseeable future.

In 2013 Funding Circle launched in the US and partnered with San Francisco based business lender Endurance Lending Network Inc. which now trades under the Funding Circle name. Only a few blocks away one of America's earliest and most successful peer to peer firms Lending Club has moved with stealth towards increased institutional lending. The success of Lending Club's IPO has been a game changer for the global Fintech sector. In 2015 institutional investors provided approximately 45 % of Lending Club's funding.[22] The early days of alternative finance being seen as something that was most likely to be a one off experiment in social economics now seems like a distant memory and an industry with such a strong start in life should be able to weather the storms ahead routinely associated with our global cyclical economy.

In the UK the extra money that institutions have injected into P2P business lending has boosted its performance and is overtaking its original counterpart P2P consumer lending. With larger loans and the attraction of higher returns new entrants have entered the business lending market. Without much competition from banks who are still notoriously cautious in lending to SMEs there are now more business lending platforms than those lending to consumers. Together with the government's willingness to encourage SMEs with new incentives for both new businesses and alternative finance, FinTech has been able to create new automated systems unburdened by archaic over-complicated legacy systems and increased bank regulations. SMEs can now raise funds via this technology within a fraction of the time than banks can offer. The wider implications on the economy during these critical times are positive as the widening ecosystem of FinTech companies who are building and maintaining these platforms are also attracting record levels of investment into the UKs financial technology services.

[20] Cambridge Alternative Finance: Moving Mainstream 2015.

[21] Cambridge Alternative Finance: Moving Mainstream 2015.

[22] http://www.ft.com/cms/s/0/9e966ff2-ed48-11e5-9fca-fb0f946fd1f0.html.

## 4 Business Models and Drivers Behind the Success of Equity Crowdfunding

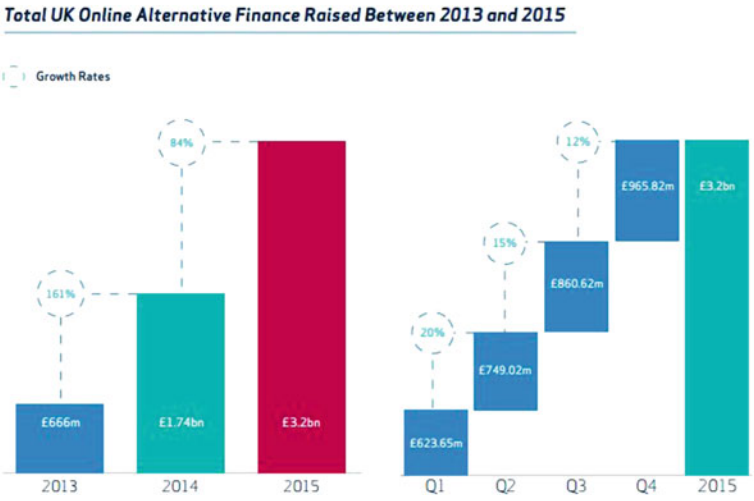
Crowdfunding platforms have reached larger groups of investors from a wide range of backgrounds, otherwise inaccessible to entrepreneurs and early stage companies. Originally a platform used most commonly by SMEs, bigger companies are also using this platform to pitch for funds. Innovation agency. Nesta reported that equity crowdfunding in the UK had raised £332 m in 2015[23] This comes at a time when raising funds for new business ideas would have been impossible for many without crowdfunding websites to publicise their proposals to the large number of potential investors that these platforms attract.

Historically business angels and early stage venture capitalists have financed the best funding rounds when banks have not been as open to supporting early stage businesses. At first funding rounds many startup founders still rely on friends and family to invest in them during their early days. With an increase in the access to funds and equity, crowdfunding has encouraged new entrepreneurs to launch companies contributing towards economic growth. That is a good example where the FinTech revolution clearly benefits all sectors of our economy and not just financial services.

The funding process starts with a brief presentation of the business raising funds posted on one of several crowdfunding sites along with the founder's background and their financial projections. The crowd is then invited to invest within a number of weeks to close the entire raise. These campaigns are not aimed exclusively at sophisticated investors and are in general inherently more risky than investments on peer to peer lending sites. The UK Crowdfunding Association, was formed in 2012 with the aims of promoting crowdfunding as a valuable and viable way for UK business projects or ventures to raise funds, to be the voice of all crowdfunding businesses in the UK (donations, loans and equities) to the public, press and policymakers and to publish a code of practice that is adopted by UK crowdfunding businesses.

Most startups do not succeed in the long run. Disclaimers on crowdfunding sites warn would be investors of the risks and suggest not to part with more money that can be afforded to be lost. Business angels and venture capitalists usually only expect a small percentage of their investments to create their overall return. For example, it is expected that on average only one or two companies out of ten investments will generate a healthy return. This strategy can be taken further with crowdfunding allowing investors to back a larger number of companies with smaller investments as a way to manage risk. Unlike peer to peer lending you will not be able to cash in an investment for a number of years, if at all. If the company

[23] http://www.nesta.org.uk/sites/default/files/pushing_boundaries_0.pdf.


Total UK Online Alternative Finance Raised Between 2013 and 2015

makes a profit this money is usually reinvested back into the company and there is no obligation to pay dividends. The best opportunity for an investor to sell their shares often comes when the company is sold to a trade buyer or is floated via an Initial Public Offering (IPO) on a securities exchange. These exit options combined with the high risks of investing into early stage companies are commonly known among experienced investors. What also needs to be taken into account is that dilution in follow-on rounds (all companies have to go through several funding rounds before they exit) is almost a certainty for early stage investors.

When a business goes forward to another round of funding, it issues new shares which lower the percentage of the company an original shareholder owns. Preferential rights can also be granted to new, larger shareholders and individuals closely associated with the company which will have a negative effect on shares previously bought. Thus crowdfunding investors need to be aware in which share class they are investing in and the various rights they have in comparison to other investors in other share classes. On occasion crowdfunding sites themselves are able to act as a representative of the investors that can help towards maintaining pre-emtion and voting rights and can prevent the over dilution of shares. In general, the transparency of alternative finance and crowdfunding platforms has been good, but in the case of shareholder rights extra due diligence is required.

The risks of crowdfunding such as the dilution of shares, illiquidity; lack of dividends and potential loss have been presented with clear disclaimers on the main equity crowdfunding sites as hopeful investors attempt and sometimes succeed in making many times their invested amount. What is unclear is to what extend the majority of crowdfunding investors really reads and fully appreciates the legal meaning of these risk disclaimers. The last thing this prospering new sector needs is a mis-selling scandal which has so heavily tarnished the image and reputation of established players. Quite often backers simply enjoy the opportunity to help a worthy cause, or are happy to become involved in a multitude of interesting projects now accessible online. The diversity of investors attracted to the online deals is at the grass roots of the business model. Its growing popularity has not gone unnoticed by institutional investors as more activity takes place on these platforms. With inherently higher risks the returns on a successful equity investment can also be significantly higher than opportunities found on P2P lending sites.

In another development that would appear to endorse crowdfunding, corporate finance houses in the UK are also using equity crowdfunding sites to raise early stage funding rounds. With some of these deals having already received institutional funding, individuals have been able to invest smaller sums with the same shareholder rights. Independent broker FinnCap launched its own equity crowdfunding site available for public and private companies to use, shortly after its client Chapel Down became the first listed company to successfully raise funds via crowdfunding. Mill Residential recently became the first crowdfunded company to float on AIM after raising over £2 million on SyndicateRoom[24] signifying the potential for larger businesses to not only raise funds but to gain public awareness during highly publicised rounds that can generate positive publicity for raises that might have otherwise remained unknown.

With crowdfunding sites attracting high numbers of visitors on a daily basis a posting can create exactly the type of awareness and recognition a company needs even before any money has changed hands. Information on who has raised how much and how fast travels across social media and word of mouth in real time. The press and popular blogs frequently publicise big wins and points of interest which all link back to the sites and funding campaigns themselves. In cases where a campaign is successful, crowdfunding sites on occasion will promote the result validating further the interests of the companies and investors. When it comes to marketing a crowdfunding campaign on places like Twitter the FCA have strict rules and social media guidelines on financial promotion.[25]

In order to succeed in public, entrepreneurs have to lay open the details of their business and financial forecasts which undoubtedly will be reviewed by their competitors, suppliers and clients which often are also part of the "crowd". The realities of creating a successful fund raising campaign are that it requires pre-agreed investors who invest as soon as the campaign is live to create momentum and careful management as articulated very well by an article of Sian's Plan.[26]

As a small team raising £100,000 for a consumer led business, equity crowdfunding became the chosen route to start Sian's Plan. Preparation for the campaign started a month before going live which involved connecting with the growing community of successful campaigners and building a database of potential investors and influential contacts within their market. A widely held opinion was that if 35 %

[24] https://www.syndicateroom.com/about-us/success-stories/mill-residential-reit.

[25] http://www.fca.org.uk/static/documents/finalised-guidance/fg15-04.pdf.

[26] http://allabout.siansplan.com/hacked-way-100k-crowdfunding.

of the raise was achieved in the first two weeks this would signal that the full amount would follow. With Sians Plan they managed 40 % during this time but had to work overtime to revive the raise after incoming investments dropped off the charts half way through their 90 day time window. A daily routine of engaging posts on Twitter, Facebook, LinkedIn and email created some momentum and around 50 % of investments came from social media activities. With money coming in and lots of visible marketing efforts the crowd is more likely to be inspired by a busy and popular campaign.

Rapid growth and the publicity generated by ongoing successes, usually in the form of numerous large raises done in record time has led to concern that some companies could be overvalued. This can be overcome by funding rounds being endorsed at the beginning by recognised investment companies or angel networks whilst still maintaining the unique advantages of a crowd led platform. Overvaluing startups with too optimistic projections is a frequent mistake by the company's founders and management teams risking a down-round the next time they raise money leading to dissatisfied investors and bad publicity. Experienced business angels and VCs will always take the valuation into consideration when analysing the risk-adjusted returns. For the many individuals who do not have professional experience, this aspect of investing is not as transparent and the importance of understanding valuations and projections is a good example of why seeking independent financial advice would be a worthwhile endeavour for the uninitiated investor wanting to become involved in equity crowdfunding as a long term investment strategy.

One of the most significant developments in alternative finance in the UK is the Innovative Finance ISA announced during the 2015 budget. A consultation has established that equity crowdfunding can overcome issues such as illiquidity and become ISA eligible. These eagerly anticipated new ISA products have seen delays since the initial start date of April 2016. Many applications that have been submitted to the Financial Conduct Authority (FCA) are still waiting to be processed and may be months away from approval.[27]

Government support for FinTech initiatives has been strong in the alternative finance arena in tandem with their focus on helping SME businesses drive the UK economy. The Seed Enterprise Investment Scheme,[28] (SEIS) and the Enterprise Investment Scheme (EIS)[29] both support the funding of SMEs by providing attractive tax breaks in the form of income tax relief for private investors who take the risks of investing in early stage companies. A clear indication that the government wants to create more competition with alternative sources of financial support for businesses.

[27] http://www.moneysavingexpert.com/news/savings/2016/04/major-peer-to-peer-lenders-still-months-off-unveiling-ifisas-amid-approval-backlog-.

[28] http://www.gov.uk/seed-enterprise-investment-scheme-background.

[29] http://www.gov.uk/government/publications/the-enterprise-investment-scheme-introduction.

With no shortage of support from individuals, institutions and the government, equity crowdfunding will continue to grow into the foreseeable future. The ecosystem of services provided by a burgeoning FinTech industry has consolidated and is attracting the best talent to the UK challenging global hot spots like Silicon Valley. As with any industry experiencing sustained accelerated growth the main challenges ahead are focused on not becoming a victim of its own success. Equity crowdfunding models will be tested as the industry moves into the future with wider sections of society using this platform. The FCA will continue to monitor the treatment of investors as more inexperienced individuals buy shares. Balanced against the increasing influence of institutional activity, equity crowdfunding can continue to enjoy the diversity of the crowd and businesses can rely on a new legitimate source of finance.

In summary, with a thriving FinTech industry and a strong financial heritage the UK is set to carry on its leading position within Europe into the foreseable future while the growth of other FinTech hubs and Alternative Finance Centres across Europe Cdn only be encouraged to ensure that the European Financial Services sector and its customers Cdn fully benefit form the “FinTech Revolution”.

## Author Biography

**Susanne Chishti** is the CEO of FINTECH Circle, Europe’s 1st Angel Network focused on fintech opportunities and the FINTECH Tours, Chairman of FINTECH Circle Innovate and Co-Editor of the Finance Bestseller “The FINTECH Book”—the 1st Crowd-Sourced Book on Fintech globally. Susanne has been recognised in the European Digital Financial Services ‘Power 50’ 2015, an independent ranking of the most influential people in digital financial services in Europe. She was selected as one of the 100 leading Women in FINTECH and top 15 FINTECH UK twitter influencers.

Susanne is an entrepreneur and investor with strong FINTECH expertise and keynote speaker at leading global finance and fintech conferences. Mentor, Judge and Coach at FINTECH events and competitions such as SWIFT Innotribe, Cambridge Judge Business School Accelerator, Fintech Startup Bootcamp and Barclays Techstars Accelerators. She has more than 14 years’ experience across Deutsche Bank, Lloyds Banking Group, Morgan Stanley and Accenture in London and Hong Kong. Susanne can be followed on Twitter on @SusanneChishti @FINTECHCircle @The FINTECHBook @FTCInnovate and the @FINTECHTours. www.FINTECHCircle.com

# FinTech in China: From Shadow Banking to P2P Lending

Jànos Barberis and Douglas W. Arner

**Abstract** In 1978 China Financial sector has began a gradual reform process. Within 40 years the country went from a mono-bank model to one composed of hundreds of wholly-owned State banks and joint stock commercial banks. Yet this diversification has the banking landscape has not resolves credit allocation inefficiency. Indeed, whilst SME represent 80 % of the economic output of the country, it is only receiving 20 % of the credit originated by banks. This has spurred the development of shadow banking, an informal and unregulated network of lenders and borrowers. The emergence of Financial Technology has allowed for this activity digitized itself in the form of Peer-to-peer lending channel. The combination of and unregulated market and large credit gap has lead to the emergence of a sector that had only one platform in 2007 and over 2000 in 2015. Therefore the author submit that the emergence of the P2P sector in China is neither new, nor unexpected. Ultimately, this systemic shift caused by the P2P sector offers China a regulatory and market reform opportunity as the shadow has been brought to the light.

**Keywords** Financial technology • FinTech • Financial innovation • Financial globalization • Financial regulation • China • Regulatory Technology • RegTech

J. Barberis (✉)
Asian Institute of International Financial Law, Faculty of Law,
University of Hong Kong; and FinTech HK, Pok Fu Lam, Hong Kong
e-mail: janos@fintech.hk

D.W. Arner
Duke-HKU Asia America Institute in Transnational Law, and Member,
Board of Management, Asian Institute of International Financial Law,
Faculty of Law, University of Hong Kong, Pok Fu Lam, Hong Kong
e-mail: douglas.arner@hku.hk

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_5

## 1 Introduction

In 1979, China began the transformation of its economy and the modernization of its financial sector. However, ever since, its credit market has suffered from allocation inefficiencies that particularly affect small and medium sized enterprises (SMEs). In a time of slowing economic growth, this misallocation of capital has an important impact in that SMEs represent 80 % of the economic output of the country, whilst only receiving 20 % of the credit originated by banks.[1] This mismatch has spurred the growth of the shadow banking industry in China, an informal sector performing credit allocation between lenders trying to move liquidity from savings accounts with yields limited by restrictive rate ceilings and non-State firms looking for the much needed capital to finance their growth. Since 2009 China's shadow banking industry has expanded its activities via Peer-to-Peer (P2P) lending channels. In just a few years, financial technologies (FinTech) have allowed a trillion-dollar and decade-old industry to emerge at the beginning of the second decade of the 21st century.

In July 2015, China's P2P lending platforms numbered 2,136, with settlements of around RMB 82.5 billion transactions in that single month.[2] More worryingly, 130 closed in the previous 2 months alone and over 1,250 are regarded at risk by local credit rating agencies.[3] The speed with which this sector emerged has prevented regulators from drafting adequate legislation to ensure consumer and prudential safeguards, while at the same time underpinning development of the market. However, in March 2015, the Chinese Banking Regulatory Commission (CBRC) announced the enactment of new capital requirements for P2P platforms.[4] The sector went from light-touch regulation with low barriers to entry to one where actors may need to set aside over Yuan 30 million in regulatory capital.[5]

This change of approach by regulators is a reflection of the fact that the P2P sector in China has reached a critical size. It went from too-small-to-care to too-big-too-fail.[6] Yet, it performs an important allocation role, especially for SMEs that have constrained credit access. As a result, and going forward, a balancing act needs to be performed by the legislators and regulators.

[1] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 84.

[2] The data information is collected from http://www.wangdaizhijia.com a Chinese website providing all sorts of information on P2P lending in China. For the P2P data, see http://shuju.wangdaizhijia.com/industry-type-0-7-2015.html.

[3] Judy Chen, "Internet Loan Alarms Dagong with 1'250 Red Flags" (13 March 2015) Bloomberg, available at http://www.bloomberg.com/news/articles/2015-03-12/internet-loan-alarms-dagong-with-1-250-red-flags-china-credits.

[4] Daniel Ren, "China mulls tighter rules on booming P2P lending business" (17 April 2015) South China Morning Post, available at (http://www.scmp.com/business/china-business/article/1744711/china-mulls-tighter-rules-booming-p2p-lending-business).

[5] Ibid.

[6] See Douglas W. Arner and Janos Barberis, "Regulation FinTech Innovation: A Balancing Act" (1 April 2015) available at http://www.law.hku.hk/aiifl/regulating-fintech-innovation-a-balancing-act-1-april-1230-130-pm/.

This chapter is accordingly composed of four sections, following this introduction.

Section 2 introduces the origin which led to inefficient credit allocation within China. To counter-act this credit gap the private sector, led by Internet finance companies, has acted to disintermediate banks and, by extension, the State when it comes to providing credit to the economy. However, technology has exponentially increased the ability of private actors to do so and China saw the rise of over 2,000 P2P lending platforms in 2015, compared to only one in 2007. This seismic shift challenges not only the viability of traditional banks, but also classic financial market infrastructure and the capacity for the State to maintain a resilient financial system.

Section 3 covers the recent regulatory changes that are occurring within China's P2P market and views them within the broader market reform trends that have been initiated following the newly issued 2015 Internet Finance Guidelines. Whilst the emergence of P2P lending has disrupted credit origination channels and created risks outside a regulated financial market, it may also provide a unique regulatory opportunity. Indeed, in light of the recently promulgated Internet Finance Guidelines, China may be able to retain the technological efficiency of P2P lending platforms, introducing competition within an otherwise immutable State-controlled sector and reforming a shadow banking industry that has eluded most policy efforts to date.

Section 4, considers potential regulatory opportunities brought by the use of technology within financial services. In particular, the authors highlight the fact that already prior to 2000, regulators in the USA considered using IP addresses of computers to map, in real time, concentration risk within the mortgage industry. This is turn leads to the broader theme of the use of technology within regulation, also known as "RegTech". However, it will be pointed out that whilst the rationale for the development of RegTech is clear (e.g. lower compliance cost, better risk assessments) the practical implementation remains distant, especially as China is still focused on setting a broader framework for FinTech development, as opposed to the application of highly advanced regulatory methodologies.

In conclusion, the authors submit that the emergence of the P2P sector in China is neither new, nor unexpected. Indeed, the shadow banking industry has simply transited over to the 21st century, attracted by the efficiency and market share gains brought forward by the use of FinTech. Therefore, it is instead the scale of the sector (over 2,000 existing platforms) that has taken both international commentators and regulators by surprise. The Internet has brought to light the shadow banking sector, and by doing so revealed the scope and dynamism of this industry that previously benefited from asymmetry of information prompted by its off-line operation methods.

Ultimately, this systemic shift caused by the P2P sector offers China a regulatory and market reform opportunity with profound consequences for the country and the developing world. Indeed, the Internet Finance Guidelines released in July 2015 indicate that the country is creating both a financial market infrastructure and a regulatory framework that is built with FinTech in mind. China would effectively transform its last-mover advantage in the field of financial reform into a first-mover advantage,[7]

[7] This topic is explored in more detail by Zhou, Weihuan and Arner, Douglas W. and Buckley, Ross P., Regulation of Digital Financial Services in China: Last Mover or First Mover? (September 2015) available at (http://ssrn.com/abstract=2660050).

by setting, global, standards for financial market and regulatory developments that can be looked upon by developing markets in South-East Asia and Africa.

In other words, the 21st century may witness a shift where the country's exports went from "*Toys made in China*" to "*Regulation made by China*".

## 2 Banking in China: The Politics of Money

A discussion of the Chinese financial system necessarily starts by highlighting the role of the State. This is warranted by the function of the Chinese Communist Party (CCP) in the Chinese economy—it is at the same time "*the regulator, the financier, the banker, the business man, the guarantor and the employer.*"[8]

However, not all banks are State-owned. Indeed, Chinese banks have faced successive waves of reform. The start of this gradual process began in 1978 with the end of the mono-bank model,[9] whereby the People's Bank of China (PBOC) represented the entirety of the banking system. Today, the banking landscape is composed of wholly-owned State banks,[10] equitized commercial banks, local banks and joint stock commercial banks.[11] In 2007, four foreign banks[12] were the first to receive full licences to freely operate within the PRC,[13] whilst most recently, following the introduction of a new deposit insurance scheme in 2015, there has been the emergence of five new online banks owned by private capital (e.g. WeBank and MyBank from Tencent and Alibaba respectively).[14]

Against this background towards a more heterogeneous and liberalized banking sector, State impact in many respects remains constant. The fact that 80 % of bank CEOs and 54 % of senior executives[15] are CCP members and appointed by the CCP,[16] provides some notion of the enduring pervasiveness of State involvement in the banking system. Another figure to help visualize the situation is biased credit allocation, which benefits mainly State-Owned Enterprises (SOEs). The latter

[8] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 63.

[9] Ibid. 4.

[10] The Agricultural Development Bank of China (ADBC), The China Development Bank (CDB) and the China Exim Bank (CEB).

[11] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 2.

[12] Those are: HSBC, Standard Chartered, Bank of East Asia and Citi.

[13] J. Cheng, *China: A New Stage of Development for an Emerging Superpower* (City of University Hong Kong Press, 2012), 336.

[14] Xinhua, "Can private banks survive and thrive?" (20 May 2015) China Daily, available at (http://www.chinadaily.com.cn/china/2015-05/28/content_20848289.htm).

[15] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 54.

[16] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 26.

account for only 35 % of GDP and are responsible for 20–30 % of overall economic growth, yet they capture over 80 % of all loans made.[17] In this context, the rise of P2P platforms is enhancing the speed at which two main stakeholders are being disintermediated. Namely, the primacy of the formal banking system in originating loans, and therefore, by extension, the State itself.

## 2.1 Political Intervention and the (Mis)Allocation of Money

Whilst the inclination of the State to control banks is by no means new and can be seen in other jurisdictions such as Japan, France and Germany,[18] State interference causes a series of problems, ranging from inefficient credit allocation within the economy, accountability issues[19] and even in some cases—financial crises. Indeed, part of the responsibility for the Asian Financial Crisis of 1997 was attributed to "crony capitalism", whereby loans were made on political considerations, as opposed to sound commercial sense.[20] As it stands, Chinese banks today are in a hybrid position between making loans based solely on commercial logic on the one hand (and thus benefiting the non-State sector) and following directions that may only be based on political/personal motives, on the other.[21]

This conflict in the policy of loan allocation is reverberated at the regulatory level. The PBOC—which was made responsible for the stability of the financial sector following the 1995 *Central Bank Law*[22]—has a clear position in requesting that banks increase the availability of loans to SMEs.[23] However, the CBRC, created in 2003, is more focused on the safety and soundness of individual institutions. As a result, it tends to focus on the avoidance of non-performing loans (NPLs).

A recent example of the impact of government intervention on shadow banking occurred in the wake of the 2008 Global Financial Crisis, in the context of a massive Chinese economic stimulus. Indeed, the shadow banking sector was stimulated by a CNY 4 trillion package (approximately $570 billion) introduced by the Chinese government in an objective to prevent recession and maintain high levels of domestic

[17] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 84.

[18] Simon Cox, 'Pedalling Prosperity' The Economist Special Report (May 2012) available at: (http://www.economist.com/node/21555762).

[19] See (1.2).

[20] Douglas W. Arner, *Financial Stability, Economic Growth, and the Role of Law* (Cambridge University Press, 2007), 225.

[21] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 1.

[22] Stephen Bell and Hui Feng, *The Rise of the People's Bank of China. The Politics of Institutional Change* (Harvard University Press, 2013).

[23] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 124.

growth.[24] When, however, the government interventionism slowed down and the size of the stimulus package decreased, the public's demand for credit could not be satisfied by the regular banking system alone. This in turn increased the demand for alternatives and greatly boosted shadow banking activities.[25]

In this respect, it is perhaps important to note that the development of the P2P sector in China, similarly to that in the USA, witnessed an increase since 2008.[26] However, the difference is that whilst the United States was faced with an important credit supply shortfall, forcing people to seek alternative lending channels, China's P2P sector can attribute its growth to the fact that SMEs were looking to maintain the situation of credit abundance that followed the stimulus program of the government.[27]

## 2.2 *Preparing for the Necessary Liberalization of Finance*

For many years China was therefore in a situation where it had to strike a balance: maintaining sufficient economic growth necessarily implies financial reform to better allocate savings into the financial system.[28] At the same time, regulators must also be able to prevent the liberalization process from creating various asset bubbles that would affect the real economy if they were to burst. This dilemma is reflected in former Premier Wen Jiabao's demands for reform and PBOC Governor Zhou Xiaochuan's concerns regarding financial stability.[29] So far, the decision had been to reach a compromise. Violaine Cousin's book *Banking in China* referred to an analysis conducted by McKinsey Global Institute in 2006, which estimated that the foregone GDP growth resulting from an inefficient financial sector was 13 %.[30]

It transpires that this "sub-optimal" growth level is the result of a conscious choice. The factions that are prone to liberalization and the ones that prefer stability have "*settled for a compromise: a slightly lower rate of growth, but more stability which do not put the*

[24] Guo, Li and Xia, Daile, In Search of a Place in the Sun: The Shadow Banking System with Chinese Characteristics (July 15, 2014). European Business Organization Law Review, Vol. 15, No. 03, page 398, Available at (http://ssrn.com/abstract=2562288).

[25] Guo, Li and Xia, Daile, In Search of a Place in the Sun: The Shadow Banking System with Chinese Characteristics (July 15, 2014). European Business Organization Law Review, Vol. 15, No. 03, page 398, Available at (http://ssrn.com/abstract=2562288).

[26] See Morgan Stanley, "Can P2P Lending Reinvent Banking" (17 June 2015) available at (http://www.morganstanley.com/ideas/p2p-marketplace-lending/).

[27] Arner, Douglas and Barberis, Janos and Buckley, Ross. "The Evolution of FinTech: A new post-crisis Paradigm?" (September 2015) page 17 available at (http://papers.ssrn.com/abstract=2676553).

[28] Janos Barberis, "A crack in the great wall – Too-big-to-Fail Them: A societal perspective" (Sept 2013) page 36.

[29] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 44.

[30] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 58.

*financial resources unnecessarily at risk.*"[31] However, as the economy slows down, the capacity of engaging in a sub-optimal efficiency path for China's financial market is not sustainable. Indeed, it has been pointed out that failing to adequately reform China's financial system poses the risk to jeopardize future economic growth.[32]

In other words, it is submitted that the combination of slower economic growth as well as the rise of P2P lending platforms in China is challenging the extent to which this balancing act can be maintained. The gatekeepers of financial liberalization, namely the State power to grant a banking charter or licence, are losing their effectiveness. Since 2007, the barriers to entry into China's financial system have been side-stepped by private individuals and Internet finance companies[33] delivering over RMB 251 billion of credit in 2014 directly to the public and SMEs.

It may be argued that this is nothing new, indeed the *raison d'etre* behind shadow banking is precisely that of providing financial products and services to the public, outside of a traditional and supervised regulatory framework. As discussed in the introduction section to this chapter, this industry has a decade old history that can be traced back the Xi-Zhou Dynasty (1045-256 BC).[34] However, the point at which this parallel and informal banking system, described by Kellee S. Tsai as "Back alley banking", has been able to come to the light is largely missed.[35] In less than 7 years, China has witnessed the emergence of over 1,500 P2P lending platforms with a total loan origination capacity of RMB 251 billion (Fig. 1). To put this in perspective, in 2007 China only had one P2P platform (Fig. 2). These numbers reflect the year-on-year growth of the market and not its absolute size within the financial sector as a whole. It is difficult to evaluate the precise weight of the P2P sector within the total outstanding loans in China's credit market, but to date this remains marginal.[36]

This exponential growth rate of the P2P industry in China has directly challenged the government's capacity to gradually implement liberalization policies within the banking sector.[37] Whilst regulators, government and SOEs were "crossing the river by touching the stones",[38] the private sector, led by Internet

[31] Ibid.

[32] This idea is explored in more details in "Regulation of Digital Financial Services in China: From Last Mover to First move?" by Weihuan Zhou, Douglas W. Arner and Ross P. Bucley (Sept 2015).

[33] Arner, Douglas and Barberis, Janos and Buckley, Ross. "The Evolution of FinTech: A new post-crisis Paradigm?" (September 2015) page 34 available at (http://papers.ssrn.com/abstract=2676553).

[34] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 14.

[35] Kellee S. Tsai, "Back-Alley Banking: Private Entrepreneurs in China" (2004) Cornell University Press.

[36] Guo, Li and Xia, Daile, In Search of a Place in the Sun: The Shadow Banking System with Chinese Characteristics (July 15, 2014). European Business Organization Law Review, Vol. 15, No. 03, page 408, Available at (http://ssrn.com/abstract=2562288).

[37] Arner, Douglas and Barberis, Janos and Buckley, Ross. "The Evolution of FinTech: A new post-crisis Paradigm?" (September 2015) page 34 available at (http://papers.ssrn.com/abstract=2676553).

[38] This expressions illustrates the cautious approach of the government in China when reforming markets.

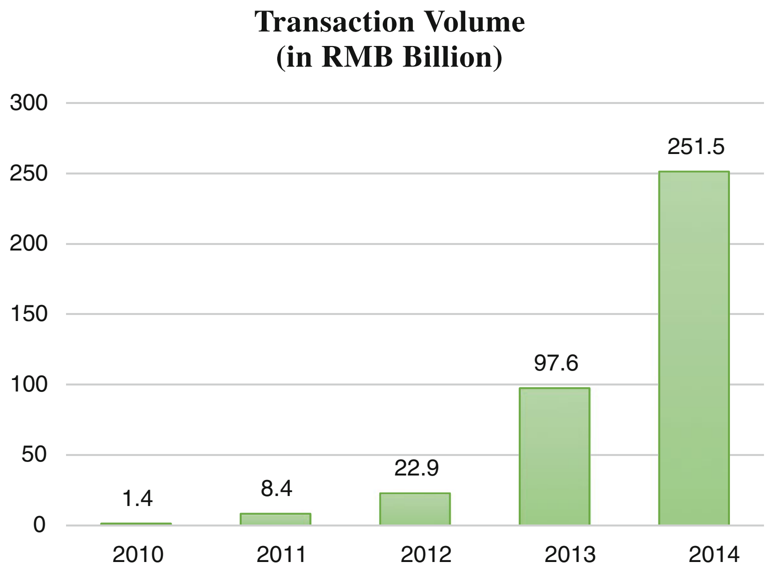


**Fig. 1** Transaction Volume (in RMB Billion). *Source* iResearch (showed during HKIFA conference)

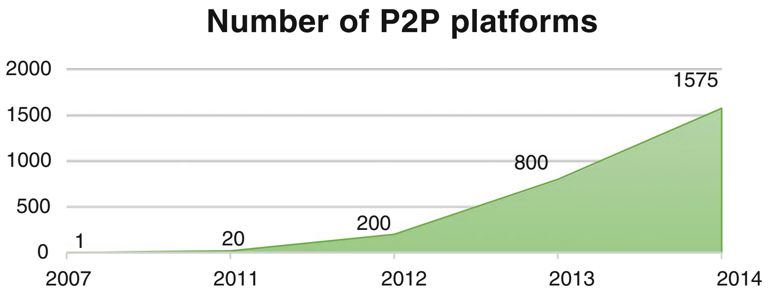


**Fig. 2** Number of P2P platforms. *Source* wangdaizhijia.com, end of 2014

finance companies, has been literally leapfrogging their traditional regulatory and banking counterparts.

It may be argued that, irrespective of its origin, financial liberalization is positive since it is expected to both support growth, but also increase job prospects.[39] Yet, it also needs to be remembered that the latest crisis revealed the negative effect of inadequate liberal deregulation, which destroyed more jobs than those saved and created in the 1980s.[40] There is therefore value in government intervention that is

[39] Avgouleas E, *Governance of Global Financial Markets: the Law, the Economics, the Politics* (Cambridge University Press, 2012), 106.

[40] Ibid. 60.

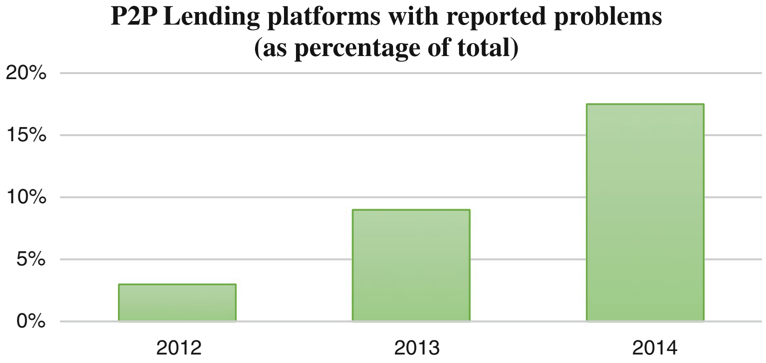


**Fig. 3** P2P Lending platforms with reported problems (as percentage of total). *Source Data Source* wangdaizhijia.com (from HKIFA conference)

highly targeted and precise. Even more so, because every change *within* the financial sector will affect a fragile economic, social and political equilibrium.[41] Indeed, even the P2P sector itself is currently experiencing an increased amount of defaults and closures, as can be seen in Fig. 3.

Whilst the initial wave of financial liberalization was driven from the bottom-up, as the industry increasingly engenders systemic risks within the financial system, this needs to be effectively addressed by regulators.

It is neither desirable nor possible for the P2P sector to continue its development in isolation from government policies and regulatory obligations. This is equally because of the systemic size of the sector as well as of the beneficial economic impact it yields.[42] Therefore, one can expect that this sector, which had thus far been unregulated, will now be fitted within the broader context of financial market infrastructure. This forms the subject of the following section.

## 3 A Window of Opportunity: Bring the Shadows to the Light

The remainder of this chapter considers the market reform opportunities brought about by the current developments of P2P lending. The misallocation of credit within the Chinese economy has been endemic for decades, and this has lead individuals and corporate parties to create a parallel and non-official network that

[41] For more details, refer to Janos Barberis “A Crack in the great wall – Too-big-to-fail then: a societal perspective” (Sept 2013).

[42] Arner, Douglas and Barberis, Janos and Buckley, Ross. “The Evolution of FinTech: A new post-crisis Paradigm?” (September 2015) page 24 available at (http://papers.ssrn.com/abstract=2676553).

would perform the credit intermediation that they were otherwise lacking. In the context of China, non-bank finance and shadow banking thus capture both the essential elements that we now see in the P2P sector, namely the need for alternative forms of financing to support non-State growth, particularly among SMEs whilst at the same time addressing potential risks to consumers and the financial system.[43]

The thesis of the second part of this chapter is that for the Chinese government, the emergence of P2P lending offers a unique opportunity that solves a decade-old tension which thus far prevented the formalization of the shadow banking industry.[44] As will be detailed below, the various routes towards market reforms had the potential to generate negative externalities which would outweigh the initial objectives. In essence, because both the shadow and the formal banking sector provide a vital lifeline of credit to SMEs and SOEs respectively, any reform had the potential of disrupting a fragile equilibrium. More specifically, in respect of shadow banking, the fact that it was informal and "off-line" generates a level of information asymmetry which made it difficult to evaluate the potential consequences of bringing the sector to the light. Policy-makers risked forcing the sector deeper into the shadows or simply impeding its much-needed function from an economic growth perspective.

Most importantly, as was seen in Sect. 2, it appears that since 2008 the shadow banking sector has indeed been increasingly brought to light, both as a result of greatly increased academic, policy and market research attention as well as the result of technology. This is the critical element providing the basis for the authors' submission. Namely, that shadow banks have been attracted to the light by the market share potential and efficiency gains brought by technology, as they move their operations from off-line to on-line models, which in turn gives a regulatory window of opportunity to reform this sector in a way that was not possible until now.

The positive impact of that transition is that not only has it removed the pre-existing information asymmetry that limited the possibility of government reform, but it has also constrained the capacity of the sector to move further back to the shadows. Indeed, SMEs and individuals who were former users of shadow banks, and now borrowers or lenders of P2P platforms, are unlikely to settle for the necessarily less competitive and transparent terms offered by the "off-line" shadow banks.[45]

[43] In other words, China is witnessing the rise of Shadow Banking 2.0. For more of the historical analysis on the use of technology within the financial services sector, please refer to Arner, Douglas and Barberis, Janos and Buckley, Ross. "The Evolution of FinTech: A new post-crisis Paradigm?" (September 2015) page 24 available at (http://papers.ssrn.com/abstract=2676553).

[44] This is illustrated in Sect. 2.1.

[45] As it currently stands there is limited qualitative and quantative surveys that exactly looks at the P2P industry and would allow to bring empirical data to this statement. However a recent research project lead by Tsinghua University and Sydney University will offer valuable data set in that respect.

### *3.1 Bringing the Shadows to the Light: A Regulatory Approach*

The risks caused by shadow banking are not novel and in 2013, a survey reported that 63 % of respondents expected that "shadow banking [will] cause a crisis in China".[46] As a result, the idea that shadow banking should be left free of government intervention is not viable. This is because there is an inherent risk of social unrest attached to a failing informal banking sector.[47] This has led the government to experiment, with limited success,[48] over an extended period of time with various approaches of bringing the shadows to the light by regulating a sector that is by definition informal.

If it is true that *some* regions are more relaxed in letting informal banks operate within their jurisdiction with little or no control, this is because local officials view shadow banking operations as "a popular (*minjian*) form of grassroots credit".[49] This lenience can be regarded as "active non-action". In other words, as long as the activities of the local informal operators do not disturb the economic, social and political climate, they are left untouched. In that respect, a regulatory official interviewed by Joe Zhang confirmed this by characterizing the sector as a tolerable nuisance.[50]

However, if this was about to change, we would witness an immediate crack-down on the sector. Indeed, this is precisely what happened in October 2012 when a default of informal banks in Wenzhou threatened to transform into a regional crisis.[51] The event would perhaps have remained unnoticed if it were not for the fact that the potentially affected province, Zhejian, is home to 55 million people, and also considered to be the historical capital of entrepreneurship in China. One should bear in mind the fact that three leading officials (then Premier Wen Jiabao, PBOC Governor Zhou Ziachuan and then Finance Minister Xie Xuren) went there to personally witness the problem caused by informal finance, and subsequently called for the closure of those institutions.[52]

[46] Caixin survey, available at: (http://service.caixin.com/pollcode/resulten/batch/576).

[47] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 144.

[48] Yet, the difficulty of introducing comprehensive financial reform in the shadow banking sector is not exclusively confined to China. United States regulators have also struggled to provide for complete coverage of this sector, as seen by the sparse treatment of shadow banking in the otherwise extensive Dodd-Frank Act.

[49] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 144.

[50] Joe Zhang, *Inside China's Shadow Banking: the Next Subprime Crisis?* (Enrich Professional Publishing, 2013), 91.

[51] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 7.

[52] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 44.

Therefore, we see that government inaction is only acceptable up to a point.[53] Furthermore, because of the lack of regulation and transparency, this sector runs a high likelihood that operators will default on their obligations. An example of this is when *Hehui*[54] turned into a Ponzi scheme.[55] As such, it is expected that the inaction of the state could only be a temporary relief and not a long-term policy of the central or local authorities. Hence, reforming or banning informal banking appears a more likely course of action. Indeed, both solutions have been attempted in recent years.

The other corner solution—to simply shut down companies operating outside the law—had varied success, but a long history. Since 2002, over 500 *underground* banks have been closed, out of which over 100 had assets exceeding RMB 200 billion.[56] As for the individuals running those operations, or benefiting from them, the most recent high-profile case concerns Zeng Cheng Jie who was executed after being found guilty of "fraud in raising funds".[57] Similarly, between 2011 and 2012, the CBRC forced over 5,000 guarantee companies to shut down, while increasing regulation of the remaining enterprises.[58]

However, there exist a number of limitations in the ability of the government to shut down the shadow banking sector. Putting aside the historical argument that this type of activity has existed in China since the Xi-Zhou Dynasty (1045-256 BC),[59] three examples of failure to ban shadow banking can be given.

First, when the PRC was established in 1949, the central government's stance on informal finance was clear: it should be prohibited. The rationale was that it should be only for the State to provide such services. This campaign against shadow banking was successful to the point that the sector almost disappeared.[60] The banned institutions were replaced by Regional Credit Cooperatives (RCC). However, because those were the creation of the State, rather than arising out of real economic need, they had deficiencies that hindered their success.[61] In 2011, 12 % of the total deposits in China were placed in such institutions.[62] However, this large

[53] With a similar point being made about P2P lending and current increase in market risk it creates.

[54] A private money-lending association, and thus—part of informal finance.

[55] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009) pp. 21 and 141.

[56] Michael F. Martin, 'China's Banking System: Issues for Congress' (Congressional Research Service, 2012), 2.

[57] China Daily, "Entrepreneurs face dilemma over funds" (22 July 2013), available at: (http://usa.chinadaily.com.cn/opinion/2013-07/22/content_16811976.htm), accessed 24 August 2013.

[58] Joe Zhang, *Inside China's Shadow Banking: the Next Subprime Crisis?* (Enrich Professional Publishing, 2013), 84.

[59] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 14.

[60] Ibid. 17.

[61] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 16.

[62] Ibid. 19.

number is attributable to the fact that membership was made compulsory in villages, explaining the sheer size of the sector by an obligation people have, as opposed to a genuine inclination to use RCCs. Because Regional Credit Cooperatives did not respond to a true social necessity, informal finance has risen again.

Second, the government's next attempt to crack down on this sector was seen in 1998 with the fall of the Three Star Holding Company. Following government investigations, this informal bank faced a lack of confidence from its depositors and investors. This caused a bank run, which in turn prompted the local government to close the company, leading to over 30,000 people marching on the streets.[63] As a result, the government's measures of closing down a company formed by a farmer, as opposed to even more inefficient State-run enterprises, had occasioned instability and controversy.

Finally, the persistence and pervasive nature of informal finance in China can be explained by the theory of institutional demand.[64] Indeed, informal finance is simply the symptom of a formal sector that is both dysfunctional and unable to provide small, often unsecured loans to SMEs or individuals. Thus, suppressing informal finance would be ineffective and push that sector even deeper into the shadows.[65] The risks of such an approach stem from the likelihood that this will further impede both the monitoring,[66] and also the prospect of regulating this segment of the economy in the future.

From the above analysis, it appears clear that the reform margin government bodies have is very narrow. Because of the fact that shadow banking and P2P lending supply credit to the non state actor that generate 80 % of the country's economic output,[67] any regulatory heavy-handedness may be destabilising from a social, economic and financial perspective.

At the other side of the spectrum, one needs to consider that instead of fixing the symptoms of shadow banking, the government may have more success in resolving the inefficiencies within the formal banking sector itself, especially given the far reach of government control within banks. In practice, this revolves around the liberalization of the formal financial sector. Yet, this move towards a more market-orientated financial system has its own limitations, three of which are highlighted below.

First, the liberalization of market rates will have political repercussions in the sense that the State would lose its control over the financial sector, which it is reluctant to do, although it is now likely that this process will largely be complete

[63] Ibid. 93.

[64] Ibid. 25.

[65] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 35.

[66] The UK has shown the advantage of not cracking down on sensitive sectors. For example, by allowing extremist Salafist groups to openly protest on the streets and in front of Parliament, this helped intelligence services to gather data on the membership of such groups. Therefore, even if the government cannot regulate the informal sector, it should at least monitor it and identify major supporters and participants.

[67] Janos Barberis, "A Crack in the Greal Wall – Too-big-to-Fail-Them: A societal perspective" (Sept 2013) page 40.

before 2017.[68] Second, economically-speaking, if SOEs were to pay market rates, a report by the Economist estimated that between 2001 and 2008, these companies would have suffered large losses, or even gone bankrupt.[69] In other words, liberalizing interest rates would expose the misallocation of resources that has been occurring for decades now.[70] Nevertheless, with the focus of the Xi-Li administration on restructuring of the economy, this is now seen as a desired and necessary result, albeit one that must be managed carefully. Third, removing the limit on the deposit rate would erode banks' profit margins. This, in turn, has consequences on the ability of formal institutions to actually be able to handle NPLs themselves—as opposed to relying on State intervention as hypothesized earlier—because this profit margin enables banks to be easily recapitalized.[71] Nonetheless, the fact that banks have become increasingly commercialized, combined with previous successful experiences in resolving NPL issues through asset management companies and deferred financing, makes this less problematic than previously. Most importantly, even if the liberalization of the traditional sector could be achieved without any of the above negative externalities, this would not necessarily imply the disappearance of shadow banking, which has now taken on a life of its own beyond its initial nascence in regulatory arbitrage.

Different factors play a role here, including the fact that the size of the loans offered (and thus requested) by individuals or SMEs is too small to be profitable for larger entities, without significant developments in internal systems. As such, they are unlikely to offer small loans,[72] but assuming that they were to provide credit in the first place, it would not be at a competitive, or even affordable, rate as their due diligence costs would be very high.[73] Moreover, even if the lending rate of the traditional sector could align itself to its shadow counterpart, P2P platforms still benefit of flexibility and speed advantages,[74] giving them a strong competitive edge.[75]

[68] Violaine Cousin, *Banking in China* (Palgrave Macmillan Studies in Banking and Financial Institutions, 2011, 2nd edition), 10.

[69] Simon Cox, 'Pedalling Prosperity' The Economist Special Report (May 2012) available at: (http://www.economist.com/node/21555762) 7.

[70] However, the benefit of liberalizing interest rates of loans is that SOEs will not borrow as much and thus free up the much-needed capital for SME's. (*Source* Joe Zhang, *Inside China's Shadow Banking: the Next Subprime Crisis?* (Enrich Professional Publishing, 2013) 104).

[71] Michael Pettis, *The Great Rebalancing: Trade, Conflict, and the Perilous Road Ahead for the World Economy* (Princeton University Press, 2013), 95.

[72] L.T. Alexander, 'Cyberfinancing for Economic Justice' (2013) 4 Wm. & Mary Bus. L. Rev. 309, available at: (http://scholarship.law.wm.edu/wmblr/vol4/iss2/2), 319.

[73] See Sebastian Diemer, "Lending club IPO – what drives the value of P2P lending platforms" (11 Dec 2014) Kreditech, available at (https://www.kreditech.com/blog/lending-club-ipo-what-drives-the-value-of-a-p2p-lending-plattform/).

[74] See Peter Baeck, Liam Collins and Brian Zhang, "Understanding Alternative Finance: The UK alternative finance industry report 2014" (November 2014) NESTA page 23 available at (https://www.nesta.org.uk/sites/default/files/understanding-alternative-finance-2014.pdf).

[75] Hsu S. and Li J., *Informal Finance in China: American and Chinese Perspectives* (Oxford University Press USA, 2009), 133.

### *3.2 Bringing the Shadows to the Light: The Technological Route*

Importantly, for the purpose of the authors' argument, the exponential growth of the P2P industry in China cannot be understood in a vacuum. Instead, it is submited that the P2P boom in China is not only attributable to the same arbitrage opportunities (i.e. negative interest rates payable on current accounts, moving excess savings towards P2P platforms that yield a higher return), but also to the fact that traditional shadow banks have moved their operations online, attracted by the lower operating costs and broader market share they can reach by using the Internet.[76]

This is not to say that the P2P industry is only composed of long-standing actors, as undeniably there have been new players in the market that have no previous history as shadow banks. Indeed, this is illustrated by two key new companies. First, the most publicized example is AliFinance, part of the Alibaba group, which has already originated 409,444 loans with an outstanding portfolio of 105 billion RMB ($17.2 billion).[77] Second, and perhaps the most (in)famous illustration of a market overheating is Panda Firework Group Co., a listed fireworks manufacturer that changed its core business entirely to become a P2P lending provider.[78]

Thus, until a detailed study is performed to examine the origins and sources of funds of all P2P platforms in China, it is difficult to determine whether this is a wholly novel industry or a new twist on the old shadow banking model.[79] However, it would be fair to assume that the P2P lending sector is predominantly supported by operators or funds of shadow banks. It could thus be argued that there is little to distinguish shadow banks and P2P lenders in China. In both cases they operate without a formal regulatory framework and perform an intermediation function between lenders and borrowers, the most noticeable difference being in the origination channel, which is principally online. Unlike the formal banking system, shadow banking, whether in its traditional or online form, relies on a different

[76] There is currently a very limited amount of primary research on the P2P industry in China and Asia which limits the capacity of formally linking shadow banks with P2P platforms. It is expected that the new effort lead by Cambridge, Tsinghua and Sydney Universities is conducting an Asia wide Alternative Finance Benchmarking Survey will offer the necessary data set to confirm the above argument. See JD Alois, "The University of Cambridge, Tsinghua University & the University of Sydney join forces to launch the 2015 Asia-Pacific Alternative Finance Benchmarking Survey" (Crowdfund Insider, November 11) available at (http://www.crowdfundinsider.com/2015/11/77114-the-university-of-cambridge-tsinghua-university-and-the-university-of-sydney-join-forces-to-launch-the-2015-asia-pacific-alternative-finance-benchmarking-survey/).

[77] Leesa Shrader, 'Microfinance, E-Commerce, Big Data and China: The Alibaba Story', 11 October 2013, CGAP (Consultative Group to Assist the Poor).

[78] Bloomberg News, 'Seeing Bang for Buck, Even China Fireworks Makers Now Do Finance', April 13, 2015, (http://www.bloomberg.com/news/articles/2015-04-12/seeing-bang-for-buck-even-china-fireworks-makers-now-do-finance).

[79] It is expected that Tsinghua University will conduct quantitative and qualitative research on the topic in 2016.

financial market infrastructure to fund and originate its loans. In this relation, Guo and Xia point out some of the variations in the financing mechanisms of traditional financial institutions in China and shadow banks:

> In the regular banking system, the whole process of credit intermediation takes place within one bank. However, in the shadow banking system, institutions coordinate to complete the intermediation chain. In this system, commercial banks and financial companies also originate loans, as in the regular banking system, but they do not hold the loans or bear the credit risks. […]The shadow banking system does not rely on bank deposits to support its lending business. 'Shadow bank deposits' come from money market mutual funds (MMMFs).[80]

In addition, Guo and Xia note that the borrowers who resort to the services of shadow banking or P2P lending providers are often individuals or entities who have had difficulty obtaining credit through the "normal" financial system.[81]

Once one accepts the fact that shadow banking and P2P lending represent the same industry, but are conducted via new channels, this opens an important regulatory window of opportunity to reform shadow banking in a way that was not possible before. Section 3.1 of this chapter revealed that the difficulty in reforming the shadow banking system came from two elements:

1. High asymmetry of information limiting the capacity to evaluate the positive/negative externality of any reforms, and
2. Irrespective of its unregulated nature and the risk it holds, the shadow banking sector performs an important credit supply role for SMEs.

For policy-makers and regulators this means that the capacity for reform is exceptionally narrow, with a high probability that the negative externalities outweigh the benefits of formalizing the sector. Nevertheless, with hindsight, it might appear that this inaction has played in regulators' favor and will ultimately allow them to better regulate the shadow banking sector in future.

The authors' submission, and contribution to this topic, is that the (active?[82]) absence of regulation of the P2P lending sector had the outcome of eliminating

[80] Guo, Li and Xia, Daile, In Search of a Place in the Sun: The Shadow Banking System with Chinese Characteristics (July 15, 2014). European Business Organization Law Review, Vol. 15, No. 03, page 395, Available at (http://ssrn.com/abstract=2562288).

[81] Ibid, 402.

[82] Active or not, this point can be the one of discussion. Indeed, if active, it would have meant that both policy makers and regulators were the mastermind to let a sector remain unregulated in views of formalizing it in the future. This is perhaps giving too much credit to these bodies, however, in itself this may not be surprising. China has already used its accession to the WTO as a way to bring back-door liberalization into State-owned-enterprises. Direct reform, without having recourse to the WTO obligations would have made the task much harder for political reasons. Second, again using a WTO analogy, China has revealed its capacity of playing a forward-looking chess game in the context of the card networks. In practice, this meant that China has allowed the Union Pay card network to grow by shielding it from the competition of its US counterparts (e.g. Visa and MasterCard) and against WTO rules. China was aware of that but kept the infringing behaviour up until the point of the WTO court judgement, confirming that this was the case. Importantly, China knew that it had a losing

barriers to entry. As a result, between 2007 and 2014, P2P lending platforms have gained traction and market acceptance emanating from SMEs that seek credit and lenders who look for higher yields than those offered within the traditional banking sector. Importantly, the technological component of P2P platforms creates a competitive advantage vis-à-vis physical shadow banks that translates into better interest rates paid or charged to users of P2P platforms. Not only this, but the lack of physical location, beyond pure cost benefits, removes friction and increases ease of use for consumers. Therefore, whilst one may see shadow banks and P2P platforms as substitutes, the latter are clearly superior.

Since mid-2014, there has been an increase in consultation activity on the part of Chinese regulators to gradually consider the imposition of rules for P2P platforms.[83] Namely, these are meant to cover regulatory capital, licensing obligations as well as better loan origination and credit scoring mechanisms so as to avoid excessive credit creation. These upcoming obligations will necessarily increase the operating cost of P2P platforms which in turn erodes the cost-competitive benefit that they hold against physical shadow banks.[84]

Yet, it is very unlikely that the future onus on P2P platforms would be so high that it turns into a regulatory overkill which makes this online business less economically viable than physical origination.[85] Moreover, whilst certain actors may have been solely operating on the pre-condition that this sector remains unregulated, one may at most witness a concentration of players within the P2P space. Importantly a reduction in the number of platforms is not expected to equate to a fall in the number of users. For example, between them My089.com and LuFax have over 30 billion RMB in outstanding loans, or over 10 % of a market valued at 241 billion RMB for 2014.[86]

The outcome of the above analysis is that, if understood correctly, regulators in China may have willingly allowed for the unregulated development of the P2P

(Footnote 82 continued)

case but also knew that any damages to be paid are from the date of the judgement and don't back-date to the start of the infringing behaviour. As a result, China has rightly "masterminded" the plan to grow the Union Pay card network and give a de facto dominant market share and its cost for doing so would be negligible (e.g. legal fees) as they won't include WTO fines. This analysis of the UnionPay case was made by Jane K. Wing in a 2012 seminar entitled: "The US-PRC UnionPay WTO Dispute: Bringing the Back Office Front & Center" available at (http://www.law.hku.hk/aiifl/wp-content/uploads/2012/05/ppt-ProfWinn-5Oct2012.pdf).

[83] Liz Mak, "Consolidation imminent as new rules hit China's P2P Sector (12 August 2015) South China Morning Post, available at (http://www.scmp.com/business/banking-finance/article/1848743/consolidation-imminent-new-rules-hit-chinas-p2p-sector).

[84] This observation is an extension of the cost structure analysis between banks and P2P platforms which can be found on the following figure (http://www.kreditech.com/wp-content/uploads/2014/12/10845953_10206006364738406_740803989809562525_n.jpg).

[85] The reason from this comes from the fact that the cost and human capital structure of online P2P platforms is much leaner than traditional banks.

[86] Zoe Zhang, "Overcoming Challenges of Internet Finance Innovation in Hong Kong" (28 May 2015) HKIFA.

lending sector. This then lead to a mass market adoption which is hard to reverse due to the cost benefits (e.g. flexibility, convenience, time[87]) for all the stakeholders, even after factoring for compliance costs. Furthermore, the scalability opportunity provided by the online business model of these "shadow banks of the 21st century" means that it becomes much more cost effective for regulators to supervise one institution with a critical mass of users (e.g. for example AliFinance has over 400,000 borrowers) as opposed to a fragmented industry.

In other words, regulating the P2P industry appears to have been not only the most efficient way of handling the problem caused by shadow banking, but the only way to do successfully. Whether or not this is the result of careful planning from policy-makers, or sheer coincidence, this is positive for China as a whole as it creates a framework around the P2P sector which plays a critical role into the country's financial market reform and economic growth.

## 4 RegTech: Maximizing the Benefits of FinTech

Whilst Sects. 2 and 3 illustrated the regulatory and policy benefits of bringing the shadow banking to the spotlight, albeit indirectly, through P2P lending, the chapter now turns to the broader topic of regulatory added value in the context of FinTech. Indeed, if the authors left open for further discussion the point whereby Chinese regulatory inaction was actually intended to formalize a sector that eluded them thus far, China has the opportunity to make a claim as a forward-looking regulator in line with the 21st century.

This section starts by introducing the concept behind Regulatory Technology (RegTech) before focusing on the extent to which this is applicable to Chinese P2P sector. The relevance of discussing RegTech echoes the fact that, with the increased use of technology within the financial services industry, regulatory bodies have the opportunity to access a level of granularity in risk assessments that did not previously exist. Indeed, Andy Haldane, the ex-head of stability at the Bank of England, when discussing the future of regulation shared his vision:

> What more might be feasible? I have a dream. It is futuristic, but realistic. It involves a Star Trek chair and a bank of monitors. It would involve tracking the global flow of funds in close to real time (from a Star Trek chair using a bank of monitors), in much the same way as happens with global weather systems and global internet traffic. Its centre piece would be a global map of financial flows, charting spill-overs and correlations.[88]

[87] See Peter Baeck, Liam Collins and Brian Zhang, "Understanding Alternative Finance: The UK alternative finance industry report 2014" (November 2014) NESTA page 23 available at (https://www.nesta.org.uk/sites/default/files/understanding-alternative-finance-2014.pdf).

[88] Andrew G. Haldane (Keynote), "Managing global finance as a system" (29 October 2014) Bank of England, available at (http://www.bankofengland.co.uk/publications/Documents/speeches/2014/speech772.pdf).

This vision of a data-led regulatory system is not new. Back in 2009 the SEC created the division for Economic and Risk Analysis under the supervision of Henry Hu,[89] looking at driving data insight for better regulation. However, it seems clear that since 2007 there has been an increase in activity emanating from regulators, industry and academia alike on this topic. For example, in 2014 in Australia, the Center for International Financial Regulation initiated a research project entitled Regulatory Analytics and Data Architecture (RADAR).[90] In addition, post-2007, Scott Peppet published a paper on "smart mortgages" whereby the use of data could limit the default risks.[91] However, one needs to balance the opportunity opened by technology and some practical barriers to actual and successful implementation, all of which are discussed below.

## *4.1 Compliance: An Extensive Case for Automation*

The financial sector has been the largest spender on IT systems for decades[92] and this trend is unlikely to stop, especially in respect to regulatory and compliance spending. Indeed, prior to 2007, technology was used by banks as part of their tool-kit to comply with their various reporting and compliance obligations, including but not limited to[93]:

- Legislation/regulation gap analysis tools
- Transaction reporting tools
- Regulatory reporting tools
- Activity monitoring tools
- Case management tools

In the wake of the 2008 Global Financial Crisis, the regulatory onus and the level of scrutiny requested by regulators has dramatically increased.[94] Indeed, regulators have moved towards a risk-based approach where access to data is key to performing

[89] Professor Henry Hu is teaching Law at the university of Texas at Austin, before that he was the inaugural director of the Division for Economic and Risk Analysis within the SEC. Full biography available here (https://law.utexas.edu/faculty/huht/).

[90] Centre for International Finance and regulation, "Regulatory Data Architecture and Analytics" (2014–2015) available at (http://www.cifr.edu.au/project/T019.aspx).

[91] Peppet, Scott R., Smart Mortgages, Privacy and the Regulatory Possibility of Infomediation. U of Colorado Law Legal Studies Research Paper No. 09-13. Available at SSRN: (http://ssrn.com/abstract=1458064) or (http://dx.doi.org/10.2139/ssrn.1458064).

[92] Arner, Douglas and Barberis, Janos and Buckley, Ross. "The Evolution of FinTech: A new post-crisis Paradigm?" (September 2015) page 40 available at (http://papers.ssrn.com/abstract=2676553).

[93] Lory Kehoe "RegTech is the New FinTech: How Agile Regulatory Technology is helping firms better understand and manage their risks" (2015), page 5 DELOITTE available at (http://www2.deloitte.com/content/dam/Deloitte/ie/Documents/FinancialServices/ie-regtech-pdf.pdf).

[94] Tony Ciro, "The Global Financial Crisis: Triggers Responses and Aftermath" (2013) page 143.

appropriate prudential supervision of the firm. This appears to be a natural move, so as to avoid the risks of regulatory capture which did occur in the lead up 2008.

This trend towards a data-driven regulatory approach is clear, for example Daniel Gutierez illustrated how data is playing an increasing role in ensuring that financial institutions are not only held accountable for their actions, but that their responsibility is quickly established[95]:

- The Dodd-Frank Act requires firms to maintain records for at least 5 years.
- Basel guidelines mandate retention of risk and transaction data for three to 5 years.
- Sarbanes-Oxley requires firms to maintain audit work papers and information for at least 7 years.
- FINRA/Tradeworx Project—SEC requires the creation of a real-time transaction monitoring system to detect potentially disruptive market activity stemming from high-frequency trading.

At the same time new legislation, such as the Dodd-Frank Act in the USA, has been regarded as too-big-to-read,[96] whilst European initiatives such as the Resolution Regimes for Banks had unclear deadlines and reporting requirements.

For financial institutions the above has translated itself into an immediate cost increase, whether from a capital (e.g. Basel 3), operational (e.g. human resources) or penalty fine perspective. On the last point alone, since 2008, banks in the west have been fined over US$242 billion[97] out of which US$2.3 is attributable to the Libor scandal.[98]

Arguably, both the industry and regulators have a common interest in fraud levels. For example, the investigation to uncover the chain of responsibility for Libor took months. In a similar fashion, it took years to fully appreciate the exposure of various counterparties during the Global Financial Crisis.[99]

In is understandable that there has been an interest from various stakeholders to increase transparency and create firm monitoring processes. In June 2015 the Bank of England issued its Fair and Effective market review, looking at the role that technology may play,[100] noting that:

[95] Daniel Gutierrz “Big Data for Finance—Security and Regulatory compliance considerations” (20 Oct 2014) available at (http://insidebigdata.com/2014/10/20/big-data-finance-security-regulatory-compliance-considerations/).

[96] Formulation coined by Glen Hubbard in ‘Financial reforms fails on ‘too-big-to-fail’’.

[97] Micahel Mainelli, “RegTech - worthy of Investment” (24 June 2015) available at (http://igtb.com/article/regtech-%E2%80%93-worthy-investment).

[98] Halah Touryalai, “Big Banks Fined $2.3B over illegal Libor cartels, more Fines on the way” (4 December 2013) Forbes, available at (http://www.forbes.com/sites/halahtouryalai/2013/12/04/big-banks-fined-2-3b-over-illegal-libor-cartels-more-fines-on-the-way/).

[99] Janos barberis, “The 2007 Metldown: A legal Phenomenon” (June 2012) page 12 available at (http://ssrn.com/abstract=2296812).

[100] Charles Roxburgh, Minouche Shafik and Martin Wheatley, “Fair and Effective Market Review: Final Report” (June 2015) available at (http://www.bankofengland.co.uk/markets/Documents/femrjun15.pdf).

> Firms have started to make progress in response to the limitations of existing surveillance solutions, including the use of new technology and analytics which go beyond the key-word surveillance and simple statistical checks previously used by firms to detect improper trading activity and discussed earlier in this section.[101]

In particular, the Bank of England highlighted the following regulatory add values of specific technologies:[102]

- "**Pattern analysis**" which can be used to identify unusual patterns of activity, such as "spoofing" (placing an order and then cancelling it seconds later to encourage others to drive up the price of a particular asset), front running and wash trades, using predefined patterns of trading behaviour;
- "**Big data" techniques**, which typically use a far larger number of inputs than standard surveillance techniques, helping to straddle information silos. The algorithms used have the potential to detect a wider range of suspicious activity than pattern analysis, and can also be used to identify networks of trading and communications activity which may themselves identify vulnerabilities;
- "**Predictive coding"**, which looks to identify patterns of activity, such as unusual use of communication, non-routine patterns of leaving the office, non-completion of training, or missing mandatory leave, which may flag potential conduct concerns, and
- **Digital isation of voice communications**, which some firms claim has the potential to be more effective than analysing written communications.

As a result, the argument for cost reduction within the compliance sector has never been as strong, and RegTech never looked so beneficial for firms. Yet, one also needs to be balanced as to what is currently feasible when it comes to fully automating regulatory systems. In 2009 Vytautas Cyras and Reinhard Riedl[103] addressed certain technicalities of having built IT system that can automatically comply with rules and regulations. In brief, their paper seems to highlight two main obstacles to be overcome.

First, a rule-based as opposed to principle-based approach to regulation seems to be more suited for automation. This is because it is difficult for computer systems to understand the nuances and the spirit of the law within which these rules have been

[101] Charles Roxburgh, Minouche Shafik and Martin Wheatley, "Fair and Effective Market Review: Final Report" (June 2015), page 90 available at (http://www.bankofengland.co.uk/markets/Documents/femrjun15.pdf*)*.

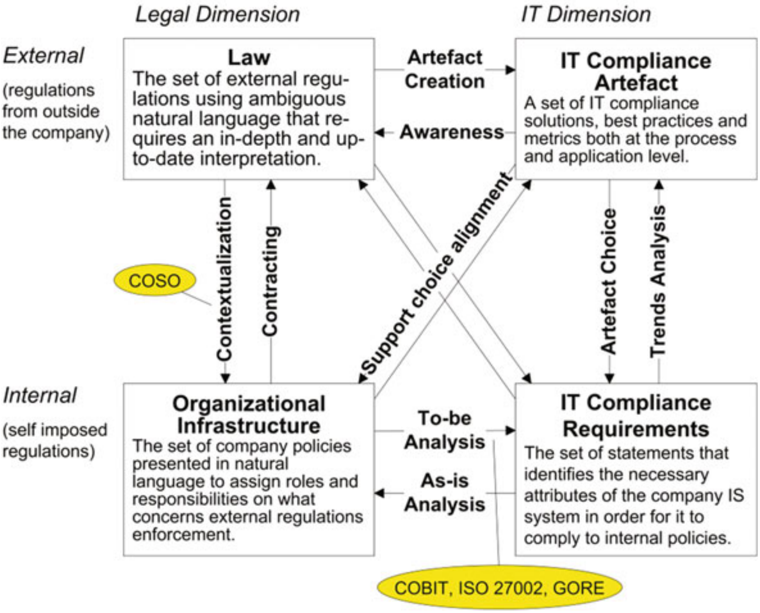
[102] Charles Roxburgh, Minouche Shafik and Martin Wheatley, "Fair and Effective Market Review: Final Report" (June 2015) page 91 available at (http://www.bankofengland.co.uk/markets/Documents/femrjun15.pdf), (http://www.bankofengland.co.uk/markets/Documents/femrjun15.pdf).

[103] Vytautas Cyras and Reinhard Riedl, "Formulating the enterprise Architecture compliance problem" (2009) available at (http://ceur-ws.org/Vol-924/paper14.pdf).

drafted.[104] Yet, at the same time narrowing down compliance obligations to a simple tick-box exercise has limits as it is prone to omit the development of a compliance culture within an institution or region.[105]

Second, once, and if, rules can be identified, these need to pass the test of being transcribed into automated processes that can be handled by computers and the data available to financial institutions. In that respect, two useful diagrams were provided to illustrate the logical process behind this.

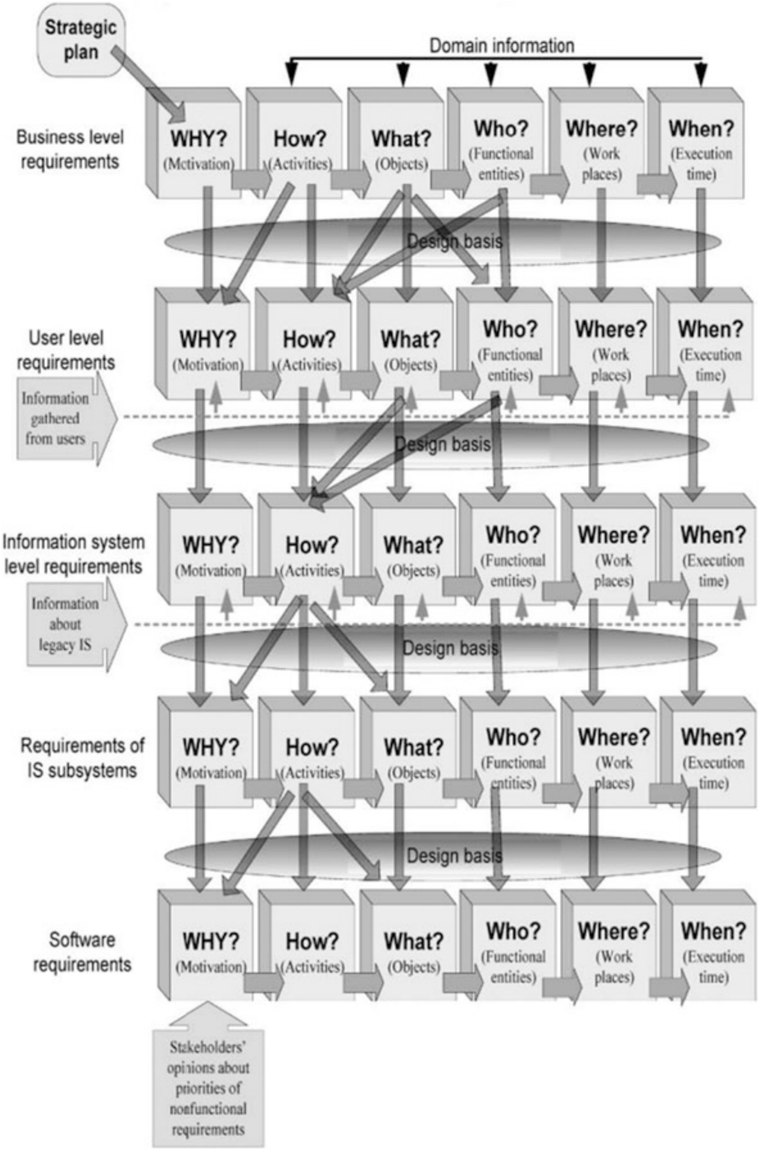
The first diagram provides a macro-level view of interrelation between Legal and IT demission when designing automated reporting processes:


Legal Dimension
IT Dimension
External
(regulations from outside the company)
Law
The set of external regulations using ambiguous natural language that requires an in-depth and up-to-date interpretation.
Artefact Creation
Awareness
IT Compliance Artefact
A set of IT compliance solutions, best practices and metrics both at the process and application level.
Contextualization
Contracting
COSO
Support choice alignment
Artefact Choice
Trends Analysis
Internal
(self imposed regulations)
Organizational Infrastructure
The set of company policies presented in natural language to assign roles and responsibilities on what concerns external regulations enforcement.
To-be Analysis
As-is Analysis
IT Compliance Requirements
The set of statements that identifies the necessary attributes of the company IS system in order for it to comply to internal policies.
COBIT, ISO 27002, GORE

The second diagram provides more granularity by segmenting at a micro-level and the different layers of transcribing a business strategy (e.g. in this case automatic regulatory compliance) into IT steps:

[104] Vytautas Cyras and Reinhard Riedl, "Formulating the enterprise Architecture compliance problem" (2009), page 146 available at (http://ceur-ws.org/Vol-924/paper14.pdf).

[105] To some extent if regulation if fully automated, the concept of compliance culture may become challenged all together.


Strategic plan
Domain information
Business level requirements
User level requirements
Information gathered from users
Information system level requirements
Information about legacy IS
Requirements of IS subsystems
Software requirements
WHY? (Motivation)
How? (Activities)
What? (Objects)
Who? (Functional entities)
Where? (Work places)
When? (Execution time)
Design basis
Stakeholders' opinions about priorities of nonfunctional requirements

The above two illustrations serve and important purpose within the debate around the potential and benefits of RegTech. Indeed before looking at the (re)transcription of compliance obligations into IT processes the first question is much more fundamental—how should Financial Technology itself be regulated?

To date the debate, especially in Asia, seems to be more on understanding what is the best framework so as to provide the right balance between market innovation (e.g. which as seen is beneficial in the case of P2P lending in China) but also market confidence (e.g. again the P2P sector has shown how it can destabilize markets, as show with China's recent stock market volatility).[106]

Furthermore, whilst is the West the topic of RegTech has been developed much more by regulators (with the UK government dedicated a chapter of the Blackett Review[107] on the Topic and Europe is pushing towards increase data transparency with MiFID) in practice there are still uncertainties, as reported by Chris Brummer and Daniel Gorfine,[108] as to whether or not principle based approaches are better suited than rule based approaches.

Therefore it seems that whilst the rational and potential benefits of a fully data driven regulatory system are clear,[109] the application in practice of such a system remains distant. Thus, and in the context of China, it is fair to say that whilst FinTech provides an efficient method to engage into market reform process, neither the regulators nor the industry is ready to fully move compliance into the digital ages. However, and as it will be discussed in the concluding part, this is not to say that China may not export its FinTech innovation.[110]

[106] Unknown, "Some Chinese are take 22 % margin loans to finance sock purchases" (1 July 2015) available at (http://www.bloomberg.com/news/articles/2015-06-30/hidden-china-stock-debt-revealed-in-online-loans-at-22-interest).

[107] Government Office for Science, "FinTech: Blackett Review" (18 March 2015) available at (https://www.gov.uk/government/publications/fintech-blackett-review).

[108] Chris Brummer and Daniel Gorfine, "FinTech: Building a 21st Century Regulator's Toolkit" (October 2014), page 8, available at (http://assets1b.milkeninstitute.org/assets/Publication/Viewpoint/PDF/3.14-FinTech-Reg-Toolkit-NEW.pdf).

[109] Given the fact that the authors expect that wide adoption RegTech in China is unlikely in the next 5 years—potential applicability in the context of P2P lending will not be discussed in length. However, on an introductory note and expanding on the theme of how Shadow Banks transited to P2P platforms, technology could be used to maintain certain benefits of physical networks and originations. Indeed, part of the low delinquency rates of loans made by informal networks can be explained by the social peer pressure emanating from the fact that the borrowers and lenders are from the same community. Furthermore, specific lending groups share not only capital but also expertise. Geographical proximity acts both as a deterrent for borrowers to default but also participate in the skill transfers necessary to improve the success of the enterprises financed by the loan. Therefore, platforms can consider using geo-location as provided by IP addresses of borrowers and lenders so as to geographically match these. Obviously the limitation of this use of technology is that you arbitrarily limit the scalability benefit of the internet as you select only local participants. From a regulators perspective doing the above would also increase concentration risks and perhaps consumer protection risks if the physical proximity favours the recourse of force for debt recollection. Therefore, the benefit might be in creating a balanced ratio between local/regional P2P lenders for any borrower.

[110] See, Gulveen Auakh "Alibaba, Ant Financial invest about $680 million in Paytm, up stake to 40 %" (30 September 2015) The Economics Times, available at (http://economictimes.indiatimes.com/industry/banking/finance/banking/alibaba-ant-financial-invest-about-680-million-in-paytm-up-stake-to-40/articleshow/49148651.cms).

## 5 Conclusion: Leap-Frogging the World?

In closing, this section places the discussion of China's P2P sector within the broader context of the role FinTech plays in China's financial market development. This discussion matters because P2P advances need to be understood as integral to China's objective of devising a framework that supports and supervises the development of digital financial services.

For China the benefit of doing so is clear. As we saw in the second part, P2P lending opened a window of opportunity to regulate the shadow banking industry. Likewise, FinTech also opens the path for a gradual liberalization of the country's financial system. This is done by indirectly introducing competition (via the new private banks) and efficiency (via the use of technology) within a State-owned banking system hampered by legacy IT systems and behavioural biases that end up benefiting SOEs.

Whilst still a work in progress, there have been noticeable developments. Since 2014, there is a clear trend where the government is actively promoting complementary, if not alternative, financial products and services aimed at SMEs and individuals. Indeed Zhou, Arner and Buckley reported that the introduction of the new deposit insurance system has allowed the arrival of "*5 new private banks and approved the establishment of 13 privately controlled financial leasing companies and financial companies affiliated to corporate groups and 162 village and township banks with private sector taking a dominant share*".[111] The latest and most significant policy landmark is without doubt the issuance of the Guidelines on the Promotion of the Healthy Development of Internet Finance[112] on 18 July 2015.

China's Great Leap Forward in 1958, was Mao's objective to quickly transit the country from an agrarian society to one powered by industrialization and socialism. However, when it comes to financial market reforms, the speed at which these occurred was much more gradual, giving to the expression "crossing the river by touching the stones" all its meaning.

This changed in 2007 as China swiftly transited from shadow banking to P2P lending. The country has scratched the surface of the broader trend of financial market structures reformed as a result of technological changes. Looking ahead, it is important for China to reach the balance between supporting the efficiency brought by the financial technology sector, whilst framing this within a regulatory

[111] Zhou, Weihuan and Arner, Douglas W. and Buckley, Ross P., Regulation of Digital Financial Services in China: Last Mover or First Mover? (September 2015), available at (http://ssrn.com/abstract=2660050).

[112] *Guan Yu Cu Jin Hu Lian Wang Jin Rong Jian Kang Fa Zhan De Zhi Dao Yi Jian* (*Guideline on the Promotion of the Health Development of Internet Finance*), promulgated on 18 July 2015. The Chinese official version of the Guideline is here: (http://www.mof.gov.cn/zhengwuxinxi/zhengcefabu/201507/t20150720_1332370.html).

framework that maintains healthy competition and market resilience. To date, this appeared to have been the case. Even though P2P market growth has been explosive, the reform process engaged in by the recent consultation will favor market concentration as opposed to rupture. Not only this, but China has been able to both regulate the industry itself and settle it within a specific complementary role to banks.

Going forward, China is developing a tiered regulatory regime and by doing so, the competitive and liberalization pressure brought by the FinTech sector is manageable, both for regulators but also for incumbent financial institutions. This decision to move towards a tiered regime has consequences beyond China's borders. Indeed, worldwide, the FinTech industry is challenging traditional financial market infrastructure and pre-existing regulatory frameworks, and P2P lending is spearheading this charge.

In the West it is the market itself that is adapting to this shift. The P2P sector is essentially turning towards "Institutional-to-Peer" system and allowing traditional banks to originate loans or deploy excess liquidity in a more effective way.[113] However, China is formalizing this harmonious relationship between banks and FinTech players by creating a tiered regulatory regime. In other words, China is leapfrogging the world in terms of FinTech regulation and building a specific framework for it. Indeed, the UK which is often regarded as the most advanced jurisdiction in terms of FinTech regulation has to its credit moved from a rule- to a principle-based approach, granting slightly more flexibility to new entrants but failing to perfecting a framework for collaboration.[114]

This puts China at the forefront of regulatory developments within FinTech and signals a dramatic change in the origin of where regulatory standards may emerge from. In effect, China is potentially challenging the pre-emminence of the UK and the USA in terms of financial regulation in this area. However in practice we may expect that only developing nations with a similar level of financial infrastructure and necessity for broad market reform (e.g. Vietnam, Malaysia) to look at the China model as a standard.[115]

[113] Zoe Thomas, "Institutional investors eye P2P lending Platforms" (19 June 2015) IFLR, available at (http://www.iflr.com/Article/3463890/Institutional-investors-eye-P2P-lending-platforms.html).

[114] To some extent this is not fully accurate. The FCA has recently engaged into a consultation for the feasibility of opening bank API's to third parties. Furthermore and most noticeably the recent announcement of a regulatory sandbox for spring 2016 would create a very important precedent for the UK and other regulatory bodies globally. See FCA, "Regulatory Sandbox" (10 November 2015) available at (https://www.fca.org.uk/news/regulatory-sandbox).

[115] Arner, Douglas and Barberis, Janos and Buckley, Ross. "The Evolution of FinTech: A new post-crisis Paradigm?" (September 2015) page 30 available at (http://papers.ssrn.com/abstract=2676553).

However, as the country goes from duplication to innovation in terms of financial regulation this creates a new set of risks (inter)nationally. The limited capacity of Chinese regulators to draw from international best practices increases their probability of developing inadequate regulatory frameworks, which may compromise financial market resilience.[116] To the rest of the world and as Fareed Zakaria captured it, this means that "*almost all problems spill over borders.*"[117]

In that context and in the short term, the capacity of China to handle the growth and prevent the burst of the P2P sector will serve as a strong indicator as to the country's capacity to devise a forward-looking financial markets regulatory framework in the 21st century.

**Acknowledgments** The authors gratefully acknowledge the financial support of the Australian Research Council Linkage Grant (Regulating a Revolution: A New Regulatory Model for Digital Finance) and the Hong Kong Research Grants Council Theme-based Research Scheme (Enhancing Hong Kong's Future as a Leading International Financial Centre).

## Author Biographies

**Janos Barberis FinTech HK Founder & Senior Research Fellow Hong Kong University Law School**

Janos Barberis is the founder of FinTech HK, an online hub for Hong Kong's financial technology scene. His expertise focuses on the new regulatory considerations raised by the development of financial technology. He also founded SuperCharger, a FinTech accelerator that focuses on Hong Kong as a gateway to Asia. In 2012, Mr. Barberis proposed to reform unregulated practices in the Chinese banking sector by developing peer-to-peer lending channels. He also introduced the framework for developing real-time and dynamic regulatory supervision models for financial networks. Mr. Barberis holds a Master of Laws degree in Corporate and Financial Law from the University of Hong Kong, a Bachelor of Science degree in Economics and Finance from the University of Southampton and a Bachelor of Laws degree in Law from the University of Birmingham. He received a Research Postgraduate Scholarship from the University of Hong Kong Faculty of Law, and co-authored an academic paper titled "The Evolution of FinTech," which ranked among the Social Science Research Network's Top Ten list.

[116] Ashley Lee, "Chinese deposit insurance to prompt FinTech innovation" (2 April 2015) available at (http://www.iflr.com/Article/3441991/Chinese-deposit-insurance-to-prompt-fintech-innovation.html).

[117] Fareed Zakaria, *The Post-American World: Release 2.0* (W. W. Norton & Co.; 2nd Revised edition, 2011), 34.

**Douglas W. Arner** is a Professor of Law at the University of Hong Kong and Project Coordinator of a major five-year project funded by the Hong Kong Research Grants Council Theme-based Research Scheme on "Enhancing Hong Kong's Future as a Leading International Financial Centre". In addition, he is Co-Director of the Duke University-HKU Asia-America Institute in Transnational Law, and a Senior Visiting Fellow of Melbourne Law School, University of Melbourne. He has published fifteen books and more than 100 articles, chapters and reports on international financial law and regulation, including most recently *Reconceptualising Global Finance and its Regulation* (Cambridge 2016) (with Ross Buckley and Emilios Avgouleas).

# Features or Bugs: The Seven Sins of Current Bitcoin

**Nicolas T. Courtois**

**Abstract** Bitcoin has a number of features and properties which are sometimes presented as interesting and positive. In fact they are closer to engineering mistakes. Serious problems are programmed in the DNA (the source code) of great majority of crypto currencies. Small details in the source code can make very big difference. In this chapter seven major 'sins' of Bitcoin are discussed highlighting risks and suggesting solutions.

**Keywords** Bitcoin • 51 % attack • crypto currency security

## 1 Bitcoin: A Cryptographer's Dream

We call the *Cryptographer's Dream* the idea, prevalent in cryptography research community, of building "trust-less" systems and a "trust-less" society where participants can interact with each other without help of trusted authorities or trusted service providers such as governments, banks, police forces, courts, notaries, etc. The very existence of trusted institutions and services is usually replaced by more or less sophisticated cryptographic techniques, and some weaker "trust assumptions" such as assuming that at least some fraction of participants are trustworthy or/and behave well. Bitcoin (Nakamoto 2008) is a major attempt to achieve just that in the area of currency and payment technology.

Bitcoin has been a tremendous innovation. It is undoubtedly one of the key break-through inventions in human history. In some ways bitcoin has been incredibly successful, achieving a market cap of many billions of dollars and worldwide adoption with millions of more or less active bitcoin addresses. However bitcoin has also fallen short of our expectations in many ways. In fact ever since Bitcoin was

His blog covering crypto currency technology is blog.bettercrypto.com.

N.T. Courtois (✉)
University College London, London, UK
e-mail: n.courtois@ucl.ac.uk

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_6

launched (Nakamoto 2008; Nakamoto et al. 2014) in 2009 it has been always been clear that it is an experimental rather than mature electronic currency ecosystem. A paper at the Financial Cryptography 2012 conference explained that Bitcoin is a system which *uses no fancy cryptography, and is by no means perfect* (Barber et al. 2012). In a more recent paper (Courtois 2014) we have taken the view that Bitcoin and other similar crypto currencies has a number highly problematic **self-defeating** properties, which do not contribute to the success of bitcoin and somewhat create a space for bitcoin clones to thrive. In modern startup culture, very frequently technology push replaces common sense and bugs are presented as features. In contrast, we believe that our duty of academics is first of all to study and inform. Our job is to cultivate an informed debate about advantages and disadvantages of various technical design choices which are inevitably made in every real-life system.

Bitcoin has been a victim of its own success and has created great expectations which it can now hardly live up to. It has for many years already been in an unchartered territory which the mysterious founder (Nakamoto 2008) of bitcoin has clearly not anticipated, for example the centralization of mining (Felten 2014) and the full scope of 51 % threats, see Courtois (2014) and our later Sect. 6. Bitcoin is a relatively simple system yet in which billions of dollars are at stake. While banks and governments spend billions on security, bitcoiners are expected to trust cryptography and wisdom of a handful of developers to steer through all the security pitfalls. This is a lot to ask and surely academics can help in this task too.

In this chapter we explore seven major issues which we view as the most important technical or/and security problems in current bitcoin. Bitcoin has been largely an imperfect design suffering from serious fundamental flaws and things did not always work as predicted. A key observation in Courtois (2014) is that a number of unfortunate engineering mistakes are programmed into bitcoin source code, they are in the DNA of bitcoin. There are also other protocols such as Stratum which have made quite controversial choices, cf. Courtois (2014, 2015). Bitcoin could be quite difficult to fix, as it is not always obvious that the right choice will be made by the bitcoin community, or that they will be made at the right time, and it is simply very naive to believe that the right choices will naturally prevail. Bitcoin allows researchers to discover the task of designing an autonomous decentralized financial system is very hard. On the one side, it seems that bitcoin have already made the impossible possible: it works and has known a relative success. On the other side, the ideal of decentralized crypto currency, which bitcoin has actually created, and the reality of it, are yet very remote. Yet potentially, bitcoin is “good enough” as explained in Antonopoulos (2014). Good enough to achieve some sort of persistent dominant position, cf. Antonopoulos (2014), Courtois (2014), a sort of self-reinforcing natural monopoly due to its tremendous popularity and large adoption (the network effects).

## 1.1 Short Description of How Bitcoin Works

Bitcoin implements a certain type of peer-to-peer financial cooperative without trusted entities such as traditional financial institutions. Bitcoins are essentially entries in a certain public database called *the bitcoin blockchain*, and transfer of bitcoins is like signing a bank check which allows to transfer some bitcoins to a new owner. These checks are part of the official bitcoin history which is stored precisely in this “blockchain” database. Bitcoin is an open protocol in which anyone can participate. A bitcoin equivalent of a bank account is a certain string of some 33 characters which is produced using cryptography, which allows the digital signatures on these “checks” to be implemented: only the owner of a certain secret quantity (known as a private key) can spend bitcoins from one account, while anyone can send bitcoins to that account. All the money transfers ever made in bitcoin are entirely public, except that in principle we do not know who is the owner of any given account.

In addition events in the “blockchain” ledger are hard to counterfeit: participants in the bitcoin network must spend substantial computational effort in order to produce valid blocks. Events are added to bitcoin history in increments called “blocks” and each block contains about 500 transactions. Adding valid events to bitcoin history is very much like burning a DVD: requires both certain relatively costly equipment and to spend energy (electricity). The exact implementation of this is through solving a certain hard cryptographic puzzle which works like a lottery and which we studied in detail in Courtois et al. (2014a, b).

This process of manufacturing the (common) bitcoin transaction ledger has an interesting incentive mechanism: basically participants in this costly process are rewarded with newly created bitcoins. They have strong incentive to be honest, as the bitcoins which they earn for participating are only valid if other participants later confirm their block as being valid and correct. This process is called *bitcoin mining* and works very much like a lottery in which the next successive winner approves a bunch of recent transactions and also the block generated by the previous winner (miner of the previous block). This is expected to create conditions in which it is not profitable to cheat (e.g. falsify the bitcoin history and spend again the same quantity of coins). The bitcoin network is expected to police itself, miners not following the protocol risk that their blocks will be later rejected by the majority of other miners and such miners would simply not get the reward for which they work.

We refer to Sect. 3 of Courtois (2014) and to Lee Kuo Chuen (2015) for a longer description of bitcoin. A more detailed technical description can be found in Antonopoulos (2014) and the primary “official” bitcoin protocol specification is available at Technical Specification of the Bitcoin Protocol (2014).

## 2 Problem 1: Gold Rush Syndrome

Bitcoin digital currency (Nakamoto 2008) is an electronic payment system based on cryptography and a self-governing open-source financial co-operative. In April 2013, the leading global newspaper “The Economist” have famously called bitcoin “digital gold”: a scarce yet highly valuable new high-tech commodity, which is here to stay and shape the future of finance and payment. This is also more or less the date since when bitcoin has been widely recognized and used as a mainstream financial instrument which ordinary people can use.

Bitcoin has also known a "gold rush" which has been short-lived yet highly reminiscent of the historical Klondike gold rush in the 1890s. The rapid appreciation of bitcoin in 2013–2014 and possibility for anyone to mine bitcoins for their own account has transformed bitcoin, at least temporarily, into a potential "get-rich-quick scheme" (Matthews 2014; Mease 2014). In the long run this has not contributed to bitcoin being taken seriously as a payment instrument and its substantial volatility (but also usability) are among the most frequently cited reasons why bitcoin has not known a larger adoption in ordinary commercial transactions (Fig. 1).

Bitcoin has once achieved market price of more than 1000 USD, after which a correction followed. In contrast in the last 12 months the bitcoin price have remained remarkably stable at around 250 USD.

It is also in early 2013 when bitcoin become a major high-tech business topic. A new type of industry have emerged, bitcoin startups, companies which live exclusively within and for the bitcoin economy. In particular companies manufacturing specialized equipment (ASIC machines) the only purpose of which is to produce (mine) new bitcoins very efficiently, cf. Courtois (2014a). It is also in 2013 that bitcoin has transitioned from a geek amateur community to a more professional phase with new bitcoins are produced for profit, by a restricted group of 'bitcoin miners' in which people need to invest money upfront with entry barriers. However, miners, this including ourselves and our friends, have known highly uncertain and disappointing returns on their investment.

In this respect, we have at several occasions such as public conferences about bitcoin, claimed the following conjecture to be true, in practice if not in theory:

**Conjecture 2.1** (Courtois) *Mining is almost always done at* **a loss**.

*Justification 1:* One reason for that could be that the investors have been facing an extremely fast exponential decline in mining profitability. In fact for a very long time in bitcoin history, the income from mining would be divided by two every

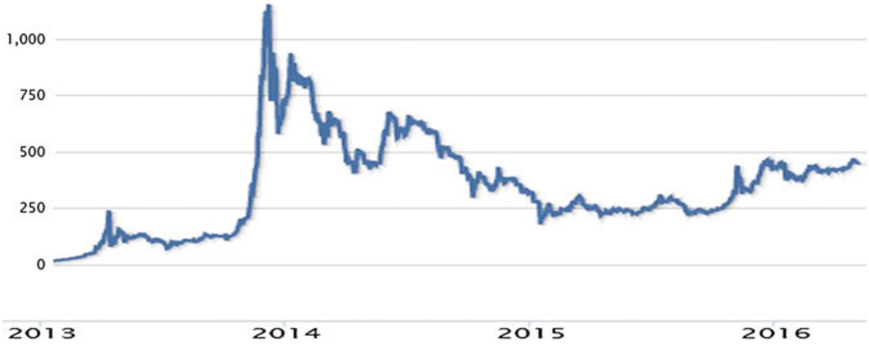


**Fig. 1** The bitcoin price in the last 3 years

month, which is just an incredibly fast decrease unlike for any ordinary investment ever seen, cf. Sects. 2.1–2.3 of Courtois (2014). A quick calculation then shows that the income from mining is not much larger than for example twice the income from the first month of mining. This is a very fast decline in profitability which probably will come as a surprise for many investors. In addition there have been major moral hazards delays and losses due to dishonest ASIC manufacturers, and some outright scams, and generally an asymmetry of power between small and large investors, cf. Sect. 2.4 of Courtois (2014) and Appendix of Courtois (2015) for a detailed discussion and specific examples. Overall investors could very hardly predict the return on their investment correctly and therefore have rather overinvested.

*Justification 2:* We also offer a **privacy economics** argument: freshly mined coins provide anonymity services: they have no origin and cannot be traced to the origin of funds which have been used to purchase mining equipment and pay for electricity. Furthermore, new bitcoins created can be attributed to cryptographic keys chosen independently at random and later transferred to other parties privately (outside of the bitcoin blockchain) without any digital trace-ability for these secondary transfers. These anonymity services are valuable and we conjecture that there will always be a certain non-negligible percentage of people who are willing to mine at a loss. Such miners will contribute to the expansion of the bitcoin hash rate which will negatively affect mining profitability for all miners. It is possible that some investors will anticipate all this and avoid investing in bitcoin mining, and there will be adjustments with investors switching their miners off earlier than planned. However in general many miners are trapped with sunk costs (cost of the mining hardware paid upfront). Therefore a larger number of rational miners will inevitably also mine at a loss in order to recover as much money as they can, and minimize their losses.

## 3 Problem 2: Weak Integrity Protection

This has been a key nearly central question in our work. In Courtois (2014), Financial Times Videos (2015) it has been estimated that more than a billion dollars have been invested into purchase bitcoin miners with the intention of bitcoin mining. This can be seen as a distributed "hash infrastracture" of bitcoin which underpins bitcoin and allows it to run. Arguably the bitcoin cryptographic computation power and hash rate is now just incredibly large, cf. Courtois (2014, 2015). Now the question is, if we put aside the race to acquire a scarce number of new bitcoins and the speculative bid on their future market price, does this "monumental investment" bring additional benefits. For example, does it make bitcoin very robust and secure, so that it could not be broken or abused by some powerful entities. On the surface is seems that yes, for example in (Sams 2014) we read that:

> The amount of capital collectively burned hashing fixes the capital outlay required of an attacker to obtain enough hashing power to have a meaningful chance of orchestrating a successful double-spend attack on the system […] The mitigation of this risk is valuable, […]

In reality, this protection is very largely illusory and ineffective as we are going to show in the present paper, cf. also Courtois (2014). In general it is a fallacy to consider that money currently burnt in hashing serves as an effective protection against attacks. This is because money at risk, for example in large transactions, can be substantially larger than the cost of producing a short term fork in the block chain. It is easy to show that the amount of money needed to commit for-profit double spending attacks remains **moderate** and has nothing to do with hundreds of millions of dollars spent on ASIC miners by investors. Mining is highly centralized due to the fact that most miner mine in miner pools (Courtois 2014; Rosenfeld 2013) and it is sufficient to hack some pool manager servers in order to command a substantial fraction of the bitcoin hash network. A lack of correct appreciation of 51 % attacks is a big recurrent problem in bitcoin community, cf. Sect. 6 below. In addition the current bitcoin specification mandates the so called *The Longest Chain Rule*, and there is a number of additional important technicalities which make things worse and bitcoin even more fragile and more prone to attacks, cf. Courtois (2014, 2015a, b), some of which questions we are going to explain below. We also need to stress that bitcoin could implement additional integrity protections on the top of existing ones, some such ideas are outlined in Sect. 7 of Courtois (2014).

## 4 Problem 3: Poor Speed and Instability

The current bitcoin has been designed to be truly decentralized and function in an asynchronous way even in highly imperfect network conditions. The key underlying principle which allows to achieve this objective is **the Longest Chain Rule** of Satoshi Nakamoto (Nakamoto 2008). It can be stated as follows:

1. Sometimes we can have what is called *a fork*: there are two equivalent solutions to the cryptographic puzzle, or two equally valid blocks are mined.
   This happens about 1 % of the time, cf. Table 1 in Courtois (2014b).
2. Different nodes in the network have received one of the versions first and different miners are trying to extend one or the other branch. Both branches are legitimate and the winning branch will be decided later.
3. The **Longest Chain Rule** of Nakamoto (2008) says that if at any later moment in history one chain becomes longer, all participants will switch to it automatically.

With this rule, Satoshi have shown (Nakamoto 2008) that that bitcoin should quickly reach a consensus. Importantly this rule is also how bitcoin attempts to solve the problems of 51 % attacks and fraud or double spending.

### 4.1 Genius or Engineering Mistake?

We are now going to explain why this rule is problematic. In fact this same consensus mechanism in bitcoin is a solution to two entirely distinct problems:

1. It allows to decide **which blocks** obtain a monetary reward and resolve potentially arbitrarily complex fork situations in a simple, elegant and convincing way.
2. It is also used to decide **which transactions** are accepted and are part of official history, while some other transactions may be rejected.

Overall one single mechanism to rule both blocks and transactions is rather a mistake. For example it violates one of a well-known principles in security engineering: the principle of *Least Common Mechanism* (Saltzer and Schroeder 1975), cf. also Courtois (2009). We need to observe that the transactions are generated at every second. Blocks are generated every 10 min. In bitcoin the **receiver of money is kept in the state of incertitude for far too long** and this **with no apparent reason**. The current bitcoin currency produces a situation of discomfort and dependency or peculiar sort. Miners who represent some wealthy people in the bitcoin network, are in a privileged position. Their business of making new bitcoins has negative consequences on the smooth processing of transactions. It is a source of instability which makes people wait for their transactions to be approved for far too long and delays their acceptation cf. Courtois (2014), Financial Times Videos (2014). At then end of the day this ends up violating also another very widely accepted principle of security engineering: the principle of *Network Neutrality*. We claim that it should be possible to design a better and **faster** mechanism in bitcoin, cf. Courtois et al. (2014), Courtois (2014).

## 5 Problem 4: Bitcoin Monetary Policy

In crypto currencies, the central bank and the monetary policy which is expected to regulate the number of coins in circulation has been simply replaced by a relatively simple algorithm. In traditional fiat currencies, the main objective of a successful monetary policy is to control the inflation, insure financial stability and overall healthy functioning of the economy. In crypto currency we also have that, except that the original bitcoin monetary policy is quite peculiar. It is clearly the one thing which is the most frequently modified by designers of various bitcoin clones with a whole array of interesting variants which generate new coins at different speed according to some pre-determined scheme.

Interestingly in crypto currency and unlike in traditional currencies, this algorithm or monetary policy plays a sort of **dual role**. It surely regulates the bitcoin monetary supply and the bitcoin economy, but it also has a **security function**. Production of new coins in an incentive for miners to behave well and not abuse the network, and if this incentive is removed, the network will be less secure against for example 51 % or double spending attacks (our primary focus). In bitcoin the total number of bitcoins ever to exist is bounded by 21 million, which property has been very frequently criticized. In Wired Entreprise (2013) J. Kroll from Princeton university explains “This limited-supply issue is the most common argument against the viability of the new currency”. We refer to Sect. 5 of Courtois (2014) for a detailed discussion. A fixed monetary supply implies that the income from mining is bound to decline substantially in the future. This has alone has serious security consequences as explained also in Wired Entreprise (2013) “there will be no incentive for people to keep contributing processing power to the system […] If the miner reward goes to zero, people will stop investing in miners,”. Then the hash rate is likely to decrease and bitcoin will no longer benefit from a protection against double spending attacks.

Moreover the author explicitly says that the problem is NOT solved by transaction fees and says: […] You have to enforce some sort of standard payment to the miners, […] change the system so that it keeps creating bitcoins. In a paper presented at WEIS 2013 and co-authored by Kroll (2013). this is presented as a clear dilemma, either break the monetary policy or increase the fees. Yet increasing the fees is something which is likely to destroy bitcoin. This is brilliantly explained by Sams (2014). The argument is that basically sooner or later “deflationary currencies” and “growth currencies” will be in competition. Then all the other things being more or less in equilibrium, in deflationary currencies most of the profit from appreciation will be received by holders of current coins through their appreciation. Therefore less profit will be made by miners in these currencies. However miners control the network and they will impose higher fees. In contrast in growth coins, there will be comparatively more seignorage profit and it will be spent on hashing. Miners will make good profits and transaction fees will be lower. Thus year after year people will prefer growth currencies due to lower transaction fees.

Overall we see that this is crucial question of how the cost of the infrastructure necessary for the maintain a digital currency is split between new adopters (which pay for it through appreciation) and users (which pay through transaction fees). It is obvious that there exists an optimal equilibrium between these two sources of income, and that there is no reason why the creator of bitcoin could possibly get it right. Serious adjustments should become necessary in the future.

## *5.1 The Appreciation Argument*

There is yet another argument: it is possible to believe that bitcoin will appreciate so much that halving the miner reward (currently every 4 years in bitcoin) will be absorbed by an increase in bitcoin price. We claim that this is unlikely. This is mainly because the bitcoin adoption has been stable in the recent years and sometimes even declined (cf. Sects 2.5 and Fig. 9 in Courtois (2014). Therefore we find it very hard to believe that it is going to double every 4 years [this would be very fast] and even less it is expected to double by sudden jumps at the boundaries of the intervals arbitrarily decided by the creator of bitcoin.

The overall conclusion is that it is easy to see that the bitcoin current restricted monetary supply is a **self-defeating** property on at least two accounts:

1. If bitcoin is limiting the monetary supply beyond what is 'reasonable', and if as a result of this bitcoin economy suffers from excessive deflation, bitcoin adopters are likely to circumvent this limitation by using alternative coins. This is likely to erode the dominant position of bitcoin.
2. With time the miner reward in new bitcoins per block decreases and tends to zero. Then actual cost (in bitcoins) of manufacturing each new block will also tend to zero, and the price tag (in bitcoins) for creating a fork in bitcoin blockchain should also tend to zero, while the amount of money (in bitcoin) at risk of double spending in each block, does not decrease. Then with time it becomes increasingly easier and more profitable to commit fraud in bitcoin blockchain.

The only solution to this problem we are aware of, is to reform the bitcoin monetary policy.

## 6 Problem 5. Misunderstanding the Threats

A common misconception in bitcoin is that a 51 % attacks are hard to do and are about very powerful attackers (Nakamoto 2008; Perry 2012). In reality there is a much larger variety of attacks which could be or should be called a 51 % attack and not all of them are difficult and expensive. It appears that there have been a lot of confusion around this questions in the bitcoin community and almost everybody, including the legendary anonymous founder of bitcoin Satoshi Nakamoto, gets it wrong in some substantial way. In a paper linked by the official bitcoin wiki (Perry 2012) we read that "the 51 % attack is the oldest and best-understood attack in all of Bitcoin". In reality, it is rather the least well understood attack in bitcoin. In this section we provide an introduction and brief discussion of this question and we try to underline the key issues.

**On Powerful Attackers.** We hear about 51 % attack and powerful entities who own or control 51 % of hash power and it seems that only incredibly powerful or wealthy people (Antonopoulos 2014; Cawrey 2014; Perry 2012) could execute such attacks using "every top-secret ridiculously expensive supercomputer" as claimed in Perry (2012). In Antonopoulos (2014) we hear that the practical effort required to run such an attack is "ridiculous", at least 100 million dollars of equipment OR the collaboration of a massive distributed network of miners. Many commentators stress that 51 % attack are only *theoretical* attacks, cf. Antonopoulos (2014, Perry (2012, Wong (2014), and try to convince us to "stop worrying". The official bitcoin wiki, does even consider that there are any real problems in bitcoin. The section about 51 % attacks does NOT even get into the part entitled “Might be a problem”. It appears in the following part entitled “Probably not a problem”, cf. Official Bitcoin Wiki (2014) which many people would maybe not read, why bother if it probably is not a problem?

**Satoshi on 51 %.** The very serious misconceptions on this topic go straight back to the original paper of Satoshi. The inventor of bitcoin describes “a greedy attacker” being “able to assemble more CPU power than all the honest nodes”, see Sect. 6 in Official Bitcoin Wiki (2014). The attacker is also portrayed as having considerable “wealth” which he would endanger by engaging in the attack. It is clearly suggested that the attack would have little to gain and a lot to lose from being dishonest.

Satoshi has invented a term “CPU power” and always explicitly states the principle of “one-CPU-one-vote”. In reality nowadays it is rather “one-ASIC-one-vote”. A reasonable term is “**hash power**” commonly measured in GH/s where one hash per second is a capacity to hash one block header. cf. Courtois (2015).

**Control versus Ownership.** In general a very common mistake is to claim that 51 % attacks occur when the attacker **owns** or is in **possession** of 51 % of all the hash power. This mistake again goes back to Satoshi (Nakamoto 2008) and is committed again and again by major Bitcoin experts and evangelists, cf. for example Cawrey (2014), Perry (2012). The Official Bitcoin Wiki (2014) has a subsection with this super highly misleading title: “Attacker has a lot of computing power”. Quite happily just below they correct it and say it is rather about temporary control not ownership.[1]

Most people fail to see that the key problem is the control (not ownership) of hash power for the purpose of mining blocks, and this can be **a lot** easier and cheaper. For example the attacker could be one single malicious pool which gathers more than 51 % of hash power under his sole control (controlling but not owning hash power). It is worth noting that this situation has already happened at least once in both Bitcoin, Litecoin and Dogecoin Courtois (2014).

Another serious mistake is to consider that “control” is exclusive. For example in the Abstract of his paper Satoshi writes: “As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network they’ll [...] outpace attackers”. This is not correct in general. The key point is that **control is NOT exclusive**, both the miners and the attacker can have some control on the mining process. So “a majority of CPU power is controlled by nodes” as Satoshi says and also at the same time it could be controlled by the attacker in a more or less subtle ways, cf. for example Sect. 8.3 in Courtois (2014).

[1] They explain that the exact scenario is when he “controls more than 50 % of the network’s computing power” and they make it clear it can be temporary: “for the time that he is in control”. However almost to make things worse again, this official wiki at numerous places refers to another article about Bitcoin attacks written for more general audience (Perry 2012) which again claims that 51 % attacks are “so amazingly cost-prohibitive to perform”.

**On Visibility.** Many people stress that that 51 % attacks, and for example double spending events would be visible to anyone to see on the public blockchain (Cawrey 2014). This is simply not true, the bitcoin blockchain does NOT record double spending events, it rather hides them and would show only one transaction out of two, cf. also Decker (2014).

## *6.1 Emerging Threats*

The notion of a 51 % attack takes a very different meaning in a cloud computing world: the attacker does not need to own a lot of computing power, he can rent it for a short time, and then a 51 % attack can have a surprisingly low cost. In addition one should not assume that threats are static, while they can be ephemeral and dynamic, e.g. man in the middle attacks.

Alternatively an attacker could also trick miners to help him to execute the attack without their knowledge and consent (man in the middle attacks). This is particularly easy with mining pools: the attacker just needs to compromise extremely few web servers used by tens of thousands of individual miners and he can command very substantial hash power without owning any of it. At this moment less than 10 pools control over two-thirds of all the hash power, cf. Courtois (2014), Todd (2014).

**Birth of Centralization.** It is important to remember that not only Satoshi did not predict ASIC mining and mining pools, but also he did **NOT specify** bitcoin fully in the sense that the mining pools typically use the Stratum protocol (Marek (slush) Palatinus 2014). This protocol was specified in 2012 and it took **an important strategic decision** about the future of bitcoin which is clearly stated in documented in Marek (slush) Palatinus (2014) which allowed to move the choice and the control of which transactions are included in a block from miners to the pool managers, see Courtois (2015, Marek (slush) Palatinus (2014). This decision **broke the bitcoin peer network** because miners do no longer have any incentive whatsoever[2] to support this network by running peer nodes, and the bitcoin peer network has been seriously declining in 2014–2015, cf. Cawrey (2014).

In fact, even if large pools had only 10 % of hash power each, we should see reasons to worry: it would be sufficient to hack just 5 pool manager servers in order to be able to command 51 % of hash power and execute double spending attacks.

**Is Bitcoin Secure?** Nobody has yet stated under which exact assumption bitcoin is expected to be secure and there is a lot of ambiguity in this space. Knowing the assumption is crucial because if we have stated our assumption and bitcoin is later

[2] This decision also has definitely infringed on the initial intentions of Satoshi explicitly stated in Sect. 6 of his paper (Nakamoto 2008) where he explains that the fact that a block provides a monetary reward for the “creator of the block” is something which “adds an incentive for nodes to support the network”. This incentive is now broken.

shown to be broken insecure, we can blame **either** the real world which does not satisfy our assumption, or the designers and engineers of bitcoin which have not been able to design a secure system based on this assumption. In other worlds we could determine without ambiguity who is to blame. In this respect Satoshi shows a bad example of not being clear about what his assumption is and yet explicitly several times claiming that his system is secure:

A. For example in the abstract of his paper (Nakamoto 2008) Satoshi says that he assumes that "majority […] are not cooperating to attack the network". Here Satoshi claims the system is secure under this assumption, which security claim is **not true** as people can easily be part of an attack without cooperating (as already explained above).

B. Now in the conclusion of his paper Satoshi again claims that the system is secure if "honest nodes control a majority of CPU power". which is a very different and STRONGER assumption than A. above: nodes could be not honest and deviate from the protocol for fun or for profit in a variety of creative ways without "cooperating" with any attacker.

   Does this stronger assumption make that bitcoin becomes secure? Of course not, the security result claimed by Satoshi is wrong again if you take it literally: even if honest nodes control a majority of hash power, because the control is not exclusive, bitcoin can still be attacked.

**On The Honest Option** It is nonsensical to claim that the attacker would prefer to behave honestly, and that it is "more profitable to play by the rules" (Nakamoto 2008). This is claimed by Satoshi on the grounds that the attacker should be able to "generate new coins" which would be an honest way to use his hash power, see Sect. 6 of Nakamoto (2008). In reality, in almost all bitcoin mining scenarios known to us, the attacker does NOT control the money from mining: he does NOT have the private keys used for mining. This is because **the whole process of mining requires exclusively the public keys**. It would simply be an unnecessary mistake for any miner or for any mining pool to have the private keys around to be stolen by the attacker which targets the mining process. Therefore the attacker typically does NOT have an honest option at all.[3]

**On Percentages.** The notion of 51 % attacks is also very highly misleading because presenting the hash power as a percentage figure does NOT make sense because the hash rate is measured at two different moments. Therefore the proportion of hash power used in attack is NOT a number between 0 and 100 %. It could in particular be larger than 100 %. In fact the relative hash power at one moment can be easily of the order of 500 % and many times bigger than a few minutes later, cf. Courtois (2014) for an actual historical example.

[3] In contrast Satoshi have claimed that he always has such an option, in Sect. 6 of Nakamoto (2008) we read: "he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins."

**Miners versus Adopters versus Pools.** It was also sometimes wrongly assumed that the bitcoin adopters are more or less the same as miners, they own the devices and the computing power cannot change hands very quickly.

It is in general not sufficient to trust the pools not to be malicious. Attacks could be executed without the knowledge and consent of these companies by a single rogue developer.

**Bitcoin Versus Competitors.** Many bitcoin adopters did not anticipate that in the future bitcoin will have to compete with other crypto currencies and that hash power could instantly be moved from one crypto currency to another, these questions have been studied in detail in Sects. 10–11 of Courtois (2014).

Attacks could also operate through re-direction of hash power in bulk to another pool, such attacks are studied in Sects. 8.2–8.3 of Courtois (2014) and in Courtois (2015).

In the same way, people wrongly assume that bitcoin achieves very substantial computing power which no one can match, which is still the case today however it is quite problematic to see if this will hold in the future.

**Rented Cloud Miners.** Attacks can be facilitated by the fact that an increasing fraction of all available computing power in bitcoin exists in the form of rented cloud miners. This situation is due to several factors. Investing in wholly owned mining equipment has been excessively risky. This is both due to the impossibility to know if and when miners will effectively be delivered (cf. Appendix of Courtois (2014, 2015) and due to the price volatility. Investing in short term rented mining capacity is clearly less risky. Another reason is that some large investors may have over-invested in large bitcoin mining farms consuming Megawatts of electricity (we know from the press that such facilities have been built in Sweden, USA, Hong Kong, China, Georgia, etc.) and now they want to rent some parts of it in order to get immediate cashflow and return on their investment. Furthermore renting hash power leads to the possibility of running for-profit attacks with cooperating peers who may or not be aware of participating in an attack, see Sect. 7.9 in Courtois (2014) which describes a real-life company which allows to facilitate double spending attacks and proposes to miners to rent their computing power to others for a small reward premium.

## *6.2 Is the Problem not Already Solved?*

There is some sort of intuitive understanding in the bitcoin community that the Longest Chain Rule solves all problems in this space, and there is simply no problem, or if there is, it is probably not very serious. In our experience very few bitcoin enthusiasts are willing to admit that the brilliant creator of bitcoin could have created a system which has serious security problems.

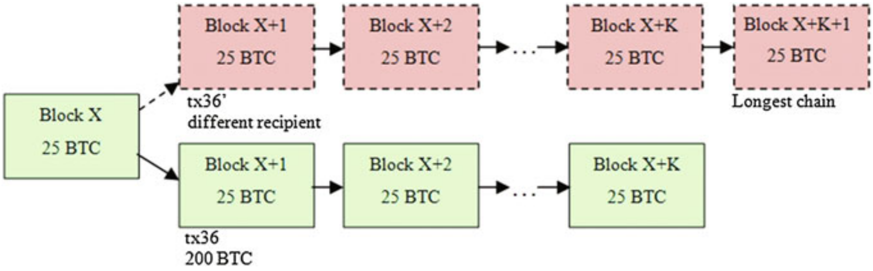


**Fig. 2** A simple method to commit double spending. The attacker tries to produce the second chain of blocks in order to modify the recipient of some large transaction(s) he has generated himself. Arguably and under the right conditions, this can be quite easy to achieve. The attack is clearly profitable and the only problem is the timing: to produce these blocks on time

For example many authors claim that the problem has already been fixed: and that the fix is to wait for 6 confirmations, cf. Perry (2012). In fact if a lot of money is at stake in a large transaction (or in many small transactions) it is possible to see that a larger attack could be mounted, e.g. as in later Fig. 2. In general as the money at stake involved in each block is likely to grow in the future, the risk will also increase and we agree with Official Bitcoin Wiki (2014) to say that "no amount of confirmations" can fix this problem. More confirmations are needed for larger transactions.

In this section we have shown that 51 % attacks have been historically extremely poorly understood and very few sources get it right. It clearly is a complex problem which involves a variety of attacks and threats which deserve to be taken seriously.

## 7 The Basic Blockchain Manipulation Attack

In this section we outline a fundamental attack on bitcoin the primary application of which is to manipulate the recent history of bitcoin for profit, for example in double spending. On the surface it is a well known (folklore) attack. However it is also clear that it has not yet been studied in due detail and that it admits endless interesting variants. We follow very closely and some of the analysis of Courtois (2014) however we are very far from addressing all possible attacks and threats, we refer to Courtois (2014, 2015a, b) for pointers to other works on bitcoin blockchain attacks.

The basic version of this attack is self-explanatory. Some attacker produces a fork in order to cancel some transaction[s] by producing a longer chain in a fixed interval of time, see Fig. 2.

The attack clearly can be profitable as $200BTC > K \cdot 25BTC$ and $K$ is small. The question of actual feasibility of this attack is a complex one, it depends on many factors. We refer to Sects. 6 and 8 in Courtois (2014, 2015) for a longer extended discussion of interesting ways in which this sort of attack can become feasible.

The key observation is that the attacker does NOT need to be very powerful, on the contrary. The most shocking discovery is that **anyone** can commit such fraud and steal money. They just need to rent some hashing power from a cloud hashing provider. This needs only to be done only for a very short time, like less than 1 h, for example through redirection (man-in-the-middle attack) of hash power which is in the physical possession of other miners but under “logical” control of extremely few pool manager servers. In a competitive market they do not need to pay a lot for this. Not much more than 25 BTC per block. This is because miners do not mine at a loss, or maybe at a small loss cf. Conj. 2.1 page 4 and therefore the inherent cost of mining one block should be just about 25 BTC. The attacker then just needs to temporarily displace the hashing power from other crypto currencies for a very short period of time which is easy to achieve by paying a small premium over the market price. We should note that rapid displacement of hash power happens every day in crypto currency community, see Sects. 10–11 in Courtois (2014).

## *7.1 The Question of Dominance*

It is important to understand that what we present in Fig. 2 is already feasible to execute today for nearly anyone, not only for rich and powerful attackers. Then as we advance in time, such attacks are expected to become easier, cf. also Sect. 5.1.

At this moment bitcoin is a dominating crypto currency: its hash power is substantially larger than for other crypto currencies combined. It appears that bitcoin could claim to be a sort of natural monopoly: it is able to monopolize the market and its competitors find it hard to compete.

Now the attack will become particularly easy if bitcoin ceases to be a dominant crypto currency. At this moment the attacker needs for example to hack some (very few) pool manager servers in order to execute the attack. But if there is plenty of hash power available to rent outside of bitcoin, the attacker will be able to execute the attack without doing anything illegal (except possible legal consequences of canceling some bitcoin transactions). At this moment will be quite easy to execute double spending attacks on many existing crypto currencies.

For example in April 2014 one single miner owned 51 % of the hash rate of Dogecoin, cf. Sects. 10–11 in Courtois (2014). We do not know if this could happen to bitcoin itself, it is potentially stronger and could potentially remain dominant and protected from this threat forever, but we see that crypto currencies can undergo “destructive” transitions from a secure state to an insecure state (Courtois 2014).

## 7.2 Attacks with Hash Rate Displacement

For example here is what happened to the UNO hash rate in 2013: it has declined in a very substantial way each time the miner reward has been decreased.

Similarly, the hash power has been moving from Dogecoin to Litecoin in very substantial ways. This was due to the Dogecoin monetary policy which has decreased the mining incentive. This resulted to a progressive transition in several steps from a situation in which both currencies had a nearly-equal hash rate and no currency could convincingly attack the other, towards a situation where a fraction of hash power used by Litecoin miners could be used to abuse the users of Dogecoin and double spend, in a way steal someone's coins.

It is important to note that shortly after we have written about this threat, the founder of Litecoin have proposed a fix to the Dogecoin community which they have later adopted, in the form of so called merged mining, which indeed fixes this problem. In particular Josh Mohland, one of the key architects behind Dogecoin have agreed with us that without a reform Dogecoin would basically face **certain death**, at least in the sense of double spending attacks, cf. Higgins (2014) (Figs. 3 and 4).

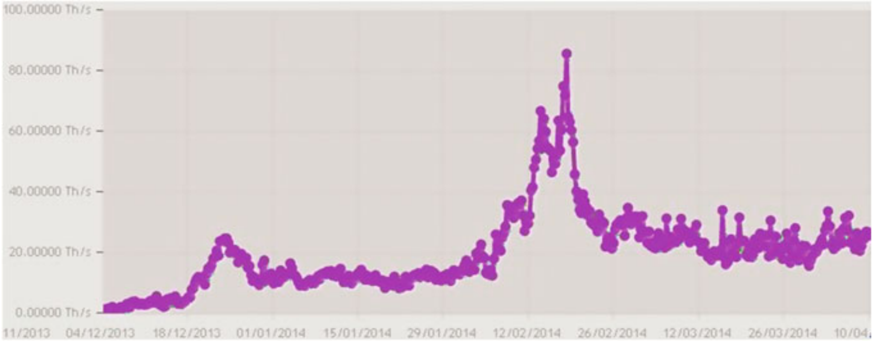


**Fig. 3** The growth and decline of UNOBTANIUM hash power in 2012/2013. we observe sudden jumps and periods of intensive mining followed by steady decline in days following each block halving dates in the hash power

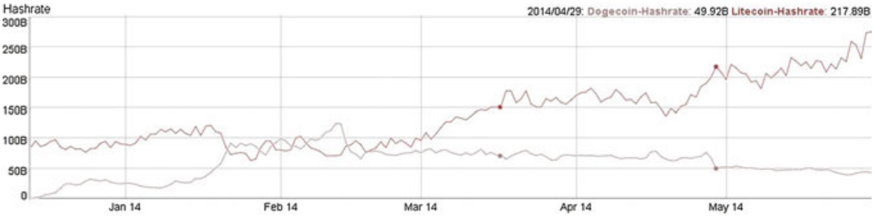


**Fig. 4** DOGE hashrate compared to LTC hashrate in early 2014

We refer to Sects. 10–12 in Courtois (2014, 2014) for a further discussion of these questions. In general it is believed that merged mining can solve this problem. However merged mining between litecoin and bitcoin is NOT possible because these currency use different incompatible hash functions and require different entirely incompatible hardware ASICs.

# 8 Problem 6: Dangers of Open Source

## *8.1 The Question of Bitcoin Source Code*

Bitcoin has this "anonymous founder" syndrome. There were numerous security scandals in which a lot of bitcoins have been stolen (Decker 2014). Alt-coins are much more vulnerable as shown above and in Courtois (2014). All this can create some uneasy feelings. In general it is a common misconception to believe that open source code is most probably secure. We don't believe this to be correct Anderson (2005), Courtois (2009) in general. In bitcoin we need to ask ourselves a number of questions:

1. Why should open source code be secure if very little or insufficient effort is typically made in order to make it secure?
2. In the traditional industry developers are paid, and seem to never get the security right: we have endless security breaches and alerts. There is little hope that bitcoin developers can do better.
3. For example the Dogecoin developers and promoters did not want to admit any responsibility for their actions. They have said that Dogecoin was never "intended to function as a full-fledged transaction network", citing (Higgins 2014) and that yes it was going towards a "certain death", mostly and exactly for reasons exposed in our papers, Can we hope that bitcoin developers will be more responsible?
4. Actually open source software is not more secure than closed source according to experts (Anderson 2005). Moreover quite possibly, on the contrary, it will be less secure. Malicious developers are **more** likely to work on such source code than honest developers. This is because rogue developers will be motivated by profit, while honest developers may see little incentive to work on this code. Accordingly, a recent paper (Maese 2014) takes a view that:

> The open-source nature of the developer population provides opportunities for frivolous or criminal behavior that can damage the participants in the same way that investors can be misled by promises of get rich quick schemes. […] Regulations could ensure that cyber-security requirements are engineered into the code […] One of the biggest risks that we face […] in the digital age […] is the quality of the code that will be used to run our lives.

More generally we need to address the question of how an open source system such as bitcoin nevertheless hope to be secure and trusted.

### *8.2 Bitcoin and the Open Design Principle*

We recall one of the most important principles of computer security and modern security at large, the **open design** principle (Saltzer and Shroeder 1975). On the surface, bitcoin seems to be an open design. We have a white paper, the original paper of Satoshi (Nakamoto 2008) and more detailed specification (Todd 2014) and source code (Nakamoto et al. 2014).

A closer examination reveals that the open source and open design are two **different** things and the open source model suffers from some major problems. An open design should mean that we should NOT use any cryptography standards of questionable origin, or run source of code of unknown origin. Unhappily a lot of code and also the cryptography in bitcoin has obscure origins. Bitcoin cryptography is clearly a closed design. 100 % of the cryptography standards in bitcoin have been developed entirely behind closed doors at the NSA, and there is some ambiguity about to what extent these standards are secure.

### *8.3 Open Design, Bitcoin and Kerckhoffs' Principle*

In cryptography we have another well known Kerckhoffs' principle from 1883: "The system must remain secure should it fall in enemy hands", cf. Courtois (1883, 2009). Most of the time this is incorrectly understood. Kerckhoffs does NOT say there is an obligation to disclose. It says that the system should be secure when the specification is disclosed, and potentially we could have better security when not disclosed, see slides 142–156 in Courtois (2009) for a detailed discussion. In particular full disclosure can be really dangerous. The Open Design principle as explained above CAN coexist with partial disclosure and with Kerckhoffs' principle (Kerckhoffs 1883). Avoiding full disclosure when it is not necessary allows to layer the defences, cf. Courtois (2009). It is also a very common thing to do in the financial industry: typically public keys are NOT disclosed in real-life financial systems (e.g. with bank cards) and this is also frequently the case in bitcoin: only a hash of a public key is disclosed by default.

## 9 Problem 7: Bitcoin Elliptic Curve

As we have already explained, bitcoin violates the principles of open and transparent design because 100 % of the cryptography standards on which it depends have been developed entirely behind closed doors. However this is also the case for most industry firms. Is cryptography in bitcoin in any way less good than the cryptography used by major security vendors? Yes it is!

Bitcoin uses elliptic curve cryptography. Here is what Neal Koblitz himself, one of the two inventors of this form of cryptography, and member of advisory board of Ethereum meant to be a successor of bitcoin, have once written about untested cryptography assumptions:

> in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed. In academia, if you write about a cryptosystem and then a few months later find a way to break it, you've got two new papers to add to your résumé! Neal Koblitz, cf. Koblitz (2007).

In bitcoin we have precisely this: an utterly untested elliptic curve cryptography system which nobody ever uses, except in bitcoin, and which no cryptography expert would recommend for any serious application. This problem could be very serious and yet remains largely ignored in bitcoin community. It has been discussed only in some obscure forums (Topic: NSA 2897). In contrast, the official bitcoin wiki claims exactly the contrary, that "Bitcoin has a sound basis in well understood cryptography", cf. Bitcoin (2014).

In fact bitcoin does NOT use a standard elliptic curve which serious people use or would recommend to use. It uses a very peculiar type of elliptic curve, sometimes called "a Koblitz curve" and more precisely the so called secp256k1. This curve is not an ordinary choice. It has an unusually simple equation which contains only very small integers:

$$y^2 = x^3 + 7 \bmod p$$

This sort of bizarre curve remains officially unbroken in the open research community, in spite of the fact that tens of academic papers are published each year about attacks related to small integers in public key cryptography. This elliptic curve is characterized by the so called "small class number" which some researchers suspect to be less secure than general curves, see Sects. 5.1 and 5.3 in Galbraith and Smart (2014). cf. also Bernstein et al. (2014). The bitcoin elliptic curve has the lowest $|D|$ of all known standardized elliptic curves, cf. Bernstein and Lange (2014) and therefore it is potentially the least secure. Following Bernstein and Lange (2014) such curves allow slight speedups for discrete log attacks however "the literature does not indicate any mechanism that could allow further speedups". To summarize no really serious attack is on such curves is known. However in cryptography there has always been a tremendous level of suspicion against such "very special" cryptographic objects. History have taught us that in cryptography special usually means broken.

Koblitz curves in characteristic p were invented by Gallant, Lambert and Vanstone cf. Galbraith and Smart (2015). and was initially recommended by the Standards for **Efficient** Cryptography Group (secg.org) which is an industry consortium created in 1998 by the Canadian Certicom company in order to popularize efficient ECC solutions. and it is recommended in ANSI X9.63 version from 2011. It is implemented in OpenSSL but not for example in GnuTLS. It is not in general widely used in the industry, because simply most academic cryptography experts would not trust and would never recommend this peculiar curve secp256k1 as used in Bitcoin.

**Timely Denial.** More importantly, SECG itself does no longer recommend this elliptic curve. Here is what Dan Brown, the SECG chair has written in September 2013:

> I did not know that BitCoin is using secp256k1. I am surprised to see anybody use secp256k1 instead of secp256r1.

We refer to Topic: NSA (2897) for more details. The only correct way to interpret this statement is that this elliptic curve is NOT supported and not recommended by the very people who have standardized it in the first place. It should no longer be used in bitcoin and no one should use it. It is very much like using Windows XP today in 2015, even though it is no longer supported and Microsoft and using it is simply dangerous.

## *9.1 Urgent Action for Bitcoin Community*

It is not difficult to switch to another elliptic curve and such a change can happen overnight without any problems. It would take 5 s to implement this change in current software and make it also accept the signatures with the old elliptic curve for some time.

It might seem that such a change would be ineffective because of the co-existence of new and old signatures. On the contrary, it would be immediately effective. All the moneys transferred to new addresses would be safe, EVEN IF the older Koblitz curve was badly broken. Therefore this change would immediately protect money of anyone willing to create a fresh bitcoin address, and abandon their old address, which is easy and could be automatically done by a majority of upgraded bitcoin software (such large scale address updates have already been done many times in bitcoin community without any problems).

## *9.2 A Fix for Individual Bitcoin Users*

There is also a solution for individual users. Yes, users of bitcoin can also fix this problem themselves, even today. They should basically never reveal their public key (the bitcoin address is a hashed version, it does NOT reveal their public key) and always destroy this key (never use it again) each time it is used, and send the remaining balance to a new freshly created address.

Thus the attackers who are able to break secp256k1 keys will have much less time: instead of having many months or maybe years to break it, they need to do it instantly within a few seconds or all the money at this address will be gone forever. Unhappily many existing bitcoin applications such as Bitcoin core do NOT yet facilitate implementing this sort of policy.

## 10 Summary and Conclusion

Bitcoin has a number of features and properties which are sometimes presented as very interesting and positive. In fact they are closer to engineering mistakes. Most of these features have been blindly copied by other currencies, so called alt-coins which typically change only the monetary policy and leave other features unchanged. Naive customers are presented with software systems which are claimed to be payment systems and currencies which creates expectations that they will be relatively stable and that they are protected against attacks. In reality serious problems are programmed right there in the DNA (the source code) of great majority of crypto currencies. Small details in the source code can make very big difference, for example the choice of the elliptic curve used to secure bitcoin transactions.

In our work we show that the question of 51 % attacks are almost never correctly understood and most crypto currencies simply do **NOT** yet have a good protection against major attacks, cf. Sects. 6–7.2. In addition sudden jumps and rapid phase transitions in miner reward are programmed at fixed dates in time which can lead to the decline of some currencies, cf. Sect. 7.2 and Courtois (2014). More importantly, hash power redirection attacks can just temporarily displace the hash power or abuse miners without their knowledge, cf. Sect. 6 and Courtois (2014). We discovered that the *Longest Chain Rule* does not solve the problems of bitcoin consensus in an appropriate way. It is probably OK for deciding for which blocks miners will obtain a monetary reward However there is no reason why **the same exact slow and unstable mechanism would also be used to decide which transactions are valid**. **This is NOT a feature, it is a bug,** An engineering mistake on behalf of Satoshi Nakamoto, the founder of bitcoin. It affects not only the security of bitcoin but also its usability: it makes transactions **unnecessarily slow**, especially for larger transactions which require more confirmations. Bitcoin could potentially be a lot faster, cf. also Financial Times Videos (2014).

In general, all the 51 % and double spending vulnerabilities can get substantially worse with time see Sects. 5 and 7.2. Here rewarding the creators and early adopters conflicts with allowing the miners a decent income later on. The current monetary policy is another very major self-defeating property of many existing crypto currencies. Accordingly the 51 % attacks are somewhat bound to get worse with time: the cost (in bitcoins) of orchestrating a double spending attack on bitcoin is likely to decrease, while the money at risk in a successful crypto currency is likely to increase with time, cf. Sect. 5.1. We agree with Wired Entreprise (2013) to say that crypto currencies should keep allowing miners to make some serious income in order to make attacks more costly.

**Acknowledgments** We thank Xavier Alexandre, George Danezis, Gerald Davis, Pinar Emirdag, Michael Folkson, Clément Francomme, Pawel Krawczyk, Jean-Jacques Quisquater, Guangyan Song, Tim Swanson and John Shawe-Taylor for their extremely helpful suggestions, observations and comments.

## References

Anderson, R.: Open and closed systems are equivalent (that is, in an ideal world). In: Perspectives on Free and Open Source Software, pp. 127–142. MIT Press (2005)

Andreas, M.: Antonopoulos: speaking at L.A. Bitcoin Meetup (2014). https://www.youtube.com/watch?v=bTPQKyAq-DMfeature=youtu.bet=49m20s. Accessed 9 Jan 2014

Antonopoulos, A.: Mastering Bitcoin, Unlocking Digital Cryptocurrencies, Book, 298 pp. O'Reilly Media, ISBN 978-1-4493-7404-4

Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to better: how to make Bitcoin a better currency. In: Financial Cryptography and Data Security, FC'12. Springer (2012)

Bernstein, D.J., Lange, T.: SafeCurves: choosing safe curves for elliptic-curve cryptography, Discriminants sub-page.http://safecurves.cr.yp.to/disc.html. Accessed 4 Sept 2014

Bitcoin Forum, Topic: NSA and ECC, cf. https://bitcointalk.org/index.php?topic=289795.80

Bitcoin "Myths" page, part of official bitcoin wiki. https://en.bitcoin.it/wiki/Myths#Bitcoins_are_worthless_because_they.27re_based_on_unproven_cryptography

Cawrey, D.: What Are Bitcoin Nodes and Why Do We Need Them? 9 May 2014. http://www.coindesk.com/bitcoin-nodes-need/

Cawrey, D.: Are 51 % Attacks a Real Threat to Bitcoin? http://www.coindesk.com/51-attacks-real-threat-bitcoin/

Courtois, N.T.: Computer security foundations and principles. In: Extended Version of Slides from COMPGA01 Computer Security 1 taught at UCL in 2009–2013. http://www.nicolascourtois.com/papers/compsec/CompSec_Intro_01_long.ppt

Courtois, N.T.: On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies, 20 May 2014 (2014). http://arxiv.org/abs/1405.0534. Accessed 10 Dec 2014

Courtois, N.T., Emirdag, P., Nagy, D.A.: Could Bitcoin Transactions Be 100x Faster? In: Post-proceedings of SECRYPT 2014, 28–30 August 2014, Vienna, Austria (2014a). http://www.nicolascourtois.com/bitcoin/POSTER_100x_Secrypt2014_v1.0.pdf

Courtois, N.T., Emirdag, P., Wang, Z.: On Detection of Bitcoin mining redirection attacks. In: ICISSP 2015, 1st International Conference on Information Systems Security and Privacy, 9–11 Feb 2015, Angers, France (2014b)

Courtois, N.T., Grajek, M., Bahack, L.: On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency, 1em plus 0.5em minus 0.4em (2014c). http://arxiv.org/abs/1402.1718. Accessed 28 Jan 2014

Courtois, N.T., Grajek, M., Naik, R.: Optimizing SHA256 in Bitcoin Mining. In: Proceedings of CSS 2014. Springer CCIS series Proceedings (2014d). http://link.springer.com/chapter/10.1007/978-3-662-44893-9_12

Courtois, N.T., Grajek, M., Naik, R.: The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining. 1em plus 0.5em minus 0.4em (2013). http://arxiv.org/abs/1310.7935. Accessed 31 Oct 2013

Decker, C.: Wattenhofer, R.: Bitcoin Transaction Malleability and MtGox. 1em plus 0.5em minus 0.4em (2014) http://arxiv.org/pdf/1403.6676.pdf

Felten, E.: Bitcoin Mining Now Dominated by One Pool. https://freedom-to-tinker.com/blog/felten/bitcoin-mining-now-dominated-by-one-pool/. Accessed 16 June 2014

Financial Times Videos: two excerpts from an interview with Dr Nicolas Courtois of UCL on Bitcoin: http://video.ft.com/3667480923001/Camp-Alphaville-on-cashless-society/Editors-Choice. Accessed 2 July 2014

Galbraith, S.D., Smart, N.P.: Evaluation Report for CRYPTREC: Security Level of Cryptography—ECDLP Mathematical Problem. http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1029_report.pdf

Higgins, S.: Dogecoin to Allow Litecoin Merge Mining in Network Security bid. http://www.coindesk.com/dogecoin-allow-litecoin-merge-mining/. Accessed 4 Aug 2014

Koblitz, N.: The uneasy relationship between mathematics and cryptography. In: Notices of the American Mathematical. Society. http://www.ams.org/notices/200708/tx070800972p.pdf

Kerckhoffs, A.: La cryptographie militaire. Journal des Sciences Militaires **IX**, 5–38, 161–191 (1883). http://www.petitcolas.net/fabien/kerckhoffs/

Kroll, J.A., Davey, I.C., Felten, E.W.: The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In: WEIS 2013, Washington, DC. http://weis2013.econinfosec.org/papers/KrollDaveyFeltenWEIS2013.pdf. Accessed 11–12 June 2013

Lee Kuo Chuen, D. (ed.): Handbook of Digital Currency, 1st edn. Bitcoin, Innovation, Financial Instruments, and Big Data, 612 pp. Academic Press. Accessed 29 April 2015

Matthews, C.: Bit Con? Veteran fraud expert sets his sights on bitcoin. http://fortune.com/2014/10/24/bitcoin-fraud-scam/

Maese, V.A.: Divining the Regulatory Future of Illegitimate Cryptocurrencies. Wall Street Lawyer **18**(5)

Marek (slush) Palatinus: Stratum mining protocol. The official documentation of lightweight bitcoin mining protocol (2014). https://mining.bitcoin.cz/stratum-mining. A compact thrid-party description can also be found at https://www.btcguild.com/new_protocol.php

Mining digital gold, from the print edition: finance and economics. The Economist, 13 April 2013

Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008). http://bitcoin.org/bitcoin.pdf

Nakamoto, S., et al.: Bitcoin QT, the original and the most prominent bitcoin software distribution which implements a full peer-to-peer network node. Originally developed by Satoshi Nakamoto, core developers are Satoshi Nakamoto, Gavin Andresen, Pieter Wuille, Nils Schneider, Jeff Garzik, Wladimir J. van der Laan and Gregory Maxwell. http://bitcoin.org/en/download with source code at https://github.com/bitcoin/bitcoin

Official Bitcoin Wiki: Weaknesses. Summary of all known weaknesses of bitcoin system (2014a). https://en.bitcoin.it/wiki/Weaknesses

Official Bitcoin Wiki: Double Spending. page dedicated to double spending threats and attacks (2014b). https://en.bitcoin.it/wiki/Double-spending

Perry, D.: Posted as GUEST: Bitcoin Attacks in Plain English. http://codinginmysleep.com/bitcoin-attacks-in-plain-english/. Accessed 5 Oct 2012

Rosenfeld, M.: Mining pools reward methods. Presentation at Bitcoin 2013 Conference. http://www.youtube.com/watch?v=5sgdD4mGPfg

Saltzer, J.H., Schroeder, M.D.: "The protection of information in computer systems." In: Proceedings of the IEEE, 63(9), 1278–1308 (1975)

Sams, R.: The Marginal Cost of Cryptocurrency. Blog entry at cryptonomics.org. http://cryptonomics.org/2014/01/15/the-marginal-cost-of-cryptocurrency/

Swanson, T.: What Dogecoin Must Do to Survive. http://www.coindesk.com/what-dogecoin-must-do-survive/. Accessed 25 May 2014

Technical Specification of the Bitcoin Protocol: https://en.bitcoin.it/wiki/Protocol_specification

Todd, P.: Why I Just Sold 50 % of my Bitcoin: GHash.io. http://daytradernews.com/bitcoin-trading/why-i-just-sold-50-of-my-bitcoin-ghash-io.html. Accessed 13 June 2014

Wired Entreprise: http://www.wired.com/wiredenterprise/2013/11/bitcoin-and-deflation/all/. Accessed 25 Nov 2013

Wong, J.I.: Gavin Andresen Rejects Bitcoin Centralisation Concerns at Web Summit, 6 Nov 2014. http://www.coindesk.com/gavin-andresen-rejects-bitcoin-centralisation-concerns-web-summit/

## Author Biography

**Nicolas Courtois** a Senior Lecturer at University College London where he teaches about cryptography and information security. His research focuses on the security analysis of cryptographic systems with particular focus on realistic attack scenarios and systems used by millions of users every day. He is one of the founding members of the group Code Breakers at LunkedIn. He has published more than 100 papers in cryptography and filed more than 8 patents on practical applications of cryptography. Previously he was employed by Gemalto, the world's largest manufacturer of smart cards. He also is an expert on electronic payment and crypto currency.

# Decentralized Banking: Monetary Technocracy in the Digital Age

**Adam Hayes**

**Abstract** Bitcoin has ushered in the age of blockchain-based digital currency systems. Secured by cryptography and computing power, and distributed across a decentralized network of anonymous nodes, these novel systems could potentially disrupt the way that monetary policy is administered—moving away from today's human-fallible central bankers and towards a technocratic, rules-based algorithmic approach. It can be argued that modern central banks have failed to stem macroeconomic crises, and may have, in fact, exacerbated negative outcomes by incentivizing excessive risk-taking and moral hazard via unconventional monetary tools such as quantitative easing and negative interest rates. A central bank typically serves three primary functions: to issue and regulate the supply of money; to serve as clearinghouse for settlement of payments transactions; and to serve as lender of last resort. Could a digital currency system serve as a rational substitute for a central bank? This perspective paper examines that question, and then suggests that indeed it could be plausible. While Bitcoin in its current form will prove to be inadequate to function as monetary authority, I put forward what an operative case could resemble.

**Keywords** Bitcoin · Digital currency · Blockchain · Monetary policy · Central banking

Fluid began to flow through plastic tubing, from one small tank to the next, as the rhythmic hum of hydraulic pumps whirred in the background. The economists who had gathered at the London School of Economics quieted down. Graduate student Bill Phillips, who would later gain notoriety for describing the relationship between inflation and unemployment, stood at the controls of the six-and-a-half foot by five foot analogue machine he had himself built. Phillips had arrived at the LSE from his home in New Zealand by way of Asia, where he was held prisoner in Java by the invading Japanese forces for three-and-a-half years. Now, in 1949, he adjusted the slider for the tax rate, set various dials, and fiddled with the valve that balanced

A. Hayes (✉)
University of Wisconsin-Madison, Madison, USA
e-mail: hayes2@icloud.com; hayes2@me.com

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_7

the budget; moments later The Phillips Machine gurgled and produced an estimate for the unemployment rate and interest rates, supposedly within a ±2 % margin of error (Phillips and Leeson 2000). Later dubbed MONIAC, it was an achievement in technology over fallible human minds in formulating monetary policy and informing central bankers to precisely what action to take upon observing the economy.

Since the Phillips Machine was first turned on, there has been a decline in the use of simple technocratic decision-making for monetary policy. Central banking has become much more nuanced, opaque, and complex as economies have grown larger and more intertwined. The nuance and complexity has also brought with it uncertainty regarding policy decisions which manifests itself in financial markets in the form of volatility: Will the bank raise interest rates? By how much? When will they do it? Why was a specific word used in a statement by the Bank versus the word they have usually used? Every last shade is scrutinized. Central bankers have shifted the conceptual basis of monetary affairs away from rules and standards such as gold or fixed exchange rates, and toward an evolving relationship with the public, rooted in sentiments and expectations (Holmes 2009).

The debate over whether central banks should be governed by rules, or instead by achieving a set of goals whatever way possible is an old and ongoing one. If market participants incorrectly judge how interest rates will change, or if the central bank surprises the market by changing rates contrary to expectations, market fluctuations could increase. This applies to both how often rates are changed and by how much. In fact, empirical research has shown that too much tinkering with interest rates can produce negative economic outcomes (Kydland and Prescott 1977).

Policy think-tanks have also voiced favor for rules-based monetary policy. In February 2015, the Heritage Foundation commented that an explicit monetary policy rule will “greatly improve transparency and predictability,” a belief echoed stridently at the November 2015 monetary policy conference hosted by the Cato Institute.[1] http://www.cato.org/research/banking/rl-monetary-policy.html.

While pneumatic tubes and mechanical dials are relics, sophisticated algorithms spanning silicon and optical fibre have replaced them. In this digital age, can cutting edge technology allow monetary policy decisions to function in technocratic manner, and bring with it the potential for stability that some level of certainty brings to markets?

For simplicity, I take the position that technology today can, indeed, produce such a result—but at the same time I am not advocating that this decision falls on the correct side of the debate over a rules-based policy being most favorable. Rather, I posit that a technology-driven rules-based system can exist within the framework of a decentralized,digital currency system, even if such a framework proves to be inferior to centralized fiat banking in terms of effectiveness, and for any number of reasons.

[1] http://www.heritage.org/research/reports/2015/02/why-congress-should-institute-rules-based-monetary-policy.

It should also be made clear that technology, in and of itself, is not sufficient to promote stability given a set of explicit rules. Algorithmic (high-frequency) trading firms are largely thought to have contributed to recent "flash crashes" (Kirilenko et al. 2015), and have also caused the public to distrust market participants (see Michael Lewis' *Flash Boys*). At the same time proponents of algorithmic trading cite evidence that the technology actually increases market efficiency and liquidity (Boehmer et al. 2014). More empirical work is needed to resolve this emerging discussion.

Regardless, there are bound to be both positives and negatives for any technological intervention, and reducing the potential negatives should be paramount. Of course, many of the algorithms employed in high-frequency trading are kept secret and proprietary, so it is unclear whether failures caused by such systems are the result of the technology itself or manmade flaws in the code. Any algorithmic approach to central banking must be both robust and transparent so that any technical errors can be easily identified and corrected.

## 1 Can Monetary Policy Adhere to Rule-Following?

Modern day central bankers face decisions and take actions which are much more complex than their predecessors (QE, negative interest rates, bailouts), making them potentially more vulnerable to mistakes, miscalculations, and unintended consequences. Their core mandates—namely to maintain price stability and low inflation—however, remain intact. Is it possible to turn some of the core roles of central bankers over to technology?

Certain facets of monetary policy already follow a systematic approach (Clarida et al. 1998). The Taylor Rule, for example, informs central bankers how they should change nominal short-term interest rates in response to changes in inflation and GDP output. One version of the Rule is:

$$i_t = \pi_t + r_t^* + \alpha_\pi(\pi_t - \pi_t^*) + \alpha_y(y_t - y_t^*) \tag{1}$$

In this equation, $i_t$ is the target short-term rate (e.g. the federal funds rate in the U.S.), $\pi_t$ is the rate of inflation as measured by the GDP deflator, $\pi_t$ * is the target rate of inflation, $r_t$* is the assumed equilibrium real interest rate (or neutral rate), $y_t$ is the change in real GDP, and $y_t$* is the change in potential GDP output, as determined by a linear trend. Taylor proposed that the sensitivities of each term ($\alpha$) should be 0.50 (Orphanides and Wiland 2008). Thus, given some macroeconomic data and observations, a certain lever of economic policy will be pulled to the specified setting.

Orphanides and Wieland (2008) find that, indeed, this sort of systematic rule-of-thumb response predominantly explains how the Federal Reserve Open Market Committee's (FOMC) decision-making has been characterized over the past decades. Even if the individual decision makers or committees formulating these responses overtly deny that they are following such a heuristic, the outcomes (incidentally or not) show otherwise.

Taylor and Williams (2010) agree that simple rules-based decision-making is a robust method of implementing monetary policy. They present evidence that historical experience has shown a set of simple rules works well in the real world; macroeconomic performance has, in fact, been better historically when central bank decisions were described by such rules, and the authors assert that such rules are not undermined by financial crises.

An argument can be made that economies are too large and too complex for central banks to deviate from a basic set of rules. How can central banks be expected to successfully manage economic stability via manipulations which can generate unpredictable results with unintended consequences? Prominent Austrian School economist Ludwig Von Mises (1953) argued that central banks actually *cause* economic instability by inducing an unsustainable expansion of bank credit. F.A. Hayek, a student of Mises, understood the need for central banks to regulate monetary policy as sort of a necessary evil lest a completely *laissez-faire* monetary system fall apart (White 1999). Former Federal Reserve Chairman Ben Bernanke (2000) has written extensively on how central bank policy exacerbated the Great Depression of 1929 by incorrectly raising interest rates instead of following the rule which would have caused them to act in the opposite manner.

A central bank may be able to leave the "every day" monetary policy to an automated set of rules governed by a digital currency regime and intervene only if and when a crisis arises. In the run-up to the latest episode of the Greek banking crisis, ex-finance minister Yanis Varoufakis surmised that his country could adopt Bitcoin (or some similar system) to function as a bridge currency to a new *drachma* if Greece did indeed leave the common euro currency. Quite correctly, Varoufakis has pointed out many shortcomings of Bitcoin itself as a practical long-run substitute for a nation's monetary system—such as its potential to be deflationary and its inability to react to external forces (Varoufakis 2014). He has, however, gone on the record stating, "[a]lmost paradoxically, the technology of Bitcoin, if suitably adapted, can be employed profitably in the Eurozone as a weapon against deflation and a means of providing much needed leeway to fiscally stressed Eurozone member-states." I believe that this technology can be so suitable adapted.

The Phillips Machine is now relegated to museums, but cutting edge information and communication technology (ICT) ought to allow an adherence to technocracy, free from human fallibility and corruptibility. Such a technology can be built upon a distributed network, such that no one individual or organization has sole control over the system, and yet it can still remain remarkably stable and robust without a single point of failure.Digital currency systems today are clear examples of a system that could function as monetary authority. These are known generically as a'cryptocurrencies', owing the name to the process of encryption that enables it,[2] the most well-established and widely used of which being Bitcoin.

[2] Cryptocurrencies today are based on a blockchain data structure, which is essentially a distributed ledger system. The technical details of Bitcoin, cryptocurrencies and Blockchains are beyond the scope of this chapter.

While it has been made apparent that Bitcoin in its current form is likely a poor candidate to operate as an important global reserve currency, a system that builds off of its core technology—the *blockchain*—may in fact be a viable use case.

Despite its shortcomings, Bitcoin has proven itself useful with respect to aspects of the concept of money. It has established that a conceptually digital money-form can be an acceptable store of value and a means of payment, both crucial features of any currency (Ingham 1996; Bamert et al. 2013).

A currency needs to have societal trust in its security and fidelity. Blockchain-based cryptocurrencies have exhibited recognition of so-called *trustless trust*. As a distributed network, Bitcoin transactions have never been compromised or hacked and a bitcoin has never been forged or counterfeited.[3] A well-understood consensus mechanism amongst a network of anonymous and far-flung nodes has shown that a central authority or overseer is not a necessary requirement.

For a digital currency to operate as monetary authority, it must at the very least satisfy the requirements of being *money*. Aristotle, in ancient times, proposed four characteristics needed for something to be a “good form” of money (Smithin 2002):

1. *It must be durable*. Money must stand the test of time and the elements. It must not fade, corrode, or change through time.
2. *It must be portable*. Money must hold a high amount of ‘worth’ relative to its weight and size.
3. *It must be divisible.* Money should be relatively easy to separate and re-combine without affecting its fundamental characteristics, i.e. it should be ‘fungible’.
4. *It must have intrinsic value.* This value of money should be independent of any other object and contained in the money itself.

Does a digital currency fulfill these criteria? Taking Bitcoin as the general example, it is durable—its security is iron-clad and its existence is permanent in the blockchain data structure without any degradation. It is portable—it can be accessed from any internet connected computer or mobile device. It is divisible—one bitcoin can be broken down to eight decimal places (the smallest such unit known as a *satoshi*), and it is fungible. It *has* intrinsic value.

This fourth point warrants some elaboration. Some have asserted that Bitcoin has no intrinsic value at all; that it has any market price is solely due to fleeting social popularity and the hope of speculators (Yermack 2013; Hanley 2013; Woo et al. 2013; Polasik et al. 2014).

Hayes (2015a), however, has demonstrated that Bitcoin does have some sort of intrinsic value, directly related to its cost of production. In other words, it behaves much like a commodity produced in a competitive market: electricity goes in and bitcoin comes out. If the average cost of production decreases, producers will offer their product in the market at lower and lower prices, in competition with each other, until marginal cost approaches marginal product (Hayes 2015b). Therefore, it

[3] Certain hacking events or theft have compromised services that use Bitcoin, such as Mt. Gox, but never Bitcoin itself.

is more accurate to consider bitcoin as more akin to a commodity form of money such as gold or silver than a fiat money. In fact, implementing Bitcoin as a national monetary system would be like a hard return to the gold standard in many ways.

There are many alternative criteria with which to evaluate the ‘moneyness’ of something, but those arguments are beyond the scope of this essay and are unlikely to change the outcome of this analysis. To Aristotle, at least, a digital currency could reasonably satisfy all the requirements to be a “good” money.

## 2 What a Viable Digital Currency System Might Look like

For a digital, blockchain-based currency system to work as an economy’s monetary authority, some of the limitations that encumber Bitcoin must be removed. For example, Bitcoin has a predetermined maximum quantity of 21 million units. This limitation would need to be removed in favor of a potentially unlimited supply; such an upper bound will likely create an artificial constraint that ultimately serves to make it an increasingly deflationary currency—each ‘coin’ will become progressively more valuable as demand for money increases and the supply cannot accommodate.

Theoretically, a limitation on ultimate supply seems to have no influence on a cryptocurrency’s relative value (Hayes 2015a, b). Cryptocurrencies do currently exist with no cap on the money supply, for example Peercoin, which has exhibited a fair amount of price stability despite its unlimited potential.

A second hurdle to overcome is that it would be technically difficult for a cryptocurrency system to directly set a target interest rate per se. Interest rate setting has become a hallmark of monetary policy, but there are other ways to influence the “price of money” with similar effect: a digital currency could still achieve monetary policy goals by manipulating the rate of change to new money formation to similar effect. There is a theoretical basis that changing the rate of money supply formation is a logical equivalent to changing the interest rate (Tobin 1969). Interest rates and the quantity of money are intrinsically linked, in that increasing interest rates makes money more “expensive”; decreasing the supply of new money would have similar effect.

In a fractional reserve banking system like we have today in much of the developed world, the central bank regulates so-called “high powered” money, also known as the *monetary base,*or M0. This base is then amplified through the financial system via lending and credit mechanisms. A digital currency system that cannot amplify itself via fractional reserve banking can still work, however. Full-reserve banking (Fisher 1935) is a proposed alternative where banks are required to keep the full amount of each depositor’s funds in cash—or in our case digital currency. This 100 % reserve system was offered as a theoretical solution for the causes of the Great Depression, although no country has yet implemented this policy. Since World War II, there has been an increasing focus on fractional banking, however a number of economists have advocated for it in the past few decades across various schools of thoughts ranging from the Monetarists to the Austrians (Kotlikoff 2009). Proponents of full-reserve banking argue that not only could such a monetary system function, but that it would also eliminate the risk of bank-runs, bailouts of the financial sector, and increase macroeconomic stability (Rothbard 1974). In the wake of the 2008 financial crisis the idea was again revived, finding favor with Martin Wolf, chief economics commentator of the *Financial Times*, who has called for stripping banks of their right to create credit money.[4] His argument that allowing banks to create money by lending out deposited funds is what is responsible for creating destabilizing credit bubbles and busts has also been echoed by a number of well-respected economists (Cochrane 2014; Krugman 2014; Polleit 2010). A digital currency-based technocratic monetary authority would likely have to operate in a 100 % reserve environment.

Bitcoin has a fixed rate of unit formation (one block every ten minutes), and a rule for constant predetermined growth of the money supply does happen to have some theoretical support. The so-called Friedman Rule (Friedman 1948) proposes that the central bank should establish a fixed constant rate of growth for the money stock, and maintain that growth rate no matter what emerged from the state of the economy. Such a rule has some advantages: it is easy for the public to understand; the rate of inflation cannot take off toward plus (or minus) infinity; and, market-determined interest rates are free to fluctuate in response to changing economic conditions (Taylor 1999). A fixed rule, however, critically ignores feedback from the economy and does not have the ability to adjust and smooth out the effects of macroeconomic changes.

McCallum (1988) and Meltzer (1969) have augmented the constant growth rate formula with quantity-based rules that yield a dynamically changing growth rate of the monetary base contingent on widely available economic indicators. Notably, the McCallum Rule has been proposed as an alternative to the Taylor Rule, and it has been empirically shown to perform better during crises (Benchimol and Fourçans 2012). Such a rule would be much easier to implement with a digital currency system as regulator of monetary supply, since there would be no target interest rate in the traditional sense. The McCallum rule determines the optimal change in the monetary base given changes in GDP, inflation and the velocity of money. It is also intended to reflect long-lasting, permanent changes in the demand for the monetary base that occur because of technological developments or regulatory changes, and not intended to reflect cyclical conditions (McCallum 2000).

If we take a monetary policy with an explicit inflation target (say 2.5 % annually), one could easily construct a rule for a digital currency to follow that will change the rate of monetary formation from one time period to the next. This can be achieved by adjusting how many monetary units are produced when each block of digital currency is created, or by changing the interval in which blocks of currency are produced. For example, if the economy is growing too rapidly, the rate of money formation should be reduced over the next time period. This would have a

[4] http://www.ft.com/intl/cms/s/0/7f000b18-ca44-11e3-bb92-00144feabdc0.html.

similar effect to raising interest rates in that it would make money scarcer on the margin. In practice, to promote stricter monetary policy the number of currency units in each block would be reduced over some interval (for example from 25 to 10 'coins' per block), and/or the time between block formation can be made longer (for example from 10 to 15 min), while to promote expansionary monetary policy the reverse would take place.

Such a rule-following digital currency could operate completely independent from the central bank. It would only need to incorporate publicly available macroeconomic data into its function as feedback in order to adjust the rate of new money formation in the succeeding periods. Not only would such a currency be independent, but it could be made completely decentralized, with no single authority or regulator in place. Like Bitcoin and other cryptocurrencies today, it could even exist across a decentralized network, democratizing the money-creation process.

A completely decentralized monetary system may seem wildly idealistic, but a digital currency can also exist across a distributed "permissioned" blockchain, where each node in the network is a known and trusted entity. Banks and financial institutions could be obvious candidates to operate these nodes, and yet still operate with transparency with a well-understood consensus mechanism from the point of view of the population. Within a nation's borders, a permissioned blockchain is probably most appropriate as it can keep out foreign actors, can greatly reduce the need for expensive and resource consuming "mining" operations, and greatly increase the speed and capacity of transactions.

Bitcoin has come under pressure lately with respect to its limitations on the block size, capping the number of transactions it can process and slowing down confirmations. An open blockchain where all nodes are (for all intents and purposes) anonymous such as Bitcoin requires an energy-intensive consensus mechanism (mining, or proof-of-work) in order to prevent bad actors from undermining the system. Under a permissioned blockchain all nodes are vetted and known, making such an expensive and potentially limiting mechanism unnecessary. The system will need to have the capacity to handle the extremely large amount of transactions that are likely to occur each and every second across a nation's economy.

Given that a digital currency system like the one described relies on publicly available, anybody can deduce its next move(s). Market participants, rationally motivated by profit maximization, will be incentivized to act on any perceived mispricings observed in the market which differ from how the digital currency mechanism is expected to behave as it reigns in or bolsters the rate of money formation. Under a fairly reasonable no-arbitrage assumption, this will serve to increase market efficiency as it will greatly reduce the asymmetry of information that people can trade on.

To sum up the above analysis, a viable digital currency system could function as "central bank" if it: (1) has a potentially unlimited money supply, (2) follows rules based on dynamically changing the rate of new money formation; (3) has a mechanism to obtain feedback from the economy; (4) operates in a 100 % reserve banking environment; and (5) operates as a permissioned blockchain with appropriate speed and capacity for all transactions in an economy.

## 3 Conclusion

Prof. Bennet T. McCallum has recently written a piece on Bitcoin which appeared in the journal for the Cato Institute (McCallum 2015). In it, he acknowledges that Bitcoin in its present form could not satisfy the role of the monetary authority. For example, he reiterates that with a limit of 21 million bitcoins and an economy that grows each year, deflation will become a rampant problem. He does, however, generally propose the viability some alternative digital currency system, such as described in this section, but (perhaps ironically) he fails to incorporate his own namesake Rule into his analysis.

With advances in blockchain technology now removed from the constraints of Bitcoin, it is possible to encode *smart contracts*, algorithms that will act as a trusted enforcer of agreements. With deployable smart contracts, a blockchain-based monetary authority, which follows a McCallum-like rule for new money creation, can also engage freely in emergency measures such as open market operations to drastically increase or decrease the money supply when warranted. Such a situation may be runaway inflation or deflation, a collapse in employment, or a period of recession. In these cases, the digital currency itself will act as a *decentralized autonomous organization* (DOA), making “decisions” on its own and interacting with real financial markets directly. Such a DOA could feasibly buy up existing digital currency—and even destroy some of that currency by sending it to unusable wallet address—in order to quickly reduce the money supply outstanding. The DOA could engage in purchases of foreign currencies in FOREX markets, as well as stabilize prices by purchasing bonds and equity in exchange for its stock of digital currency. Coupled with improvements in artificial intelligence and machine learning, an AI-enabled DOA acting as monetary authority can truly be removed from government, central authorities, or the influence from policymakers and corporate lobbies.

Bitcoin has proven itself to be a fairly robust use-case of blockchain technology in creating a global, decentralized digital currency and payments system. Bitcoin, however, is flawed in many ways if it is to be adopted as a true economic currency. Many of these issues can be rectified to make a more useful and dynamic digitalcurrency, able to meet changes in supply and demand for money. If programmed as a decentralized autonomous organization, a blockchain-based monetary authority can even engage in its own emergency measures with effects similar to quantitative easing in order to stimulate a flagging economy or else halt rampant inflation. Doing so will enable a truly independent monetary authority to operate and perhaps even improve the prospects for economic stability and efficiency.

## References

Bamert, T., et al.: Have a snack, pay with Bitcoins. In: 2013 IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P). IEEE (2013)

Benchimol, J., Fourçans, A.: Money and risk in a DSGE framework: a Bayesian application to the Eurozone. J. Macroecon. **34**(1), 95–111 (2012)

Bernanke, B.: Essays on the Great Depression. Princeton University Press, Princeton (2000)

Boehmer, E., Fong, K.Y.L., Wu, J.J.: International evidence on algorithmic trading. AFA 2013 San Diego Meetings Paper (2014)

Buiter, W.H., Panigirtzoglou, N.: Overcoming the zero bound on nominal interest rates with negative interest on currency: gesell's solution. Econ. J. **113**(490), 723–746 (2003)

Carlson, J., et al.: Credit easing: a policy for a time of financial crisis. Economic Trends 11 (2009)

Clarida, R., Gali, J., Gertler, M.: Monetary policy rules and macroeconomic stability: evidence and some theory. No. w6442. National Bureau of Economic Research (1998)

Cochrane, J.H.: Toward a run-free financial system. SSRN 2425883 (2014)

Fisher, I.: 100 % money (1935)

Friedman, M.: A monetary and fiscal framework for economic stability. Am. Econ. Rev. 245–264 (1948)

Hanley, B.P.: The false premises and promises of Bitcoin. arXiv:1312.2048 (2013)

Hayes, A.: What factors give cryptocurrencies their value: an empirical analysis. SSRN (2015)

Hayes, A.: A Cost of Production Model for Bitcoin. SSRN (2015)

Holmes, D.R.: Economy of words. Cult. Anthropol. **24**(3), 381–419 (2009)

Ingham, G.: Money is a social relation. Rev. Soc. Econ. **54**(4), 507–529 (1996)

Jones, S.: Central Banks Load Up on Equities. Bloomberg, 25 April 2013. http://www.bloomberg.com/news/articles/2013-04-24/central-banks-load-up-on-equities-as-low-rates-kill-bond-yields. Accessed 4 Aug 2015

Joyce, M., et al.: Quantitative easing and unconventional monetary policy–an introduction. Econ. J. **122.564**, F271–F288 (2012)

Kirilenko, A.A., et al.: The flash crash: the impact of high frequency trading on an electronic market. SSRN 1686004 (2015)

Kotlikoff, L.J., Leamer, E.: A banking system we can trust (PDF). Forbes.com (2009, April 23)

Krugman, P.: Is a banking ban the answer? New York Times (2014, April 26)

Kydland, F.E., Prescott, E.C.: Rules rather than discretion: The inconsistency of optimal plans. J. Polit. Econ. pp. 473–491 (1977)

McCallum, B.T.: Robustness properties of a rule for monetary policy. In: Carnegie-Rochester Conference Series on Public Policy, vol. 29. North-Holland (1988)

McCallum, B.T.: Alternative monetary policy rules: a comparison with historical settings for the United States, the United Kingdom, and Japan. No. w7725. National Bureau of Economic Research (2000)

McCallum, B.T.: The bitcoin revolution. Cato J. **35.2** (2015)

Meltzer, A.H.: Appropriate indicators of monetary policy (1969)

Mishkin, F.S.: Is monetary policy effective during financial crises?. No. w14678. National Bureau of Economic Research (2009)

Orphanides, A., Volker, W.: Economic Projections and Rules-of-Thumb for Monetary Policy, vol. 2008. SSRN:http://ssrn.com/abstract=1141653

Phillips, A., Housego, W., Leeson, R.: AWH Phillips: Collected Works in Contemporary Perspective. Cambridge University Press (2000)

Polasik, M., et al.: Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. SSRN:2516754 (2014)

Polleit, T.: The Faults of Fractional-Reserve Banking. Mises Daily (2010). https://mises.org/library/faults-fractional-reserve-banking

Rothbard, M.N.: The Case for a 100 percent Gold Dollar. Libertarian Review Press (1974)

Smaghi, L.B.: Conventional and unconventional monetary policy. Speech at the Center for Monetary and Banking Studies, Geneva 28 (2009)

Smithin, J. (ed.): What is Money? Routledge (2002)

Taylor, J.B., Williams, J.C.: Simple and robust rules for monetary policy. No. w15908. National Bureau of Economic Research (2010)

Taylor, J.B.: A Historical Analysis of Monetary Policy Rules. Monetary Policy Rules, pp. 319–348. University of Chicago Press (1999)

Tobin, J.: A general equilibrium approach to monetary theory. J. Money, Credit Banking **1**(1), 15–29 (1969)

Tobin, J.: Keynesian models of recession and depression. Am. Econ. Rev., 195–202 (1975)

Varoufakis, Y.: BITCOIN: A flawed currency blueprint with a potentially useful application for the Eurozone. http://yanisvaroufakis.eu/2014/02/15/bitcoin-a-flawed-currency-blueprint-with-a-potentially-useful-application-for-the-eurozone/, Accessed 5 Aug 2015

Von Mises, L.: The Theory of Money and Credit. Ludwig von Mises Institute, Auburn (1953)

White, L.H.: Why Didn't Hayek favor Laissez Faire in banking? Hist. Polit. Econ. 31.4; WIN (1999): 753–769

Woo, D., et al.: Bitcoin: a first assessment. FX and Rates (2013)

Yermack, D.: Is Bitcoin a Real Currency? An Economic Appraisal. No. w19747. National Bureau of Economic Research (2013)

## Author Biography

**Adam Hayes, CFA** is co-founder and CEO of ChainLink, a blockchain-based startup conferring tamper-proof certificates of title and authenticity to property and luxury items. He has written a number of research papers on Bitcoin, cryptocurrency valuation, and blockchain technology. Adam has over 15 years Wall Street experience in the derivatives markets and in private wealth management. He received his bachelor's degree from Cornell University and holds an MA in economics from the New School for Social Research in New York, NY. Adam is currently a PhD candidate in economic sociology at the University of Wisconsin-Madison and is an instructor for the University of Nicosia's MSc program in digital currencies.

# Trustless Computing—The What Not the How

Gavin Wood and Jutta Steiner

**Abstract** A recent development has provided us with a new computing paradigm: the blockchain. First described by Satoshi in 2008, it is the first example of a computer that has the functionality to remember and enforce past statements by participants, in a non-localized, resilient and auditable manner. Although the Internet has allowed us to create a global infrastructure for cheap and flexible communication, no strong statements can follow from its weak economic signals without resorting to a recognised authority. A global information system that has the properties of the Internet but also the functionality to enforce statements without a trusted intermediary is required: such a system is called trustless. The chapter follows the examples of the usage of blockchain technology as a system that provides guarantees over the rules of its operations in consumer goods, online dating and international trade, with no need of third party intervention for the creation of trust, unleashing new potential business opportunities.

**Keywords** Trustless Computing · economic signals · blockchain

## 1 Introduction

We live in a world of bits and bytes. Zipping through the air, it pervades human lives the world over. The technological backdrop to this situation is twofold: our incredible world-wide ubiquitous communications infrastructure known as the Internet and all the metal-and-plastic boxes at the ends of this network known variously as computers, laptops, mobile phones and tablets. Looking at the awesome alterations to society that have taken place in the last few decades with

G. Wood (✉) · J. Steiner
Co-Founder and CTO, ETH CORE LIMITED, London, UK
e-mail: fao.gavin@ethcore.io

J. Steiner
Co-Founder and COO ETH CORE LIMITED, Berlin, Germany
e-mail: jutta@ethcore.io

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_8

information-communications-technology (ICT), one would be forgiven for questioning if this avenue of technological endeavour is not exhausted; perhaps human research should look elsewhere for society's next big thing, as it seems sometimes that the development of many new technologies such as wearables, devices, robotics, nanotechnology, AI, big data and space exploration has become a competition in which all of these developments are contenders, looking for a prominent place in today's market.

Despite this extraordinary rivalry, ICT and the internet is far from done changing the fabric of society. Though we have a single globally connected network and, separately, countless computers interpreting and managing our various interactions with the world, we have not yet closed the space fully: we do not yet have a single globally-connected computer. This computer, which in its singularity cannot fail, be stopped or censored by any authority and at the same time be auditable is what can radically change social dynamics.

I will first share some thoughts about some basics of human interaction, namely economic signals, and how human activity is shaped around them and how society benefits from this. I will then explain how recent information communications technology might help bring economic signals into the digital realm and how attempts or potential solutions thus far are lacking. *I will explain the blockchain under this context* and demonstrate that it, alone, can fundamentally answer this problem. Finally, I'll discuss a few of the interesting ways this technology can alter society—from the interpersonal to the international.

## 2 Strong Economic Signals

Economists discern strong and weak signals. A signal is a piece of communication or information, given by an actor in an economic system. The wave of a hand, the giving of a gift, the speaking or writing of a statement; all fall under this category. Indeed the Internet has given us a plethora of ways to make such signals, and we can do so nearly effortlessly.

The difference between a strong and a weak signal is that a strong signal is implicitly tied to a material cost or ramification for the signaller. A simple example might be the engagement ring. In times gone by, at least, the veracity of a potential spouse's desire to enter into a binding exclusive agreement would be judged by the amount of expense he committed to the counter-party prior to finalisation of the contract (e.g. the ceremony). By gifting a more expensive ring, he demonstrates a greater commitment of his own resources and, in turn, the bride-to-be asserts he is more likely to abide by his engagement for, thinks she, were he to have repeated this feat with many such jilted fiancées, he would surely be penniless.

Strong signals facilitate trust among strangers. They allow us to operate in the real world without relying purely on hope and faith. They need not involve real money or precious items: we recognise with ease many common cues which betray medium-strength signals. With very few exceptions, human-dealings involve a greater or lesser extent of reliance on signals. e.g. business deals, especially between smaller firms with a single decision-maker will often proceed more smoothly when one or both make clear signals. This might include negotiating in person (the strength of the signal being underlined through the effort and opportunity cost of travel) or, if they speak different languages, learning and initiating the negotiation in the other's language (the strength coming from the effort and time to learn the language, not to mention placing oneself on unsafe ground through speaking in an unfamiliar language).

The Internet is a vast, expansive and resilient global infrastructure that affords us largely unfettered (oppressive states like China and Saudi Arabia notwithstanding), cheap and flexible communication. However, precisely because this communication is cheap and flexible means that in terms of signals, no strength can generally be derived without resorting to a broadly recognised authority, or trusted intermediary.

Through the use of such an authority, like recognized financial institutions, corporations or governmental agencies, ramifications can be enforced on participants. A badly behaved participant may be punished: participants can thus be held to their prior communications with some degree of certainty and as such, strength can be added to some of signals they do give. User reviews on eBay provide a comparatively medium-strength signal on the veracity of a seller since reviews are registered and recorded only by eBay itself and (we trust) only under certain circumstances (such as the completion of a trade). While trusted authorities provide a clear solution, such a reliance is rigid, attack-prone and, being a natural monopoly, potentially costly.

Ideally, we would like a global information system that has the properties of the Internet (fast, free and ubiquitous) but also has functionality to remember and enforce past statements by participants so that talk in the digital realm no longer will be cheap. By architecting a system that can enforce statements autonomously provide a means to an end of cheap talk and turn statements into strong economic signals. This way, as Internet users, we would be able to identify, understand and quantify the signals given by strangers. If a remote, perhaps anonymous, Internet user stated they would provide some payment immediately on receipt of a particular product, it would be very useful if there were a way of codifying this in the Internet itself without the need to identify and agree upon a third party to enforce our simple deal. In the same way as the Internet revolutionised human endeavour all over the world through rewriting the rules on human communication, such a technology would cause a similar revolution through a revision of the meaning of trust itself.

## 3 A Global Computer

If we review our ideal a little more deeply "functionality to remember and enforce past statements by participants", there are three concepts that we can explore: "remember [past statements]", "enforce [those statements]", and "by participants".

The easiest to understand and reason about is the latter. It relates to the notion of identification of a statement with a specific individual. Identification really just means the ability for someone to prove that they are the same individual as that associated with a previous statement or event. There are numerous solutions to this problem in the real world depending on the gravity of the situation. From keys and codes which are often used for entry to an inline service or building, to passports and birth certificates, often needed for entry into a country or into marriage. For mid-level purposes, however, the classic pen-and-paper signature is the de facto means of identifying oneself and recording ones approval.

Pen-and-paper signatures work (theoretically) on the basis of it being difficult to replicate another person's signature, under the assumption that one has access only to other signed documents. In the digital word of fax, scanners and Photoshop, this idea is of course ludicrous.

While the pen-and-paper signature is far from perfect, there does exist a true analogue in the digital realm, a technology that people can trust but no replicate, allowing to sign documents and make others sure it was us who did it. This technology is called public/private key cryptography (or PKI). "Us" is in fact anyone with access to a particular secret number (it's a big, random one so nobody can guess it and it's typically password protected so it's hard to steal). The term "documents", is actually any piece of digital information, and includes everything from the simplest text message to the most complex PDF. Finally, the term "sign" in this case simply means appending a small piece of information to the "document".

Using such cryptography we can begin to understand how we might be able to identify statements "by participants" made on or over the Internet in a strong fashion. Indeed this technology is used already to help us recognise fake websites: that small green lock to the left of the location in the browser is the indication that the website has a "trusted" digital signature. The other two aspects of our ideal are a little more difficult to address. While technology like PKI can solve the participants' identification issue, the 'remember' and 'enforce' elements require an unorthodox approach.

Remember statements and automatically enforcing them essentially means having a language in which it is possible to have a machine record statements and execute on them. Luckily, these machines exist: they're called state-transition machines or, more commonly, computers. The languages also exist: they're called computer languages, the most basic of which are called machine code. Under this language, we need no longer talk about statements as much as transactions, their machine equivalent, representing a valid arc between two states. Transactions are simply code executions valid for both parties.

These languages have their drawbacks, of course—they're difficult for humans to write and even more difficult for us to understand. They are abstract and deal only in the simplest mathematical and logical notions. However, they have two advantages that make them unavoidable for us: they are generally Turing complete, meaning that any conceivable logical statement can be expressed and executed—given enough time and storage space—and they are unambiguous, meaning there is only a single meaning for any given statement.

While codes are a possible solution of the 'remember' and 'enforce' elements, our great remaining problem is that we are unable to use a traditional computer to enforce these languages: The issue is twofold. On the one hand, the unquestionable attribution over who is currently using a traditional computer an thus in charge of the execution is typically lacking. We have to trust that anyone with physical access (or anyone with enough means to gain physical access) would act in a disinterested fashion. But any traditional system maintained by humans is subject to alteration of the enforcement. On the other hand and far more important: a single normal computer is not, like the Internet, ubiquitous and the costs of upkeep, unlike the Internet, are not shared across the user base. Any organisation that were able to run (and keep online) this "trustworthy" Internet computer would need to do so for free, forever, all the time, under all circumstances.

So, in order to solve the three elements in our idea we need a piece of technology with all the aspects of a single computer, but additionally with aspects similar to the internet: ubiquitous, collectively maintained by the users without central authority, and, additionally, with all interactions to be signed.

## 4 Consensus: An Old Compute Paradigm Made New

A recent development in computer science has provided us with a new exciting computing paradigm: the blockchain. First described by Satoshi in 2008 and used to create the digital currency Bitcoin, it is the first example of a computer that exists and operates without any single authority. The first blockchains were exceptionally limited in functionality, being little more than arithmetic systems (calculators). Continued experimentation and development of the technology with such systems as Omni, Counterparty and Ethereum[1] have demonstrated that the potential scope of this technology is far greater than the initial use case of a digital currency, and for the case of Ethereum in particular, can be extended to include arbitrary business logic.

The blockchain is operated through a large plurality of self-chosen independent parties, sometimes called miners (those who execute transactions by grabbing slices of dataset and hashing them together, eventually creating a block) who are empowered to collaborate in order to "operate" this computer. Use of the blockchain computer by others is paid for through a tribute to these operators or miners. Because the barrier to entry for becoming an operator is near zero, they may come from competing interests, different industries, jurisdictions and political alignments. They may even be anonymous. This broad foundation helps guarantee that no single interest is able to take control of the computer and become a de facto authority behind it.

Advanced mathematics is embedded within this computer to provide guarantees over the rules of its operation and allow operators through the application of certain rules to form a consensus, even without any sort of direct coordination or communication. These guarantees are sufficient to allow users to be comfortable that

[1] Omni and Counterparty can be defined as algorithmic extensions of Bitcoin, while Ethereum represents an open-source fully decentralized platform for smart contracts. See http://www.omnilayer.org/, http://counterparty.io/ and https://www.ethereum.org/ for more information.

their business logic (i.e. software) will run securely and as intended. Such a computer system is called trustless, because the users of it need not trust in the behaviour of any particular operator (or minority thereof), but only in the rational behaviour of the majority leading to the computer's emergence.

Does the invention of the blockchain computer match our specifications and needs for an ubiquitous trustless computer? Indeed, there are a number of key differences between the blockchain type of a computer and a traditional computer; first and foremost, it is decentralised, or physically non-localised. Secondly, as it will be discussed later, it is fundamentally secure in a way matched by no traditional computer. Finally, it is completely auditable: much like we can comprehend how our bank account's balance ends at a particular amount through reviewing all transactions on our account, we can apply the same process to the blockchain computer with ease and understand how it arrived at a particular configuration of information with complete clarity.

## *4.1 Non-localisation: A Truly Global Computer Running by Consensus*

Traditional hardware computers (e.g. desktop PC's, mobile phones, etc.) are limited by the physical world. My PC or laptop cannot run in two or more places at once however much I may wish. Even though it seems that modern (web) applications run on several devices, the truth is that to keep consistency, the application's core program is executed (or at least coordinated) on a single, centralized server, with the client device effectively being merely a powerful display.

In contrast, the computing power at the centre of blockchains need not be localized to one single machine: for any blockchain there is no single machine that similarly governs the business logic or the data on which it operates. Instead of appealing to a single authority at the core to know about the current state of the system, users unambiguously discover the state of the machine by applying a number of rules and publishing data openly. This works because the sharing of such data is incentivised by a mechanism that forms part of the rule set.

## *4.2 A Machine of Unparalleled Digital Security and Resilience*

Traditional client/server systems rely on crucial security assumptions to operate safely. With all traditional systems, security ultimately reduces to a question of physical presence; the most natural metric for permission. Physical presence is how normal hardware machines interact with and expose themselves to the outside world, and thus the users to execute operations, be it via a keyboard, mouse or other input/output (I/O) devices and conduits, such as an Ethernet cable. Having physical control over the I/O allows in addition, possibly clandestine, further operations to be executed, incoming information to be hidden or altered, the state of the system to be modified and for such actions to happen without trace.

Recent years have seen a surge in attacks undermining the protection mechanisms erected around centralized systems. Leveraging the most elevated access rights, an attack that targets IT and operational support could eventually lead to the system being fully compromised. The notion that some level of physical security is sufficient for total business information security is flawed entirely: the physical world lends itself well to providing us a false sense of security over the information and processing that happens in the digital world.

With the blockchain, security is different: it does not matter who or where you are, the blockchain computer runs totally unaware of anything until and unless strong cryptographic authentication by a user is provided. More precisely, any and all input to the machine at all times for it to be accepted is necessarily and always authenticated. This authentication is provided in terms of an unforgeable digital signature: a cryptographic widget which allows someone to prove their identity without giving away the ability to prove it in the future (see call-out box for more details). Output, or the ability to inspect the results from the machine, on the other hand is completely unprotected and open for everybody to inspect. The security of the blockchain computer differs from the physical security systems of conventional computers in that it matters not what your job is or what your physical access capabilities happen to be; you strictly cannot interact with the machine unless you provide the digital "key" required for the interaction of which you are the owner (e.g. unless you prove the ownership of an account through the respective digital signature, there is no way for anybody else to change the account's balance). In reality, this means that classic "elevated" privilege levels tend to be curbed or removed entirely. The security risk of the weakest link stemming from operators and IT administrators is drastically reduced.

## *4.3 A Perfectly Auditable System*

Computers are deterministic. This means that any decisions they make, or information the user can extract from them, is based purely on the historical input of the machine, e.g. from information received over its network cable or through the keyboard and mouse. Taken as a whole, these inputs are records of the various interactions that have led the machine into its present state (e.g. automated bank transfers in the case of a payroll system or ordering additional components in the case of a stock control system).

Determinism means that the actions of a machine can be strictly verified and audited as correct, with one proviso: that all information concerning all inputs is provided. Typically in traditional systems this is expensive, impractical or impossible. The inputs to a business system often include heterogeneous types of data (besides keyboard, mouse and network I/O, there is input coming from other applications, all of which could be time-sensitive) and the auditing itself, which would essentially be an attempt to "play back" such inputs, would be technically challenging. Furthermore, in a business context, auditing may need strong knowledge and assurance of operator identity, which can often be compromised or flawed.

A blockchain computer is different: by design it is perfectly auditable. Each individual operation of interaction, e.g. the provision of a new employee in the payroll system or the recording of outgoing stock in the stock control system, is perfectly recorded and archived. Auditing is as simple as joining the blockchain network, since the only way to interact usefully with it is to "replay" all of the operations of the past oneself in order to build a correct model of the present. Combined with absolute guarantees of authenticity for each and every interaction with it, strong and agile data systems can be facilitated which are at its core resilient to coercion and human factors.

## 5 The Perennial Problem

Digitisation of banking, which is to say, the transition of ledgers from pen and paper to electronic and magnetic, optimised the flow of credit through the economy, brought banking to the masses and consolidated authority over vast parts of the economy to a few extremely large banking corporations. But operations suffer from the centralisation and lack of transparency. Certain services, such as fast transfer of value, international transfers, digital and effortless point-of-sale payments, have hitherto only been available through the extensive infrastructure built by banking industry. Operations are extremely costly. Santander estimates potential cost saving up to $20bn annually that blockchains could deliver.[2] The fundamental complexity of this infrastructure, at its core, is little more than arithmetic: it must avoid the unauthorised creation or reduction of value.

A vastly simplified blockchain software infrastructure and smooth inter-operation would allow services to be "mashed-up" (combined) to unleash exciting potential business opportunities previously possible only through cumbersome cross-industry partnerships, without risk of leaked or stolen information being used to boost corporation's profits. Users would be safe in the knowledge that they share only as much data as is strictly required for the application to function; never giving away sensitive payment information and never having to trust one faceless organisation over another. While this is an inconvenient truth now, it will become ever more important as the data that our device manufacturers own begins to include information of a decidedly private and personal nature never before collected.

[2] For more information see: Wyman, Oliver, Anthemis Group and Santander Innoventures (2015), "The Fintech 2.0 Paper: rebting financial services", available online: http://www.finextra.com/finextra-downloads/newsdocs/The%20Fintech%202%200%20Paper.PDF.

# 6 Further Examples

## *6.1 Consumer Goods*

Most of the times, the journeys of our material products remain hidden in sprawling, complex supply chains or are veiled by marketing that can mask sad truths rendering informed purchases impossible.

At the same time, more and more consumers are demanding genuine transparency on where and how their products are made. Recent regulation, for example in the EU and UK, requires more supply chain information to be published and also ensures that perpetrators can be adequately punished. But even with increased demand and regulation, ensuring the authenticity and chain of custody of products has proven difficult.

We have long tried to entrust third parties to track and oversee supply chains employing centralised databases, without success. If that party is the brand itself, or most powerful actor in the supply chain, then motivations are not aligned. This could lead to selective disclosure since the party monitoring the information is responsible for its own bottom line only. If the supply chain data were gathered by a third party this third party would have to be totally disinterested, yet properly incentivised to deliver the technical capability of running the system. Third parties like NGOs or industry associations rarely manage even one of these two. Even if both of those things were achieved, that third party would become a single point of weakness, making them and their operations a vulnerable target for bribery, social engineering or targeted hacking. The truth is, no single third party can make supply chains more transparent. The key to transparency is the decentralisation of data as enabled by blockchains, meaning no single party can control and alter what is seen about the product’s journey.

Huge benefits for customers will emerge from the secure guarantee of a true chain of custody, along even the most complex supply chains, at a very low cost. Blockchains offer a unique opportunity for collective supply chain governance.

## *6.2 Online Dating*

Finding someone special using remote means is nothing new, however the ubiquity of the Internet has boosted the numbers of people looking for love through text and images to astronomic proportions. However, even in today’s wired world, much is wrong with the experience. The Internet’s, provision of ubiquitous, cheap communication makes it all too easy for “love spammers” to approach countless potential dates. Indeed, the technology facilitates such abusers to use the same specially concocted “introduction line” to maximise their chances of a reply. Such activity distorts the “date market”, placing potentially promising partners under heaps of thoughtless opportunists.

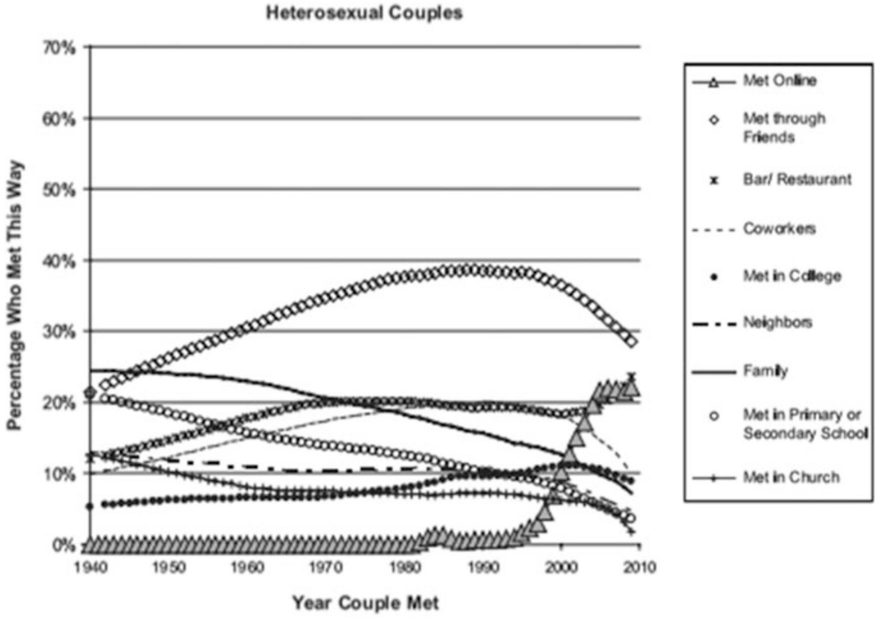


**Fig. 1** N = 2462 for heterosexual couples, respondents are age 19 and older (*Source* Rosenfeld, Michael J. and Reuben J. Thomas (2012) "Searching for a Mate: The Rise of the Internet as a Social Intermediary", American Sociological Review 77(4) 523–547, p 530. Web. 29 Oct. 2015.)

Figure 1 shows the changing pattern of how heterosexual have met over time in the US. Several of the most traditional ways of meeting heterosexual partners had monotonic declines from 1940 to 2009. The Internet is the one social arena that is gaining in importance over time.[3] Solutions to this problem typically fall under two umbrellas: extract a real-world fee for the service of being able to send messages or, use some other metric for filtering would-be dates such as a common-friend, matching mechanisms or pretty face. Both imbue a signal through placing restrictions on the communications. The latter techniques tend to be too restrictive or gameable. Charging blanket fees is a sledgehammer of a "signal" that instantly reduces the market size and makeup to a particular demographic and, unless levied for each message sent, does little to reduce spam.

The walled-gardens that constitute the dating sites that make up different configurations of clientele in terms of geography, lifestyle and interests place additional constraints on the utility of the system as a whole restricting the possibilities and market size.

[3] Ibid, p 528.

In fact, the problem has a fairly simple solution; we wish to keep many of the aspects of the internet (such as breadth of audience and depth of content), but add constraints similar to those of real-life dating to our dating communications: as a recipient we would wish to have some idea of how many other fledgling conversations our suitor is presently engaged. We might be interested to understand to what degree they would rate our attention over, say, any of the other people's attention for which they are vying. As a suitor, we might like to have an online "engagement ring" equivalent for dating, for us to be able to credibly state that we have decided on this person above all others.

Of course these constraints are fairly trivial to implement on a single computer powering a dating site, but as soon as that computer is merely part of a single website or business, we fall short of the vision: people could sign up at multiple websites, perhaps with multiple accounts and thwart the attempts at holding them to their "word". A single global computer, building on a next generation of blockchain computers that ensure additional selective privacy, facilitates precisely these sorts of rule, and placed alongside a strong digital identity system (similar to that of Estonia, Germany) or a decentralised equivalent could be used to enforce the constraints globally, honestly and without exception.

## *6.3 International Trade*

Trade finance is the lubricant of the world economy machine that enables smooth international trade. Over the course of centuries, various tools like "Letters of Credit" and "Bank guarantees" have been implemented to mitigate risks between unbeknownst parties to enable seamless commerce and remove friction from trade related to the lack of trust. In the simplest example, these tools generate the assurance that payments will take place once goods are exchanged according to certain rules. Trade finance not only tries to reduce risk but also to develop tools so that agents can leverage their trade reputation to achieve better deals. Reliable information about the flow of goods and the payment history is essential. Today's offerings usually only start at the end of the supply chain—when invoices are approved—although risks starts much earlier—when the purchase order is raised.[4] Solutions are fragmented; linking suppliers with banks' proprietary platforms proves to be cumbersome and expensive. Studies come to the conclusion that up to $1tr/yr of liquidity is lost through the lack of liquidity.[5]

[4] For more information see: SWIFT White Paper (2013) "The Bank Payment Obligation: a new start for Supply Chain Finance", available online: http://corporates.swift.com/sites/sdccor/files/trade_bpo_white_paper_201304.pdf.

[5] For more information see: Hurtrez, Nicolas and Massimo Gesua' sive Salvadori (2010), "Supply chain finance: From myth to reality", available online: http://www.finyear.com/attachment/252360.

Blockchains come with the advantage of being not only organisationally but also jurisdictionally neutral in the first place (note that yet required compliance can be implemented). Due to the lack of a single authority operating the platform and the unprecendented interoperability, on a blockchain, agreements between international parties can be implemented and related trades executed such that all parties can be sure that changes to and controls over agreements can only be exercised according to rules agreed upon in the first place.

**Acknowledgments** Dr. Sarah Meiklejohn's and Raul Romanutti's efforts at proof-reading and rephrasing some of the harder sentences are also very much appreciated!

## Author Biographies

**Dr. Wood** is the CTO and founder of Ethcore, as well as a founder of Ethereum and Grid Singularity. He was previously the CTO of the Ethereum Project. He is the co-designer of the Ethereum Protocol, created the first working Ethereum implementation, and was the project chief of the IDE, Solidity programming language, and the Whisper protocol. He has pushed the state-of-the-art in programming languages and has given seminars and presented to numerous audiences around the world. He holds a PhD in Music visualisation for Human Computer Interfacing and has coined the terms 'web three' and 'alegality'.

**Dr. Steiner** is the COO and co-founder of Ethcore. She previously oversaw the IT security audit for the Ethereum foundation before the launch of the public blockchain in 2015. She also is a co-founder of Project Provenance Ltd., a London based start-up that employs blockchain technology to make supply chains mor transparent. She holds a PhD in Applied Mathematics and used to work for management consultancy McKinsey where she supported clients in the banking and telecommunications sector with their IT strategy.

# Reinventing Money and Lending for the Digital Age

**Richard D. Porter and Wade Rousse**

**Abstract** Bitcoin and other privately created digital currencies are beginning to challenge central banks' monopolies on money creation. These decentralized cryptographic payment media could ultimately displace legacy banking, finance, and Payment services at a lower cost across the globe. These currencies are likely to continue experiencing a faster rate of improvement than traditional payment media and require less force for safekeeping. This chapter explores some of the forces that led to the rise of Bitcoin including the ball-in tax on deposits during the Cyprus banking crisis in 2013. We also examine the relative stability of Bitcoin as a store value. We also consider new internet-based P2P lending arrangements using Bitcoin rather than dollars as a payment media. Finally, we reassess Stanley Fischer's criticism of Hayek's competitive private currency proposal in light of Bitcoin and other open source digital currencies.

**Keywords** Bitcoin • Open sources crypto currencies • P2P lending with Bitcoin • Gresham's law and crypto currency adoption in china • Cyprus, and Iceland • relative stability of Bitcoin

## 1 Introduction

Money is a social invention (Samuelson 1958; Menger 1892). Through trial and error processes, societal improvements in monetary capabilities are ongoing. According to (Cohen 1998; Sargent 2002), private money predated government-sanctioned coins. Anthropologists have studied it (Hart 2005), and experiments indicate that there is greater voluntary use of monetary tokens as the size of the

R.D. Porter (✉)
Cooksville Digital Coin Lab, Evansville, WI 10905, USA
e-mail: rdouglasp@gmail.com

W. Rousse
Northern Arizona University, Flagstaff, USA
e-mail: wade.rousse@nau.edu

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_9

using group increases.[1] Native Americans used beads on strings as their form of money, wampum. Many assume that the predicates associated with traditional monetary technology must inevitably carryover to the new. But the particular form of money depends on both social customs and technology.

State-issued currency has been the norm for the two last centuries or so. Initially, gold convertibility backed U.S. currency. However, after Nixon closed the gold window in 1971, American legal tender, Federal Reserve banknotes, were only able to satisfy tax obligations or discharge debts. Oddly, in value terms 78.5 % of U.S. banknotes are held in an anomalous denomination, the $100 bill—currently a grand total of over $1T or more than 32 bills per U.S. resident. For transactions, this concentration is remarkable since $100 s are effectively disallowed at most retail outlets. Given this illiquidity, why do so many hold this particular non-interest bearing asset?

We can resolve this paradox by noting that the bulk of the $100 s are stashed overseas negating their tax-paying capabilities.[2] Since the dollar remains the world's primary reserve currency, these banknotes are readily accepted in many overseas banking and payment contexts. Thus, many households in countries with relatively high and erratic rates of inflation voluntarily choose to hold some wealth in dollars to avoid the ravages of home grown inflation (Porter 1996 and Banegas 2014).

In the last few years, new global P2P innovations, such as Uber and Airbnb, have emerged. Uber competes with taxis while Airbnb vies with hotels (Ritter 2015). Similarly, a P2P competitor to traditional bank loans emerged with the advent of Prosper and LendingClub.[3] At about the same time, a fourth category of cryptocurrencies, such as Bitcoin, began to provide P2P payment services across the entire Internet. Like Uber, Bitcoin initially exploited a relatively idle resource, home computers, to protect the integrity of its global ledger, the Blockchain, through modern encryption and other cryptographic advances.

At its core, the Blockchain ledger keeps track of who currently owns the Bitcoins as well as the chain of ownership from the first (Genesis) transaction. Any Bitcoin holder can authorize an entry on this ledger to move Bitcoins from A to B. The pseudonymous inventor of Bitcoin technology, Satoshi Nakamoto, had the Blockchain replicated widely.[4] Under his scheme, an individual transaction could be sent in clear text and verified independently by hundreds of thousands of dispersed nodes all over the world by virtue of public key/private key cryptographic methods.

[1] Cameraa et al. (2013), demonstrated this result in some carefully designed experiments in which participants voluntarily choose to use monetary tokens.

[2] Except in special locations such as Panama, such dollars are not generally legal tender outside the United States or its territories. Their use is widespread but informal.

[3] The Internet has created more efficient P2P matching mechanisms. Some of the new pairings represent the sharing economy, e.g. car rides (Uber https://www.uber.com) and rooms (Airbnb, https://www.airbnb.com), while others improved P2P pairings match investors and loan applicants. Two of the most prominent lenders are Prosper (https://www.prosper.com) and Lending Club (https://www.lendingclub.com).

[4] Champagne (2014) assembles a compendium of Nakamoto's writings on Bitcoin from November 2008 to 2011 together with responses and enquiries from others involved in the project.

Airbnb, P2P lending services, and Uber, all operate through a centralized core. The core handles bookkeeping, designs various interface apps, finds drivers, investors, or residences and deals with a myriad of regulatory challenges. Unlike these P2P innovations, Bitcoin operates without any natural center. It moves funds (Bitcoins) without the use of any trusted party, such as a commercial bank or a central bank. Inviolate mathematics, not a person or committee, runs the Bitcoin ledger and is entrusted to manage processing. As email persistently undercut the cost structure of existing communication schemes such as faxes, first-class mail, telegraph, and telephone, Bitcoin and other virtual currencies like Ripple seek to drastically challenge cost structures for many legacy payment methods: banknotes and bank wires, checks, and all forms of card payments, credit, debit, or prepaid.[5]

Like overseas holders who voluntarily use hundred dollar bills for savings, a few million individuals have willingly chosen to employ Bitcoins.[6] Compared to $100 s, Bitcoins have two unique features: They are scarce and in the digital realm. They use 21st century cryptography and open source methods. Bitcoin also ushered in a host of competitors, cryptocurrencies, now totaling around 600. Throughout this chapter, we use the term math-based currency (MBC) interchangeably with cryptocurrency or virtual currency, when referring to members of this asset class.

According to the British Museum, the best monetary tokens should be: attractive, cheap to make, controllable, durable, easy to carry, good for propaganda, good for both small and large purchases, impossible to forge, and light. Bitcoin embodies most of these features in a disembodied form as a sequence of binary digits. Moreover, Bitcoin has a rigid mathematical supply schedule. The basic Bitcoin protocol makes forging Bitcoins ostensibly very difficult. No one has been able to overwhelm Bitcoin's built-in defenses against such double-spending attacks. One can't rule out the possibility, but the decentralized Bitcoin network has successfully resisted such attacks and accumulated a huge war chest of computing power to fend off such attacks.[7] Bitcoin uses a Byzantine fault tolerance mechanism (Lamport et al. 1982), to carry out a cryptographic style of the proof of work in parallel to ascertain the legitimacy of all individual transactions.

[5] Ripple operates with a more traditional corporate/employment structure than Bitcoin. It has different mechanisms to build consensus and distribute coins (XRPs). This MBC has also sought to establish direct banking relationships in part to facilitate global financial exchange. See ripple.com.

[6] There are no definitive estimates of the number of Bitcoin users. The number of outlets accepting Bitcoin was 100,000 (Curthbertson 2015). As of late October 2015, the number of Bitcoin wallets was about 4.6 million according to blockchain.info with the leading American Bitcoin banking outlet, Coinbase, having 2.7 million users. A lengthy discussion of the pitfalls in estimating the number of users puts the figure at 2.5 million in early 2014, https://bitscan.com/…/how-many-people-really-own-bitcoins-and-why-d.

[7] The code slowly changes to incorporate improvements, e.g., to scale up. But a real shift in the underlying protocol would require close to unanimous assent. Otherwise, a large fork in the Blockchain could disrupt the overall viability of the Bitcoin project. Most users would have an incentive to avoid such a possibility. Thus, while majority rule protects the integrity of the blockchain, a higher threshold of mutual agreement would be necessary to introduce significant changes in the protocol.

Wholesale banking has been in digital form for a long time. But retail payments, particular banknotes, require physical handling and securing. By some accounts these various non-digital processing costs exert a considerable tax on dollar holders (Chakravorti 2013).

From its construction, Bitcoin transactions can avoid the omnipresent cyber-attacks that have continued to disrupt and elevate costs for legacy banking and payment schemes. The Bitcoin's potential is the ability to expunge such frictions and span the globe much more cheaply than these legacy payment vehicles. In historically poor and financially underserved communities, Bitcoin could permit billions of unbanked households to move beyond mere currency and coin.

Such a revolution has another virtue that is infeasible in the traditional payments domain. It is possible to protect the inherent wealth embodied in Bitcoins not with physical force but with cryptography. In the pre-Bitcoin world wealth protection for individuals and banks required vaults, armed guards, and array of private and public clerks and overseers.

The emergence of Bitcoin opens up a number of other possibilities. Does money have to remain a central bank monopoly? When nations standardized and verified coins and provided security for mints, it was then that physical coins became widely used as a medium of exchange in the 19th and 20th centuries. Bitcoin detractors note that since Bitcoin is a private token, it is not legal tender and is therefore not money. Those questioning Bitcoin's provenance are channeling Georg Friedrich Knapp, who said, "The soul of currency is not in the material of the pieces, but in the legal ordinances which regulate their use." (Knapp 1924, 2).

But the Bitcoin Blockchain provides safety and security without armed guards and vaults and provides more functionality than nation state monies at a lower cost. Its attractive finite issue limits are dictated by math and is not subject to pressures to inflate to escape difficult political choices. Just as U.S. banknotes have become worthy competitors to Russian and Argentinean banknotes in those countries and elsewhere as a store of wealth, what's to prevent Bitcoin or other successful MBCs from displacing inflation-prone nation state currencies?

Kenya, for example, has been transitioning to a payment system based on mobile phone technology, the M-Pesa system for an increasing share of its transactions. As such, it would not be that much of a technological jump for Kenyans to go all the way to Bitcoin-enabled payments on smart phones that the new Kenyan entrant BitPesa could conceivably provide. And beyond Bitcoin itself, the approximately 600 open source Bitcoin competitors provide a natural seedbed for a Hayekian experiment to provide MBCs privately and competitively. These new cryptocurrencies broaden the potential choices available to everyone and remove some of the difficulties with F.A. Hayek's decades-old proposal for the denationalization of currency (Hayek 1990).

Over the last century or more, nation states assumed the upper hand in defining what constituted money. As Cohen (1998) points out, however, though the arrangements varied considerably, the concept of money didn't originate with the state, but was taken over by it (Menger 1892). Hayek argued that, as the state took over stewardship of money, improvements ceased and progress retrogressed:

> The great trouble is that money wasn't allowed to develop. After 200 or 300 years of the use of coins, governments stopped any further developments. We were not allowed to experiment on it, so money hasn't been improved, it has rather become worse in the course of time. …Money was frozen in its most primitive form. What we have had since was mostly government abuses of money…. (Blanchard 1984).

Menger was writing near the end of a halcyon century of price stability, while Hayek's views were undoubtedly influenced by the destructive Austrian hyperinflation after the Great War.[8] In its immediate aftermath, J.M. Keynes concluded that such episodes were highly disruptive of societal order:

> Lenin was certainly right. There is no subtler, no surer means of overturning the existing basis of Society than to debauch the currency. (Keynes 1919)

In his manifesto, the Bitcoin founder, Satoshi Nakamoto, sang from the same hymnal as Hayek and Keynes:

> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. (Champagne 2014, 100)

In today's terms Nakamoto, was unhappy with the performance of central banks. But he was also disdainful of the lending and payment practices of commercial bankers. Such practices induced credit cycles and relatively expensive but unsafe electronic banking environments.

The outline for the chapter is as follows. Section 2 compares the readiness and fitness of Bitcoin and other virtual currencies to gold and other legacy payment vehicles. More broadly, we revisit Hayek's proposal for the denationalization of currency. Indeed, the decentralization embodied in Bitcoin and other virtual currencies makes the possibility of more transnational digital currencies such as Bitcoin or, alternatively, local currencies suitable for a narrower domain, such as Scotland or even Detroit, an opportunity that (Jacobs 1984) endorsed.

The third section briefly takes up the forces driving Bitcoin and other virtual currencies in the last few years. The long-run price of Bitcoin depends on its ultimate acceptance and what it displaces. Since Bitcoin is a networked good, the larger its penetration, the more valuable it will be according to McCalf's law.[9] We

[8] "In its origin [money] it is a social, and not a state institution. Sanction by the authority of the state is a notion alien to it. On the other hand, however, by state recognition and state regulation, this social institution of money has been perfected and adjusted to the manifold and varying needs of an evolving commerce." (Menger 1892).

[9] (Bob) Metcalf's law asserts that the value of the network is proportional to $n^2$, where $n$ = the number of network nodes. If there are n nodes, then there are $n * (n - 1)$ possible P2P pairwise network connections, distinguishing between ordered pairs. Finally, $n * (n - 1) = O(n^2)$ in Landau's symbol.

examine some of the forces operating on Bitcoin and other altcoins in the context of three dramatic events: the bail-in tax on Cypriot insured deposits, official Chinese encouragement and subsequent disavowal of Bitcoin, as well as the results of a Bitcoin-type experiment on Iceland, Auroracoin.

The resulting volatility in the price of Bitcoin, induced by these and other disruptions, has led some observers to suggest that Bitcoin may be impractical as a day-to-day currency. Section 4, however, indicates that Bitcoin appears to be achieving more stability than countries in which the dollar has made strong inroads as a store of value, such as Argentina and Russia. So, Bitcoin's viability as a means of payment and store of value is still an open question.

Compared to traditional lending vehicles, Bitcoin has two advantages: the ability to go anywhere cheaply and to be highly divisible. In Sect. 5, we show how new P2P lending platforms have exploited these advantages in over 100 countries. This platform allows private citizens to be financed outside traditional bank lending channels. A final section concludes.

## 2 Comparing Bitcoin with Other Monies

Math-based currencies or cryptocurrencies, such as Bitcoin (BTC) and Ripple (XRPs) are like cash or bank wires in being immediately irrevocable with no chargebacks. Unlike cash they are largely immune from inflation since they're firmly bounded above by a specific number of units or coins.[10] That is, like gold, Bitcoin's allure as a monetary token stems from its limited supply. In the end, there will be no more than twenty-one million coins ever mined.

In a way, Bitcoins can be viewed as improved versions of gold coins with negligible transaction costs.[11] These coins have the additional capability that cryptography (and not force) fully protects them. In uncertain and dangerous environments, this feature gives them an advantage over precious metals or traditional currencies.

What do traditional fiat currencies have to recommend them in the face of this new competition? Essentially, they can be used to pay taxes and discharge debts. But today, unbacked fiat-based currencies (FBCs) are nothing more than expressions of sovereignty or dominion:

[10] That is, Bitcoin and Ripple have a fixed supply of coins in the long run. The growth component for Bitcoin over the next 25 years is about 2 %, near the FOMC's current inflation target. Some of these alternative currencies to Bitcoin have exogenous growth components. Also, some, such as Freicoin, have a demurrage (usage) fee, to encourage use; see Keynes (1961, 353–358). An economy based on Freicoin might be able to avoid the nonstandard monetary policies that the FED and other central banks have followed recently in the aftermath of the Great Recession.

[11] Satoshi (Champagne 2014, 281–282), explicitly compares Bitcoin with gold. He notes that while it possesses none of gold's metallic features such as corrosion resistance, it does have "one special, magical property, [it] can be transported over a communications channel."

> And the vast majority of such monies are unwanted: people are unwilling to hold them as wealth, something that will buy in the future at least what it did in the past has only become apparent since the 1970s, when all the world's governments rendered their currencies intrinsically worthless. (Steil 2007)

There are, however, some important differences between gold coins and Bitcoins. Bitcoin is a virtual object whose ownership can be completely anonymous and thus totally invisible, while gold requires storage and protection.[12] The inventory holding costs of Bitcoin are relatively minor compared with gold.[13] Bitcoin is also remarkably divisible, existing in units as small as $10^{-8}$ of one Bitcoin.

In the long run, the primary allure of Bitcoin relative to the dollar is that it will preserve its purchasing power given that the dollar and other fiat currencies are no longer anchored by gold but by promises that can be forgotten. This feature is probably more important for weaker currencies than the dollar, particularly countries experiencing high degrees of instability since the world left gold. Of course, the dollar has one decided advantage over Bitcoin. Since WWII, the dollar has been the world's reserve currency. As Chairman Greenspan noted,

> Central banks can issue currency, a non-interest-bearing claim on the government, effectively without limit. A government cannot become insolvent with respect to the obligations in its own currency…. A fiat money system, like the ones we have today, can produce such claims without limit (Greenspan 1997, 2)

As an aphorism, Gresham's law refers to bad money driving out good money in the short run. But just the opposite holds in the long run as this adage flips on its head. The logic is straightforward: Should buyers use a superior longer-run value or an inferior one to complete a given transaction today? Obviously, they will be better off in the longer run using the inferior instrument today provided neither payment choice is discounted, whenever they anticipate that the better one might subsequently become more valuable.[14] This revealed preference essentially represents a penchant for good money over the long haul:

> Standing by itself, the general statement, "good money drives out bad," is the more correct empirical proposition. …Over the span of several millennia, strong currencies have dominated and driven out weak in international competition. …
>
> The same proposition holds with respect to the use of materials for international money. (Mundell 1998)

The upshot is this: If currencies can be freely chosen, then the one with the most desirable properties will win out in the long run.[15] This argument applies to all

[12] Strictly speaking, as implemented Bitcoins only have a limited degree of anonymity since the blockchain lists all transactions. More invisible MBCs are being created such as Dash.

[13] The transaction costs of holding gold are not small. Among other costs, commissions on buying or selling coins can be 5–6 % while insurance runs as much as 1 to 1-½ % per year.

[14] Hayek (1962) explores the history of thought of this concept.

[15] Guidotti and Rodriquez (1992) presents this long-run reversal of Gresham's law in an optimizing framework.

currencies, including digital ones. That is, if these MBCs represent sufficiently better payment mechanisms than fiat based monies, there is no reason they couldn't eventually displace FBCs.

Enforceable taxes create the demand for legal tender. This force will still hold even as home-production income generated on the Internet may be inherently more difficult to tax than traditional retail outlets. But MBC-based activities that end up with a sufficiently broad base of users will have the wherewithal to pay the taxes.

Thus, Greenspan's declaration that banknote claims can be unlimited requires some qualifications in light of the issue raised by Steil. Simply put, there may now be more constraints on fiat currency issuance. Given the Zimbabwean experience, for example, it is not clear that they could ever issue fiat banknotes.

On the supply side, the labor and capital content of processing Bitcoin payments appears to be orders of magnitude less than the legacy payments systems they seek to supplant. As an open source project that was freely bequeathed to the Internet by its nominal creator, Satoshi Nakamoto, Bitcoin requires only a small coterie of programmers. As a result, the associated capital and computing costs are quite small. Moreover, the vast computing power of the distributed network of thousands of nodes that support the integrity of the Bitcoin network, the mining community, voluntarily provides vast amounts of computing power in the hopes of winning Bitcoins by solving cryptographic puzzles. The resulting cost structure allows Bitcoin and other MBCs to support worldwide payments more cheaply than legacy banking institutions or governments.

In ways, these new digital tokens are analogous to the way that gold and silver coins of standard form and weight often circulated far outside their country of origin. For example, before our pure fiat monetary era, coins from the Latin American Union circulated in over a dozen countries in both Europe and the Americas for over six decades.

In a recent paper, Erb and Harvey find it difficult to gauge the target for the *price of gold*, given its present value over various time intervals. They conclude:

> In the end, investors are faced with a golden dilemma. Will history repeat itself and the real price of gold revert to its long-term mean—consistent with a "golden constant"? Alternatively, have we entered a new era, where it is dangerous to extrapolate from history? (Erb et al. 2013)

For example, Erb and Harvey find scant evidence that holding gold has been an effective hedge against *unexpected* bouts of inflation whether measured in the short term or the long term.

At first blush, MBCs seem much more alien and opaque relative to that of gold. But even under a gold standard, monetary arrangements weren't necessarily that secure or foreseeable. The standard itself was not immutable.[16]

[16] It was altered numerous times, e.g., to assuage U.S. silver mining interests. Of course, gold (or silver) discoveries would alter prices. Moreover, the prices of precious metals depend on demand and supply. But supply put onto the open market occasionally depends on the behavior of nation states. Together with the IMF, governments remain the largest holders of gold bullion.

Despite the trust issues, however, Bitcoin is not without a level of voluntary backing. A broad community of network users relies on the Blockchain ledger, which tallies users' holdings since the network's inception. In turn, the Blockchain is backed by a decentralized replication, consensus, advanced cryptographic techniques and enormous computing power. In short, Bitcoin is founded on the collective support of a fairly deep and broad community of hundreds of thousands of users spanning the globe and encompassing virtually all locations. Many of those that have used the dollar in lieu of their own fiat currencies, as arguably a poor man's gold substitute; one might view Bitcoin as disputably a better gold substitute than the USD, albeit one of somewhat limited use currently to the extent that it remains much less liquid.

Thus, in many ways Bitcoin and other altcoins are simpler and more straightforward concepts than gold. Each consists of thousands of lines of code that connects hundreds of thousands of individuals on distributed networks. And, the BTC supply function is more rigidly determined than gold because the protocol mathematically limits the total supply of Bitcoins in all horizons.

A Bitcoin supporter might even argue that BTCs are more trustworthy than gold. There were difficulties in trusting governments to preserve purchasing power, even in times when they were nominally still operating under a gold standard, e.g., during wars. The New Deal prohibited private gold holding and abrogated the gold clause in corporate bond contracts. Thus, will a strategy of holding gold as insurance against small probability tail events work when those tail events occur? Put differently, how viable will such a strategy be if society voids the protection afforded by owning gold just when its value is the highest?

While nations can still invoke the requirement of having to use *their* legal tender inside *their* borders, this imperative will not necessarily be that compelling when considerably better alternatives exist. Over 60 years ago, Abba Lerner declared confidently

> The modern state can make anything it chooses generally acceptable as money and thus establish its value quite apart from any connection, even of the most formal kind, with gold or with backing of any kind. (Lerner 1947, 313)

At the time, a fixed exchange rate between gold and various currencies imprinted an international standard so that investors didn't have to fret that their foreign

(Footnote 16 continued)

Accordingly, the incentives of these players may lineup with political and not necessarily economic objectives. Finally, one reason that gold often tends to accumulate in the hands of nations is the considerable amount of force needed to safeguard it, e.g. at Fort Knox. Monetary instruments went from being in hoards held by individuals (Peebles 2008, 235), to being held in financial institutions. There is no reason Bitcoins couldn't revert to this earlier form of dispersed "storage" in individual hoards, at least provided adequate safekeeping facilities appear. Alternatively, Bitcoins, could become part of the short-term liquidity pools in repurchase agreements and the like.

currency positions might collapse overnight. After currencies had become pure manifestations of sovereignty, the dollar emerged as an international standard and gradually became the bellwether store of wealth. This phenomenon was especially true for those in countries with unstable banking systems or currencies such as Russia, after the fall of the Berlin Wall, or Argentina, which has been subject of a crazy quilt of bizarre monetary regimes ostensibly forever (Paolera 2001).

Given all these imponderables, it is true that, no matter what happens, the dollar is currently a stronger anchor than any other fiat currency. In the world of floating exchange rates, sharp changes in relative currency valuations can occur. These fluctuations lead risk-averse investors to seek out the dollar for precautionary reasons. While the dollar may not be as safe as gold, it is currently safer than every other currency.

One might counter that while the Bitcoin space has the advantage of Blockchain technology, which arguably is a real improvement, it has faced a host of problems that traditional banknotes have not. There has been widespread fraud on many Bitcoin exchanges, Moore (2013), including one of the most prominent, Mt. Gox. Moreover, the technology, at least in the early stages, often appears to be prone to fraud: When people lose their private keys, their Bitcoins are forever lost; they do not have the recourse options that credit card holders have, but are like banknote holders who misplace cash. But considering the card space itself, fraud is hardly inconsequential and, if anything, a more thorny problem to overcome.

## *2.1 Divisibility*

Though gold and Bitcoins have some similarities, there are important differences with respect to payments. While gold and silver coins once freely circulated in the Americas, Asia, and Europe, it is not clear that would make much practical sense today. Today, a twenty-dollar gold coin would weigh only about 1-½ times that of an ordinary paper clip, which would hardly make it practical for most transactions. Bitcoins can be divided into much smaller units or fractional coins up to $10^{-8}$ of one Bitcoin, which is called a Satoshi. To illustrate, if the BTC price were $250 per coin, 20,000 Satoshi would be worth a nickel.

As a payment system, BTC transactions make considerably more practical sense than moving gold around. The advantages of BTC relative to gold coins arises from the extremely low transaction costs inherent in BTC that make it much more liquid than gold, though there has been a considerable tendency to hoard it; see (Tasca 2015). Ultimately, this liquidity reduces transaction costs and induces greater usage. The emerging Bitcoin community is also beginning to recognize that Bitcoin may be safer than fiat banknotes or coin if properly secured since their virtual status does not necessitate physical security.

## 2.2 *The Open Source Cryptocurrency Revolution and Hayek's Denationalization Proposal*

The Bitcoin revolution exploits open source technology. This feature makes the characteristics of the currency transparent for all who wish to look under its veil. Open source-based currencies accurately reflect the time series pattern of the supply function for new coins. In addition, their security properties will also be evident by inspecting the code. So with the advent of Bitcoin, the technical substitution possibilities underlying Hayek's competitive private currency proposal have changed. Hayek imagined a competitive state of affairs in which alternative currency suppliers created their own "coins" and marketed them to the public, much like the free banking era in which private banks issued their own banknotes denominated in dollars.

The Blockchain, as well other features voiding double spending in other MBCs, undermine Stanley Fischer's criticism (Fischer 1986), of F.A. Hayek's proposal (Hayek 1990). Based on the technology of the era, Fischer argued that private currency suppliers would not necessarily create currency tokens that had stable purchasing power. Rather, private currency producers might have an incentive to cheat on their promised coin policies or suddenly depart from the prudent strategies. Fischer thus argued that there were no economic forces ensuring that the private marketplace had the incentives to produce what Hayek imagined. All Hayek had in the end was the hope that the supply process would result in stable purchasing units. But there was no reason to guarantee that would happen.

Put differently, under Fischer's critique of Hayek an established private currency would be tempted to produce inflationary surprises, the problem of dynamic inconsistency. Moreover, having the state be the sole currency issuer was efficient compared to Hayek's competitive solution that required competition and multiple currencies. One currency made it easier to detect counterfeiting.

While both issues represented legitimate concerns when Fischer first raised them, the advent of the MBC protocols sweeps them aside. Most MBC protocols such as the Bitcoin protocol are immutable and strictly programmed to produce only a fixed number of coins. Assuming the protocol remains intact, dynamic inconsistency is not feasible. Secondly, the Bitcoin protocol has thus far proven to be resistant to counterfeiting attacks, which were one of the key design objectives of its creator. Indeed, we now know how to produce monetary trust after Bitcoin's creator specified the production function for the Blockchain. We also know that Bitcoin has worked quite well empirically to maintain the integrity of the transactions on Blockchain under a variety of real world challenges. This empirical success removes Fischer's objections.

Together with several dozens of successor coins to Bitcoin, such as Litecoin and Feathercoin, Bitcoin and Ripple provide a "seed bed" for evaluating F. A. Hayek's guesses regarding a competitively-determined monetary environment. Hayek's

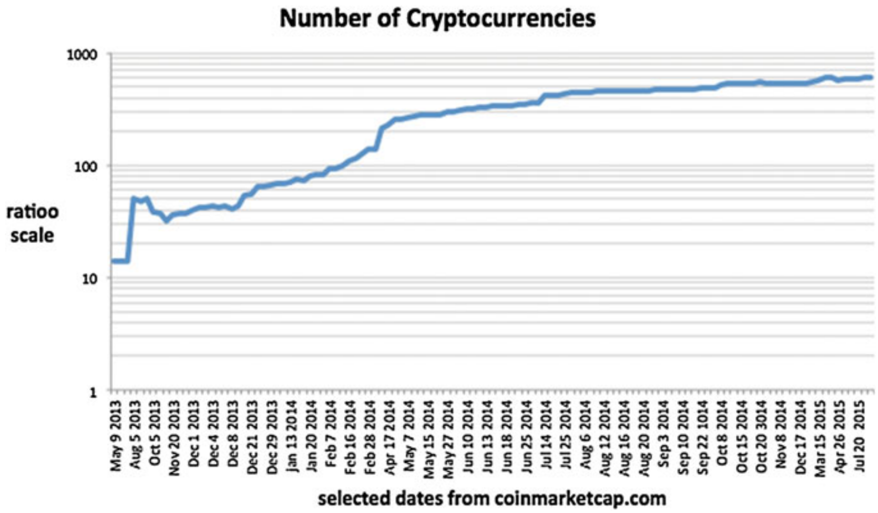


**Chart 1** Time series on the number of MBCs

ardently believed that such a currency regime would improve welfare and upend the monopoly that nation states had in currency issuance. Hayek forcibly argued that nation states had generally failed to be steadfast currency issuers. Hayek thought successful currencies able to maintain purchasing power would arise from a bottom-up marketplace of competitively provided tokens. Efficacious currencies would attract a sufficient base of users by being more stable sources of purchasing power.[17] That is, Hayek's intuited that the competitive process would yield an equilibrium in which those private currencies that provided the most stable sources of purchasing power would become the dominant currency suppliers. It is conceivable that such private MBCs could eventually displace public currencies across the globe or could conceivably be adopted by some public authorities.

It is too early to judge where the rapidly expanding list of MBCs will end up. The family of competing currencies is only now beginning to emerge together with the varied regulatory response across the globe. Perhaps most importantly, for the digital currencies to succeed and become mainstream financial products, there is a paramount need for a greater degree of stability and safety on the currency exchanges. Suffice it to say it is difficult to see where the competitive process will end up when it has matured and there is a more widespread adoption. But the variety of coins being created is interesting and impressive in ways.

[17] It is interesting that a private currency supplier (Stalnaker 2011), ended up pursuing approximately the strategy that Hayek argued a private currency producer would be obliged to follow to be successful (Hayek 1990, 60–61).

Chart 1 shows the time series of the *number* of various cryptocurrencies. The number of coins reached the 100 mark in early 2014, following the big burst in the dollar price of Bitcoin near the end 2013. Subsequently in 2014 entrepreneurs added over 400 new altcoins by October before the process began to plateau. All of these new currencies obey production functions that strongly distinguish them from legacy payment vehicles.

For example, consider security. By the very nature of the open source process, potential security holes can be directly accessed and modified if need be to incorporate technical advances in cryptology or computing.

At first glance, any open source structure seems deliberately uneconomic: Why freely share code as open source projects repeatedly do? The answer, we think, is the lines of code are not static but part of the changing structure of an ongoing project that is in a continual state of improvement. Open source efforts are, in their own way, like a currency: As more programmers use them, the code has greater value. Here is Metcalf's law at work once again. Indeed, in some computer environments, these arrangements work quite well and allow various competitors to cooperate and share knowledge with mutual benefits for all. For example, human capital regressions find greater log wages for open source coders in the Apache webserver project than others, amounting to a growing secular wage premium of 13–27 %.[18]

Open source code can be customized to suit particular requirements—to change on the fly–without waiting for the next release of commercial code. Currently, the MIT media lab supports ongoing Bitcoin programming efforts, which consist of a small staff of three programmers, plus occasional volunteers from all over the world.

The resulting speed of advance in the digital sphere of coin creation and extension compared with legacy production methods for banknotes is impressive. First, we just noted that in Bitcoin's short experience, several hundred copycat cryptocurrencies have been created. While some of these new coins are relatively trivial extensions, all have had an opportunity to thrive in the competitive cryptocurrency marketplace. Some like Dogecoin started as a prank, but has remained in the top five in market cap of all virtual currencies.

In terms of P2P money transfers Bitcoin works reasonably well as do some competitors like Ripple. The main problem confronting Bitcoin has been outside the P2P domain in trying to extract immediate value by converting Bitcoins to other currencies, such as the dollar, the euro, or the yuan. These transactions occur generally on centralized exchanges that have witnessed a considerable share of fraud and start-up problems, Mt. Gox, being the prime example.

[18] "An Empirical Analysis of Economic Returns to Open Source Participation," Il-Horn Hann, Jeff Roberts, Sandra Slaughter, and Roy Fielding. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.6697&rep=rep1&type=pdf.

## 2.3 Comparing Banknotes and Card Payments with Bitcoins

It is useful to compare technical improvements in the production function for virtual currencies with that of banknotes. Consider the most popular U.S. banknote, the $100. It took 2 years from 1989–1991 to introduce a security thread to combat the high-grade, Intaglio counterfeit $100 s produced in North Korea. Another 5 years elapsed until 1996 to upgrade that note to allow for a bigger head on the front for more accurate authentication and to improve the security thread. Finally, it took 17 years to put out the technology embedded in the current $100, the series released in 2013.

Conceivably, these relatively cautious responses to changing counterfeiting threats were optimal responses, given counterfeiting problem facing the United States has stayed at low and manageable equilibrium value (Lengwiler 1996; Judson and Porter 2012). Still, the full costs to society of all the resources devoted to U.S. currency production, distribution, and handling by all sources are not small but may amount to as much as $200B per year, Chakravorti (2013). Moving funds around electronically would be unquestionably cheaper and thus have much to recommend it. So in comparison with Bitcoin and the hundreds of new altcoin competitors, the advances in the traditional banknote space occur at a snail's pace and remain relatively expensive, all things considered.

Regulation is perhaps a worrisome prospect for Bitcoin and other MBCs. It could be too stringent and prevent these revolutionary payment means from getting a sufficient foothold to survive. Regulatory capture might mean that regulators end up doing the bidding of bankers that wish to blunt the effectiveness of these competitors in their traditional domains. Moreover, fiat currencies afford no consumer protection for inflation but cryptocurrencies generally do. So how should regulators balance these out? Can they?

There are clearly some fraudulent pump and dump schemes that wily cryptocurrency promoters have foisted on unwitting users. But the general complexity of the situation and the fact that the code is normally an open book, means that buyers can be forewarned and armed against faulty currencies. A policy of allowing users to keep their eyes open augmented by assessments by private experts may even be better than any lite-touch regulation.

If the benefits of the innovation are large enough, then in some fashion, disruptive innovations such as Uber and Bitcoin will become "legitimate" and "accepted". It is almost always the case that radical new technologies need to inveigle their way into law and regulation by a process of trial and error. If existing regulations are in strong conflict with the enhanced benefits of the innovation, participants may have sufficient incentive to skirt the initial prohibitions. Eventually regulations are likely to become less hostile to the innovations as public opinion in an open society begins to bow in the direction of the innovations.

There is undoubtedly a natural inclination to classify Bitcoins as being like banknotes. They certainly share some common properties. They are both almost instantaneous and irrevocable. In face-to-face transactions, in so-called Project

Buttonwood transaction, they would be quite comparable.[19] Moreover, it might even be rational, at least for some, to engage in such direct P2P exchanges given the serious startup problems on the public exchanges. But there are clearly important efficiencies and obvious timesavings in transacting on exchanges, including presumably better price discovery. So we believe that a set of reliable exchanges, such as San Francisco's Coinbase, will eventually become the norm.

Finally, it costs Western Union real resources to get currency to remote locations. For the millions of workers living abroad and sending parts of their salaries back home, such remittance costs remains quite large, on the order of 6–9 %. The comparable cost for Bitcoin is virtually zero, a fact that is attracting a host of competitors in hopes of becoming the "Western Union" for the emerging digital age.

## 3 Virtual Currency Adoption: China, Cyprus, and Iceland

It is helpful to gain some insight into the economic forces impinging on MBCs by looking at three actual events. The first two, China and Cyprus, catapulted Bitcoin in 2013 onto the world stage. The third, Auroracoin on Iceland in 2014, demonstrates the difficulties in supplanting nation state currencies with something arguably better.

### *3.1 The Chinese Back and Forth on Bitcoin*

The Chinese real economy has grown rapidly at nearly double-digit rates over the last 35 years or so, yet its financial system retains strong repressive elements. Chinese are still forced to hold yuan, which is not freely convertible into other currencies, but fluctuates in a relatively narrow floating band to the dollar set by the People's Bank of China (PBOC). PBOC officials have signaled that they intend to make their currency fully convertible, but Chinese citizens today have to abide by strict annual limits of $50,000 on the funds they can pull out of China.

There is considerable tension between the United States and China arising from an economic constraint of sorts, the Triffin dilemma. As the reserve currency for the world, the United States is in the enviable position of receiving an interest-free loan when it gives dollars to foreigners. But this benefit comes at a price, the Triffin dilemma or paradox. Powerful domestic political forces want their domestic industries to be competitive internationally but without large trade deficits. Triffin first showed that it was not possible to have both cheap sources of capital from

[19] Buttonwood transactions represent preannounced meetings where a buyer with cash buys Bitcoins from a seller that has the relevant information on a smart phone.

abroad and positive trade balances. So, as China's trade surplus with the United States has grown to be large, its international holdings have become more and more concentrated in dollars. As a result, China has become increasingly wary about having so many of its reserves in the U.S. dollars. In particular, they have looked askance at the nonstandard U.S monetary policies that have been undertaken in the aftermath of the financial crisis.

In short, many Chinese are unable to diversify away from the yuan as much as they might like. Given the binding constraints on their ability to maneuver, Bitcoin might seem to be an attractive option by loosening the repressive effects of Chinese currency yuan management. Indeed, Chinese officials initially supported Bitcoin as an alternative to the dollar, which enabled it to acquire a strong following.[20] Bitcoin provided one method of getting funds out of China with fewer hassles both for officials and entrepreneurs. For the Chinese, the inherent freedom and simplicity of Bitcoin made it attractive; see (Rabinovitch 2013).

By July 2013, there were over 100,000 active Bitcoin nodes across the globe with about one-fifth of them in China. Both the Chinese previous experience with the digital currency Q Coin and their penchant for gambling also played important roles in boosting the demand for Bitcoin (Popper 2015). Of course, encouraging Bitcoin is not the same as disparaging a dollar standard. Bitcoin might be an attractive option for rich Chinese urban residents. It could mitigate some of the relatively restrictive Renminbi currency regime and allow them to diversify.

In any event, Chinese demand for Bitcoin grew smartly over the fall of 2013, boosted after Baidu, the Chinese equivalent of the Google search engine, began adopting Bitcoin for certain payments in mid-October. Interest in Bitcoin within China, according to Google Trends, is shown in Chart 2. The first peak occurred at about the time of the proposed Cyprus bail-in tax and ensuing bubble-like response of BTC over the following month. The second much larger blip took place at the end of November when one Bitcoin surpassed the price of an ounce of gold; it subsequently trailed off to zero by mid-2014.

Given the relatively small size of the traded amounts of BTC, it is unlikely that the surging interest in Bitcoin threatened the Chinese currency peg. Perhaps, the dose of freedom was too difficult to fit into existing regulatory frameworks. In any event, in December 2013 China began to reverse course and slowly clamp down on access to Bitcoin by limiting bank access. Gradually, Chinese officials put more roadblocks in the way of Bitcoin trading.

To recap, Bitcoins reached a peak of $1153 in early December 2013 before gradually retracing a fair amount of the surge as China put more restrictions on Bitcoin trading. From Chart 3, it appears that the surge in Google trends users across the world fairly closely matched the run-up the Bitcoin price in 2013 and

[20] Chinese interest was partly the result of deliberate governmental policy in which a state-sponsored TV show portrayed Bitcoin in a positive light.

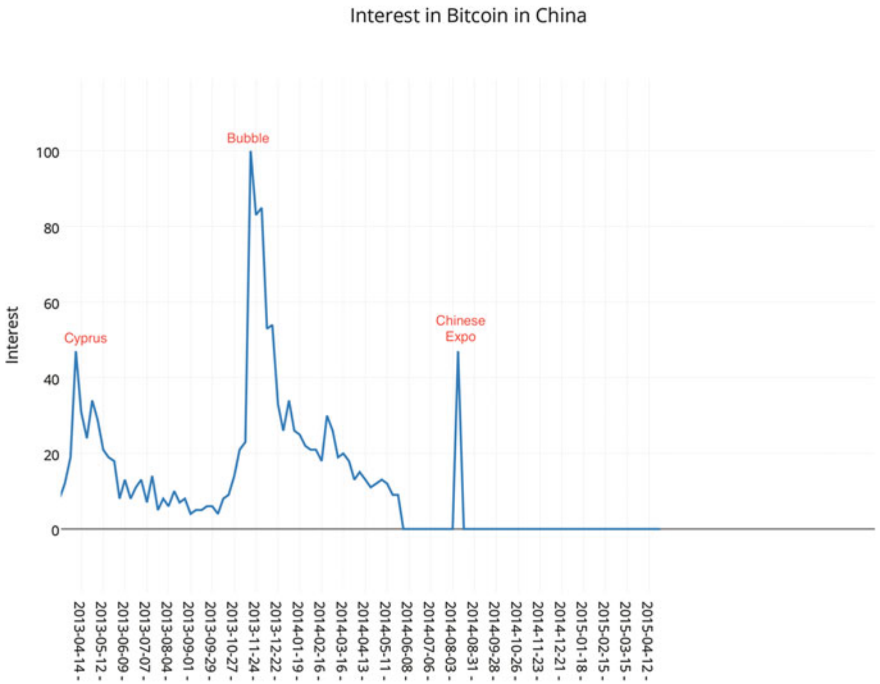


**Chart 2** The Google trend interest in Bitcoin within China, 1/1/13 to 4/30/15

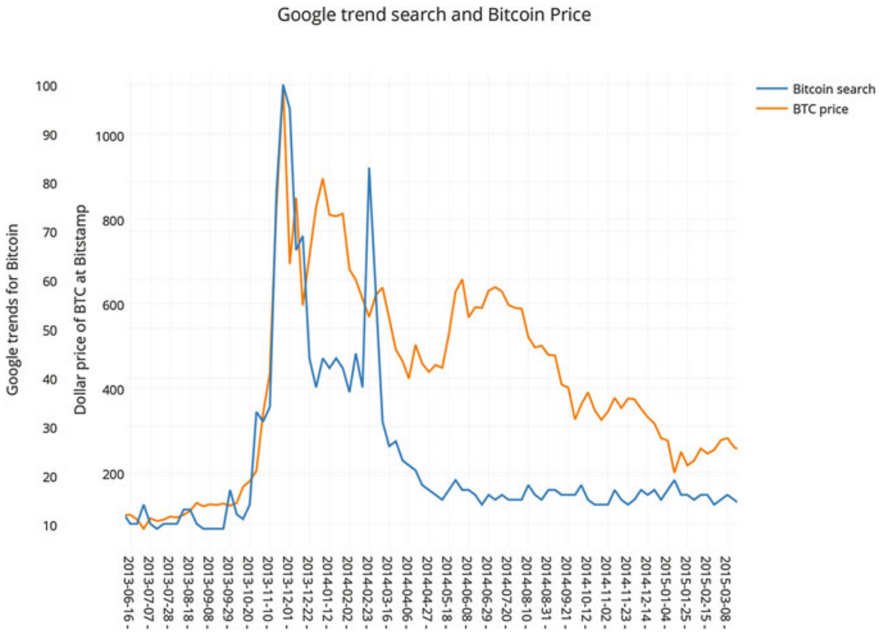


**Chart 3** Overlay plot of Google trends for Bitcoin and dollar price of BTC

early 2014. Subsequently, apart from the Mt. Gox collapse, the Google trends index has plateaued. Conceivably the stationary state reached by the index in mid-2014 eventually moderated the dollar price of Bitcoin, a development which we take up in Sect. 4.

## *3.2 The Cyprus Bail-in Tax and the Subsequent Bitcoin "Bubble"*

The U.S. financial crisis ultimately reverberated to Europe. As the fallout spread, countries on the periphery began to have difficulties in rolling over their debt, which led to a full-fledged sovereign debt crisis in Greece, which, in turn, challenged Cypriot banks that had heavily invested in Greek sovereigns (Kambas 2013).

The crisis moved to Cyprus when the Greek government subsequently defaulted on their debt, which pushed two large Cypriot banks into insolvency. A full-fledged panic ensued when Cypriot bank depositors discovered that their capital-short banks were going to be recapitalized from *within*. European authorities planned to convert depositors' balances (including those with full deposit insurance) and re-label them as equity ownership claims on the recapitalized banks. Specifically, on March 16, 2013, depositors woke up to such a plan: a one-off bank deposit levy of 6.7 % for insured deposits and 9.9 % for balances above €100,000 on all domestic bank accounts at two Cypriot banks. Not surprisingly, the announcement shook financial markets.[21] And, indeed, the fallout continues to roil markets as further policy repercussions continue to put burdens on depositors first before taxpayers.[22]

Immediately, many in Cyprus and elsewhere began to take a fresh look at the opportunities for avoiding bail-in taxes by holding Bitcoins as a defensive maneuver. Almost instantaneously, interest in Bitcoin jumped in a variety of locations, including Argentina, China, Cyprus, and Russia (Chart 4). Speculators, perceiving the new supply-demand configuration, promptly bid up the Bitcoin price. The implied increase in demand set against the backdrop of a highly rigid supply curve of new coins created pushed the price up to a peak of above $200 before ebbing back over the spring. The USD price of BTC began to drift up more steeply in February and then even more so in March when the Cyprus crisis came to

[21] The ECB, IMF, and European Parliament all agreed to this plan. Finally, at the end of July the Cypriot central bank agreed to a 47½ % haircut with international creditors on deposits exceeding €100,000 in the Bank of Cyprus with the confiscated funds used to recapitalize the bank.

[22] About a year later, the Europeans decided to extend the Cypriot bail-in strategy for all ECB bank failures. The G20 reached a similar conclusion at their Melbourne meetings in the fall of 2014. A rational depositor might now worry that that deposit insurance might not afford as much protection and thus be more willing to assume the vagaries of holding Bitcoin to avoid the potential bail-in taxes on their bank deposits.

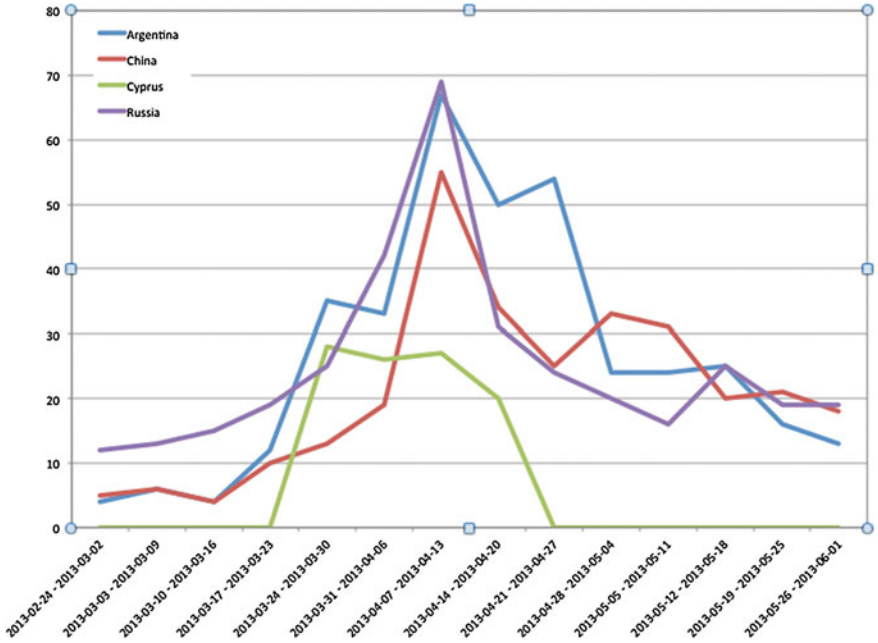


**Chart 4** Google searches for Bitcoin for selected countries: Argentina, China, Cyprus, and Russia—March to June 2013

a boil. Part of the peak outside of Cyprus appears to be in response to the price of Bitcoin itself, which peaked in mid-April.

Chart 5 shows the dollar price of BTC at the Winkdex index. After the bail-in tax was announced, the price of Bitcoin immediately shot up. (The Google trends information in Chart 4 suggests that the slightly more delayed response occurred in China.) The Russians who were heavily invested in Cyprus clearly had a direct interest in BTC because of their experiences in Russia and the former Soviet Union, see (Porter and Judson 1996), but so did many others.

After the “bubble” burst, the BTC price nosedived but soon stabilized and eventually appeared to strengthen over the fall. In retrospect, it should not be surprising that such a large induced shift in demand set against the highly inelastic ongoing Bitcoin supply function of new coins resulted in the dollar price of Bitcoin jumping in the very short run before reversing course, i.e. the intermediate price peak was not necessarily that sustainable in the short run.

The coins arrive mechanically as a Poisson process in lockstep with Satoshi’s protocol.[23] The fallback in price occurred when the demand burst ran its course so

[23] A prize block is found about every ten minutes. It is a Poisson process with parameter λ with λ chosen so that 2016 blocks are found on average every two weeks. Since the expected number of events is proportional to the elapsed time between prizes, or ten minutes, i.e., it follows that 2016/(2 * 7 * 24) Bitcoins are found on average in an *hour*.

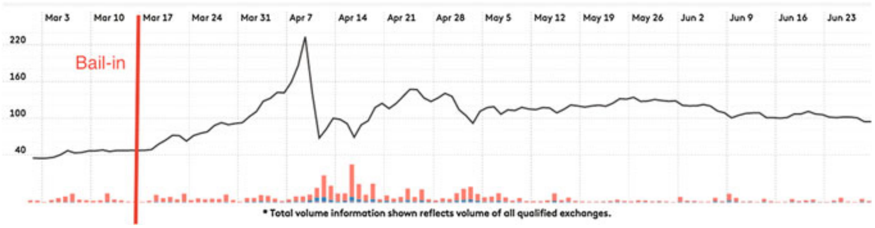


**Chart 5** BTC price in dollars at Winkdex, 3/1/13 to 6/30/13

that incoming supply of Bitcoins can only be priced at a lower value to equilibrate the declining flow demand with the increased flow supply. The mini blip in the price of BTC evident in Chart 5 may align with some definitions of a financial bubble, but we see it as a predictable response to the after-effects of the bail-in tax. Namely, it is the expected result from a downshift in the flow demand for Bitcoin set against the fixed Poisson supply process of new Bitcoins.

### 3.2.1 Further Evidence on the Reaction to the Cypriot Tax

This announcement of the bail-in tax led to the outpouring of interest in Bitcoin on Cyprus from two immigrant groups who had gone to that Island to escape monetary and civil disruptions in their home countries, Lebanon and Russia. Both became major deposit holders in Cypriot banks.

Russian language accesses in Wikipedia of the word *Bitcoin* skyrocketed by a factor of over 2.4 from 74,380 requests in March of 2013 to 178,903 in April as the Bitcoin price peaked at around $250 on April 9 before falling just as sharply to about one-fourth of that the next day. But the decline was relatively short-lived, and the currency subsequently stabilized at around $130 before advancing over the fall. Chart 6 shows a striking correlation between the price movements around the time of the bail-in tax and access of Bitcoin by Russian speakers.

It’s unclear how much of the price swing is attributable to the Cypriot proposed bail-in tax. A simple exploratory regression of prices or price changes on the daily Russian-language access requests (Table 1), finds significant coefficients on the access requests for three different specifications. Of course, these simple regressions are hardly definitive due to their small sample size; at best they can only be suggestive. The response could rationally extend well beyond Cyprus to other places such as Argentina, which reportedly also had a surge of interest in Bitcoin as a result of the Cypriot episode.[24]

[24] A kitchen-sink regression could include downloads of the Satoshi client in various countries, which is a clearer indication of more active interest than an encyclopedia inquiry. Also, the behavior of existing Bitcoiners or miners would also affect the price.

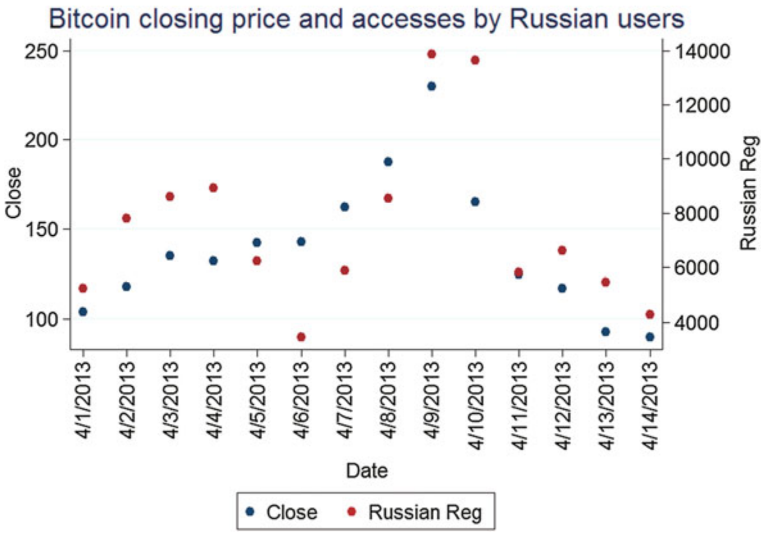


**Chart 6** Closing price of BTC in dollars on Mt. Gox and Russian language Wikipedia accesses of "Bitcoin" showing shows the positive correlation over first 14 days of April 2013

**Table 1** Regression of prices on Russian accesses of Bitcoin[a]

| Coefficient or Statistic | First differences | | Levels |
|---|---|---|---|
| Intercept | 0.6625986 (0.1) | – | 74.79286 (3.73) |
| Accesses | 0.0055818 (2.7) | 0.0055866 (2.85) | 0.0085945 (3.44) |
| Root MSE | 23.169 | 22.193 | 28.083 |
| N (sample size) | 13 | 13 | 14 |

[a] t-stats in parentheses beside estimated regressors

Thus, the willingness of Euro officials to adopt bail-in solutions is surely a precedent hanging over further Continental bailouts. The resulting capital controls that ensued in Cyprus and the general malaise that followed appeared to give new impetus and interest there and elsewhere to Bitcoin including especially Greece, which has been struggling for about the last 5 years.

## *3.3 A Crypto Currency Experiment on Iceland: Auroracoin*

In many ways, Iceland could be seen as an ideal place for a virtual currency. It had an educated workforce who understood modern finance.

> The traditional fishing-based economy was altered dramatically. Financial engineering became the preferred career path of ambitious youth, instead of the traditional natural-resource management. Young men on the streets of Reykjavík were as likely to

**Table 2** Google trend scores for Bitcoin from 2011 through June 2014

| Rank | Country or City | Google trend score |
|---|---|---|
| 1 | Iceland | 100 |
| 2 | Estonia | 94 |
| 3 | United States | 79 |
| 4 | Netherlands | 77 |
| 5 | Czech Republic | 76 |
| 6 | Canada | 75 |
| 7 | Finland | 73 |
| 8 | Hong Kong | 73 |
| 9 | Cyprus | 71 |
| 10 | Slovenia | 66 |

> know the Black-Scholes formulas as the yields from the day's salmon catch (Bagus and Howden 2011, 1–2).

This initial condition may explain the heightened interest in Bitcoin evident in Table 2. Surprisingly, the Google trend index for the term *Bitcoin* scored highest in Iceland over the period from 2011 to 2014 June. Even granting a greater smattering of financial knowledge on the Island than elsewhere, this result still seems rather anomalous. Why would this island nation—with a small population and closer to Greenland than Scandinavia–have so much interest in Bitcoin than any other location?

One possible explanation was the capital controls that were introduced in the aftermath of the financial crisis, Boyes (2009). When the financial crisis hit Iceland immediately after the Lehmann collapse in the early fall of 2008, the Central Bank of Iceland was unable to be the lender of last resort. It had no choice but to let 90 % of its banking system collapse (Gudmundsson and Thorgeirsson 2010) and introduce controls on fund movements to avert an even larger collapse.

Also, Iceland might be a candidate for a virtual currency Boyes (2009). The country had experienced an exceptionally erratic monetary policy for decades that had reduced the purchasing power of the Krona relative to the dollar to less than 1/120th of what it was 40 years earlier.

Thus, the prospect of a virtual Icelandic currency as a substitute for the unstable Krona had to have some appeal when it was announced on the Bitcoin forum on February 2, 2014. The Icelandic MBC was called Auroracoin and based on the Litecoin.[25]

> Auroracoin is designed to break the shackles of the fiat currency financial system in Iceland.
>
> Iceland has been hit hard by financial meltdown and inflation. Not only did the entire banking system collapse in 2008, but the monetary history of Iceland is one of inflation, devaluation, and currency controls. Auroracoin is an opportunity for Icelanders to free themselves from currency controls and government debasement of the currency.

[25] See http://auroracoin.org.

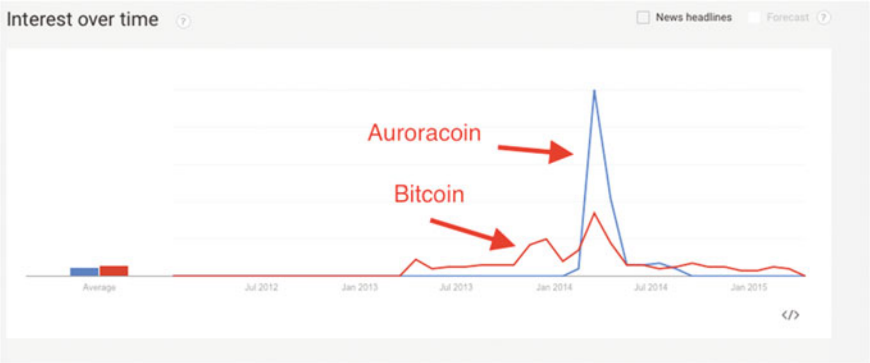


**Chart 7** Comparison of Google trends for Auroracoin and Bitcoin on Iceland, from 2011 to 4/30/15

This announcement had to be at least a partial catalyst for the extraordinary level of interest in Google trends for the word *Bitcoin* evident in Table 2 and in Chart 7.[26]

On March 25, 2014, 31.8 Auroracoins would be available to each inhabitant. Half of the coins would be dropped and half mined using a Litecoin scheme. Before the actual airdrop, a speculative frenzy propelled each existing mined coin to nearly \$96.81 (corresponding to a market cap of over one billion dollars) 3 weeks before the launch. So while there appeared to be a considerable number of Icelanders who were intrigued in some way by the concept, the actual take-up rate was only about 10 %. Afterward, the price of an Auroracoin continued to sink, ultimately stabilizing around 20¢ in early June 2014.[27]

Thus, the Icelandic reception of Auroracoin seems rather modest relative to the potential demand, as embodied in the ranking from the Google trends. Reportedly there were some mechanical difficulties in acquiring the coins, and convenient wallet apps were not initially available. So the reluctance to embrace Auroracoin may have been more a problem of execution and implementation rather than the underlying concept. To be sure, Auroracoin might be conceptually confusing to many Icelanders even if the coins were free for the taking.

For any new currency, there is always the question of whether there will be partners to exchange coins if one decides to hold onto them. It is this disparity that lies at the heart of the difference between the demand for Auroracoins and for U.S. banknotes outside the United States. For U.S. banknotes, one knows they will trade tomorrow at virtually the same price as today. One may be somewhat more assured of that for Bitcoins too since they've been around for over 6 years and have acquired some liquidity and universality. But for Auroracoins, there was no

[26] Margeirsson (2014) discusses the strong interest in Bitcoin on Iceland.

[27] As of late July 2015, one Auroracoin is worth a little over 3¢.

assurance that Icelanders would be able to sell their coins tomorrow at any price close to today's price. If enough Icelanders believed the coins might soon become worthless, they would quickly try to get rid of them. So in accord with Gresham's law, it appeared that the inhabitants decided to spend the mined coins near the peak rather than wait.[28]

Could the problems that Auroracoin encountered be overcome? A more successful initial strategy for phasing in a virtual currency might have placed a floor on the dollar price of the currency—to support it long enough for residents to became comfortable with it. No doubt, finding such a price might be difficult. Still, when the Krona has been so haphazardly managed for so long, it might be worthwhile to pursue something else. If Auroracoin is not the answer, one might imagine something less radical, such as a floating peg to basket of Scandinavian currencies or the Euro.

## 4 The Relative Stability of Bitcoin as a Store of Value

We examine raw market prices to evaluate whether Bitcoin (BTC) has the requisite stability to be considered a "reliable" store of value. Compared to fiat currencies, Bitcoin's ability to be immune from the ravages of inflation is a big plus in some states of the world. On the other hand, the considerable operational instabilities on Bitcoin exchanges undoubtedly have put a damper on Bitcoin's overall acceptance rate for many newcomers.[29]

Given gold's historical role in backing currencies, it is convenient to compare BTC with gold. Both are scarce commodities. Historically gold has been a popular alternative to fiat monies because of the inherent difficulty in extracting more ore.

Bitcoin catapulted onto the world's stage when one Bitcoin exceeded the price of an ounce of gold. Given the increasing costs of extracting either gold or mining Bitcoin, it is useful to compare the prices of the two mined "commodities." Thus, we will compare BTC with the exchange-traded fund, GLD, which accurately tracks the spot price of gold. For concreteness we will focus on the recent period from April 1st 2013 to March 31st 2015. This period captures the mini BTC price bubble provoked by the European bail-in scheme for Cyprus as well as the dramatic

[28] This possibility was anticipated by Margeirsson (2014).

[29] We believe Bitcoin's strength lies in the absence of any central authority of any kind. Ironically, this decentralized structure has also arguably been its Achilles' heel, as Moore and Christin have chronicled in their study of continuing problems plaguing a number of exchanges (Moore and Christin 2013). Well before Mt. Gox's bankruptcy in 2014, they showed that nearly half of all Bitcoin exchanges had disappeared in the previous 3 years. We believe these are temporary problems reflecting the newness and complexity of the technology and the naiveté of the entrepreneurs who started exchanges. These failures are to some degree implicit in the volatility of market price quotes from Coinbase that we use in this study. But without further information, we are not able to break them out.

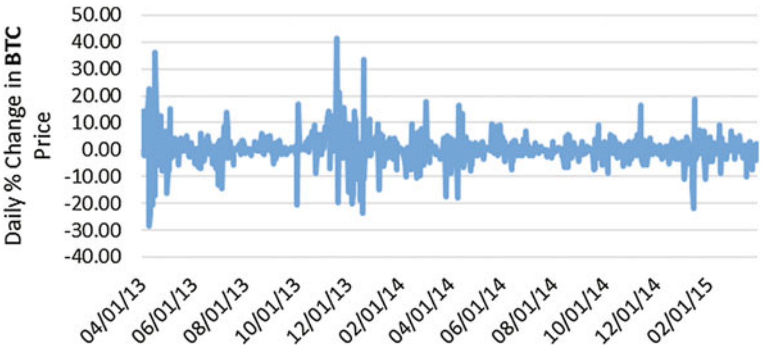


**Chart 8** Daily percentage change in the price of BTC

price changes induced by the vacillating policies toward Bitcoin by the Chinese authorities.

The latter bubble raises a red flag that BTC may be too volatile to gain critical mass as a viable private currency. Simply, if an asset is too volatile ex ante, a number of risk-averse investors will shy away from holding it as a store of value. As such, it may just not reach critical mass for acceptance as a viable private currency. Thus, the feature that makes Bitcoin an attractive inflation hedge—the strict limit of only 21 million coins that will ever be created— could be counterbalanced by excessive period-to-period price volatility. However, such a conclusion appears premature. Over time, BTC has actually become somewhat less volatile and, arguably, is gradually beginning to resemble other conventional inflation hedges such as gold.

To begin our volatility investigation, the simple daily percentage change in U.S. dollar price for both BTC and GLD are calculated and then plotted in Charts 8 and 9, respectively.

Not surprisingly, the daily percentage change in the price of BTC is more volatile than that of GLD. However, the daily percentage change in BTC appears to be diminishing over time, partially closing the volatility gap between the two assets. Chart 8 illustrates that throughout most of 2014 and 2015 the huge daily price movements of 30 % or greater that existed in 2013 vanished. So, it suggests that the daily price volatility of BTC may be diminishing. On the other hand, Chart 9 indicates the daily percentage change in price for gold remains quite stable. Except for a few spikes, it is rare to see a daily gold price move that exceeds 5 percent.

Digging a little deeper into the data, we compute the monthly Relative Standard Deviations (RSD) of the prices for both series. Namely, the monthly RSD are calculated as follows:

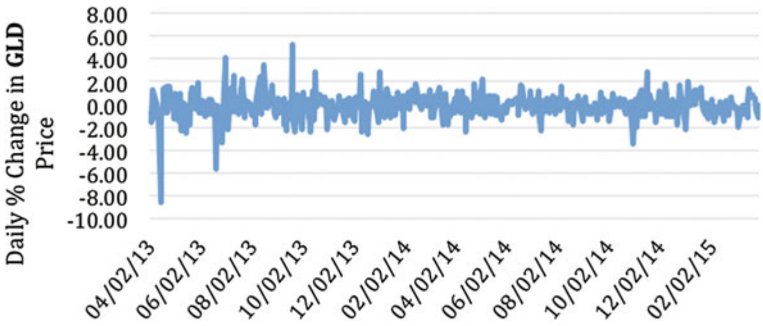


**Chart 9** Daily percentage change in the price of GLD

$$\sigma = \sqrt{\frac{(x-\mu)^2}{N}}$$

$$\frac{\sigma}{\mu}(\mathbf{100}) = RSD\,\%$$

Next we plot the 3 month moving averages of these RSDs. Then, using Excel we simply superimpose trend lines through the 3 month moving averages. BTC's results are illustrated on Chart 10.

This crude analysis, depicted in Chart 10 for BTC, demonstrates that the price volatility in BTC is falling by approximately 40 basis points a month. If this trend were to continue, BTC price volatility would be comparable to that of GLD within a year.

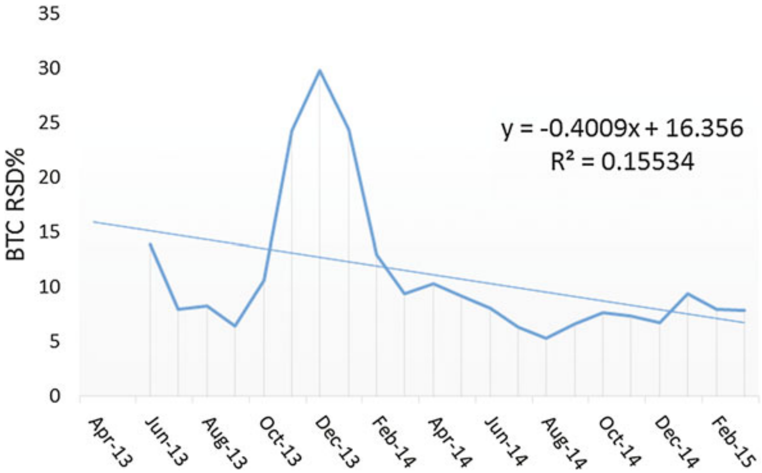


**Chart 10** BTC's Monthly RSD 3 Month moving average from 4/1/2013 to 3/31/2015

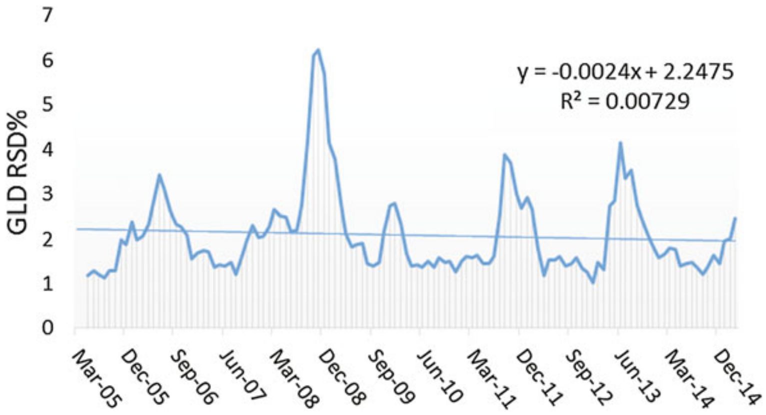


**Chart 11** GLD's Monthly RSD 3 Month moving average from 3/1/2005 to 3/31/2015

Since March 2005, we can extract data on the exchange-traded fund, GLD. We will use this 121 months of data to examine the stability of GLD, Chart 11. The trend line in Chart 11 is almost horizontal suggesting that volatility of GLD is stable. This simple analysis suggests two things: First, the price volatility of gold is stable. And secondly, the price volatility in BTC is falling. If this latter trend continues, the likelihood that BTC can be used as a store of value will increase.

Most U.S. $100 s are held outside the country, many in two countries with uneven monetary histories, Argentina and Russia; see (Treasury 2006). From that perspective, it is fitting to then compare BTC with the Argentinian Peso (ARS) and the Russian Ruble (RUB).

The exchange rate data used in the analyses are the United States Dollar to the Argentinian Peso (USD/ARS), and the United States Dollar to the Russian Ruble (USD/RUB). In parallel fashion to the comparison made earlier between BTC and GLD, we next consider the monthly *RSD%* of both USD/ARS and USD/RUB and plot the 3 month moving averages of these in Charts 12 and 13 with OLS trend lines superimposed through the averages.

The three (3) month moving average line (illustrated in Chart 12) shows a volatility spike in the Argentinian Peso. The 3 month moving average peaked in January of 2014. Since that spike, the moving average line of the RSD is below where it was before the volatility spike. Thus, because the spike occurred before the midpoint of the time series, it is not surprising the OLS linear trend line slopes downward somewhat.

Chart 13 illustrates that later during this time period, the Russian Ruble also experienced a volatility spike, which appears to have lasted longer. As the chart illustrates, the three (3) month moving average line peaks in February of 2015.

Volatility of the rubble, measured by the 3 month moving average of the RSD, is rising. According to the very crude linear OLS estimates, it is raising approximately 16 basis points a month.

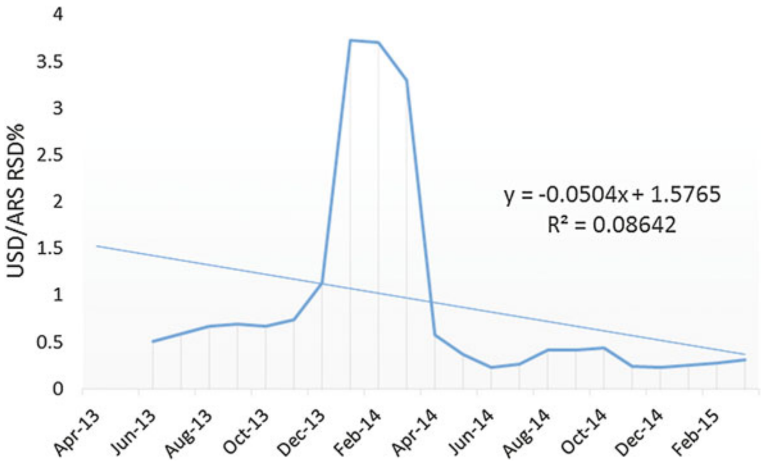


**Chart 12** USD/ARS Monthly RSD 3 Month moving average from 4/1/2013 to 3/31/2015

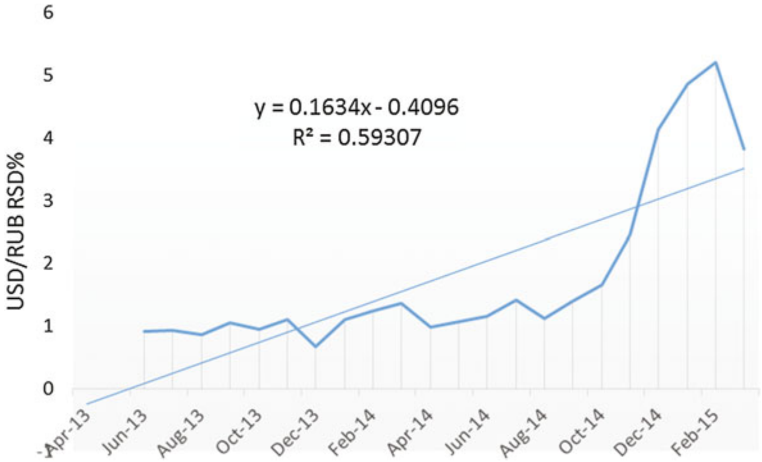


**Chart 13** USD/RUB Monthly RSD 3 Month moving average from 4/1/2013 to 3/31/2015

Obviously, it may not be sensible to imagine that such linear forecasts would necessarily continue very long. But, what is interesting is that for a number of reasons (beyond the scope of this chapter), volatility in these currencies appears to change rather abruptly. Volatility is increasing in certain periods, while moving in the opposite directions at other times. Yet, the conventional wisdom holds that fiat currencies are acceptable stores of value. While that proposition is generally true, it surely does not hold for currencies that have repeatedly experienced high bouts of self-inflicted inflation such as Russia and Argentina; historically these currencies have been prime candidates for using alternative store of values, such as the U.S.

dollar, and conceivably Bitcoin some day.[30] The data used in this chapter suggest BTC's volatility, which has often been viewed as problematical, is not that different than that from some national currencies.

### *4.1 Return on Investment*

In order for BTC or any other MBCs to gain critical mass, they must also retain their value over the long haul. This capability has been one of gold's talking point since Nixon closed the gold window. Extreme price movements of cryptocurrencies clearly limit such capability. However, if, as we have shown, Bitcoin volatility continues to decline, it could become a more viable store of value and gain considerable more adherents. And, since private currencies are networked goods, it might gather a more significant foothold and elongate the underlying trend depicted in Chart 10.

But volatility is not the only characteristic that brands money as a viable store of value. Return on investment is also important. Of the four assets we have been considering, BTC had the highest return on investment delivered by the four assets: Bitcoin (BTC), Gold (GLD), the Argentinian Peso (USD/ARS), and the Russian Ruble (USD/RUB) during the period under investigation from 4/1/2013 to 3/31/2015. In fact, BTC was the only asset that increased in value over the specified time period. In spite of its huge price spike and collapse, BTC still returned +137.36 % to investors during this period.

## 5 P2P Lending with Bitcoin

Here we consider the prospects of a paradigm shift in lending arrangements based on Bitcoin technology. Using Bitcoin lowers the transaction costs of setting up lending arrangements and reduces financial frictions. In consequence, it opens up lending opportunities to many of the world's unbanked that have been unable to tap into traditional banking arrangements.

As commerce evolves from analog to digital, lending arrangements tend to follow suit. This evolution is visible in the growth of person-to-person (P2P) on-line lending. According to the Federal Reserve Bank of Cleveland, such P2P lending has experienced rapid growth averaging 84 % a quarter since 2007:Q2, during which traditional consumer finance loans have declined by about half.[31]

[30] There is growing interest in Argentina in Bitcoin, see http://www.nytimes.com/2015/05/03/magazine/how-bitcoin-is-disrupting-argentinas-economy.html?_r=0.

[31] http://www.cutimes.com/2014/08/14/peer-to-peer-lending-poised-for-more-growth-fed.

During this period, two new U.S. firms, LendingClub and Prosper, grew to become industry leaders in P2P lending. They opportunely entered the scene just as the financial crisis was unfolding. The crisis handcuffed commercial banks, which had to restore their balance sheets—to raise equity and pay down TARP loans—to be in a position to mitigate against further shocks as the crisis continued to deepen. So the crisis itself shielded these new P2P lenders from facing commercial bank competition during their startup period. As a consequence, they experienced compound double-digit annual growth by exploiting the Internet to connect to participants at a low cost.

The LendingClub founder, Renaud Laplanche, thought that credit card companies charged extortionate interest to their consumers on unpaid balances. Given the minuscule rate of interest earned on bank deposits then, he also thought that the very wide spread signaled an opportunity, and LendingClub seized it.[32] Remarkably, since its inception in 2006, over $9 billion of loans have been funded on their platform.[33] These loans not only have a lower interest rate than comparable loans made by traditional banks, but they also pay a higher interest rate than banks. Thus, the overall spread between borrowing and lending rates narrows, resulting in a win-win situation for both borrowers and lenders.

LendingClub's main competitor has been Prosper Lending LLC.[34] Like LendingClub, its loan origination growth rate has been fairly impressive. Since its inception in 2006, over $3 billion has been borrowed on Prosper's platform with growth recently accelerating.[35]

These firms profit by using P2P technology to bring down interest rate spreads. The Internet allows these firms to match borrowers and investors without having to build branches and staff them.

Another advantage the P2P model has over traditional bank lending models is that it removes the need for deposit insurance and the associated heightened regulation to curb risk-taking by profit-seeking banks. In contrast, the only risk in an individual P2P loan stems from the full or partial default by an individual borrower. Moreover, the resulting loss is confined just to the individual investor. So if the loans are statistically independent and based on comprehensive credit scoring model, the losses can be correctly evaluated *ex ante* and bounded. When individual losses occur, as they undoubtedly will, the individual lender loses but there is no externality. There are no cascading losses across suites of lenders, which occur in classic banking lending crises, as cumulative borrower defaults eventual lead to a chain of bank failures.

[32] http://www.economist.com/blogs/schumpeter/2013/01/lending-club.

[33] https://www.lendingclub.com/info/statistics.action.

[34] http://www.lendstats.com.

[35] https://www.prosper.com/.

While P2P lending mechanisms represent definite improvements, the change does not represent that much of a real paradigm shift in lending. Like Uber and Airbnb, these two P2P lenders still have a top-down organizational structure. One could imagine a more radical structure based on more decentralized lending arrangements, similar to the P2P relationships in the Bitcoin environment.

Still, lending conceptually entails a more complicated set of relationships than payments. If I have good Bitcoin funds, I can readily send them to you on the Internet more or less immediately as a gift or in return for a good or service.

But in a lending relationship there are more complicated sets of reciprocal relationships. Lending generally entails somewhat longer horizons than payments. Banks monitor the behavior of loan recipients and collect collateral when loans default. Addressing these issues goes beyond our understanding. It is not apparent to us how these capabilities can be mimicked even within emerging Blockchain extensions enumerated by Swan (2015).

Currently, financial systems are constrained by borders and governments. As a result, they remain “centralized”, just like banking systems have been for the last 500 years. In these centralized systems, an outer hierarchical authority mediates trust. As a result of this dependence on authority, peers may have relatively little incentive to challenge the authority by searching for other alternative arrangements. The fixed costs of change just loom too large.

Still one can push in the direction of more decentralized peer-to-peer trust-based lending arrangements. And, this is just the type of trust that may be the crucial ingredient needed to enable a true paradigm shift in lending and borrowing. Interestingly, digital currencies may be the needed ingredient to move toward a more decentralized lending and borrowing environment. That is, the new market for P2P lending and borrowing based explicitly on Bitcoin represents a large step toward full decentralization.

This concept is almost brand new with relatively few, small players thus far, BTCJam, Bitbond, and Bit Lending Club. These lenders operate much like, LendingClub, and Prosper, but instead of basing decision in terms of USD, they use Bitcoin. They have online platforms, serve as intermediaries between lenders and borrowers, and charge closing costs.

The difference is that they are one step closer to a P2P network where trust has been decentralized. How? These firms have developed networks, which are backed by Bitcoin only! No traditional fiat currencies are used on these networks, only the cryptocurrency Bitcoin. Since BTCJam has the largest market share in the “P2P lending with BTC” space, we will concentrate on it for our discussion.

In just over a 2 year history, BTCJam has been the intermediary for over 52,000 BTCs.[36] Since only BTC backs loans on this network, the dollar equivalent of the BTCJam loans since inception requires more detailed information than we have

[36] https://btcjam.com.

available.[37] However, to give a sense of the amounts, BTCJam has been the intermediary for roughly $15 million of loans. For a start-up company, operating in completely uncharted waters, these numbers are noteworthy. If the company were to continue at such rapid rates, one can easily extrapolate that it could post comparable numbers to LendingClub and Prosper over a decade.

Perhaps the most impressive part of BTCJam's lending experience is the breadth of its reach: It has serviced 16,342 loans in 121 countries with many of the loans in areas normally considered to be "unbanked". Thus, a sizable majority of the earth's population, which remains unbanked, could be potential customers for this new BTC lending technology. The growth possibilities would seem to be extraordinary.

The transnational scope of Bitcoin is what is impressive with BTCJam being the first P2P lending platform to cross national borders successfully.[38] Using BTC as the backbone for the network, BTCJam (and the other firms in this space) are breaking down the national borders, which characterize the centralized financial system that's been prevalent up until now.

As a result of such lending, one might expect such P2P lending firms to enable smaller-sized loans. Under traditional centralized lending arrangements, it's often unprofitable to launch a financial business in many areas of the world that are mostly rural and quite poor—the preconditions for remaining unbanked. But, in theory, the size of the loan is irrelevant to BTCJam. The majority of their costs are fixed, namely maintaining and developing the platform. They only collect a closing cost, which is a percentage of the loan amount. So, these lenders have a strong incentive to spread their fixed costs and close as many loans as possible, which allows them to accommodate small and short duration loans.

In fact, the data is quite consistent with this description. During its first year of operation, the average size of a BTCJam loan was approximately $400 to $600. Prosper, on the other hand, had an average loan size about ten times larger, $4,800 during its first year in business.[39]

Firms like BTCJam are nudging finance away from the traditional structures involving pyramidal central controls, toward those based on the decentralization of trust. The products being lent are BTCs. The Bitcoin Blockchain is completely open sourced and decentralized, and if authorities permit this to continue to develop, the possibilities are vast. Using this BTC Blockchain technology, one can imagine a true paradigm shift in finance: an environment where the role of profit-seeking intermediaries is reduced, and the need for any central authority is significantly diminished. As in all lending, there is no guarantee that investors will be repaid. But unlike bank lending, there is no deposit insurance overhang. But failures hit individual investors and not large banks supported by deposit insurance and a government backstop. Moreover, the possibility of repeat lending arrangements for

[37] The problem is that the price of Bitcoin fluctuates at a relatively high frequency, and the chart only gives the results on a monthly average basis.

[38] http://www.netbanker.com/p2p_lending/.

[39] http://www.netbanker.com/2013/11/btcjam_p2p_lending_via_bitcoin.html.

successful borrowers can buoy the returns, particularly when the alternative arrangements are unattractive.

## 6 Conclusions

Satoshi Nakamoto's creation of the Bitcoin Blockchain has opened up several new avenues for monetary exploration beyond the traditional realm of the nation state. There was a huge "gold rush" like movement toward Bitcoin and other new math-based currencies in 2013. This swoon began with the European imposition of a bail-in tax on Cypriot deposits at two large banks. It exploded as the Chinese jumped on the bandwagon but then receded amidst growing regulatory pushbacks in China and elsewhere.

Without doubt, the creation of the Blockchain is generating whole new ways of thinking about organizing activities through decentralized trust mechanisms rather than traditional centralized approaches. Andreas Antonopoulos has emphasized this theme in Antonopoulos (2014). Indeed, IBM has been exploring the Blockchain to organize the Internet of Things (Higgins 2015).

Suffice it to say that the nation state's monopoly on money design and implementation is under assault by a myriad of developments. These innovations raise the possibility that math-based currencies could more securely and cheaply connect the world.

We have shown that an entirely new lending mechanism like BTCJam has brought P2P lending opportunities to poorer parts of the world. Previously, such opportunities have only been available to residents of advanced countries in the form of P2P lending organizations such as Lending Club. These innovations have opened the door to Bitcoin lending on a scale that was unimaginable a decade ago. The poor of the earth who remain unbanked now have access to first-world lending possibilities.

The pace at which these advances will effectively reorder nation state monetary design is unclear. The invention of the Blockchain is upsetting enough traditional payment means and opening up the possibility of a different kind of monetary order harkening back, perhaps, to an earlier period when money was more private.

Finally, the current worldwide crisis in which traditional monetary policy is virtually impotent at the zero bound of interest rates raises some questions about how to proceed.[40] Reworking regulation and monetary policy to accommodate the manifold opportunities spawned by the Bitcoin Blockchain revolution will be neither easy nor straightforward. But clearly the time has come to reconsider how we pay, and bank in an ever more tightly coupled world in which distance is receding, and the far edges may affect us at any moment.

[40] Also, see http://www.bankofengland.co.uk/publications/Pages/speeches/2015/840.aspx.

## References

Antonopoulos, A.M.: Mastering Bitcoin. O'Reilly (2014)

Bagus, P., Howden, D.: Deep Freeze: Iceland's Economic Collapse. Ludwig Von Mises Institute (2011)

Banegas, A., Judson, R., Sims, C., Stebunovs, V.: Local and Global Determinants of International Demand for U.S. Banknotes. Bundesbank (2014)

Blanchard III, J.U., Hayek, F.A.: Exclusive Interview with F.A. Hayek. Cato Policy report (1984)

Boyes, R.: Meltdown Iceland: Lessons on the world financial crisis from a small bankrupt island. Bloomsbury, New York, NY (2009)

Cameraa, G., Casarid, M., Bigonid, M.: Money and trust among strangers. In: Proceedings of the National Academy of Sciences, pp. 4889–4893, 10 Sept 2013

Chakravorti, B., Mazott, B.D.: The Cost of Cash in the United States. Tufts Fletcher School (2013)

Champagne, P.: The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. E53 (2014)

Cohen, B.: The Geography of Money. Cornell University Press (1998)

Curthbertson, A.: Bitcoin now accepted by 100,000 Merchants. In: International Business Times, 4 Feb 2015

Erb, C.B., Harvey, C.R.: The Golden Dilemma. Finance, Duke University (2013)

Fischer, S.: Friedman versus hayek on private money: review essay. J. Monetary Econ. **17**, 433–439 (1986)

Greenspan, A.: Opening Remarks. In: Maintaining Financial Stability in a Global Economy A symposium sponsored by the Federal Reserve Bank of Kansas City. Federal Reserve Bank of Kansas City (1997)

Gudmundsson, M., Thorgeirsson, T.: The Fault Lines in Cross-Border Banking: Lessons from the Icelandic Case. In: Peter, E.G., Backé, P.H. (eds.) Contaigon and Spillovers: New Insights from the Crisis. Larcier (2010)

Guidotti, P., Rodriquez, C.A.: Dollarization in Latin America: Gresham's law in reverse? Staff Pap. (Int. Monetary Fund.) **39**(3), 518–544 (1992)

Hart, K.: Notes towards an anthropology of money. Kritikos **2**, 1552–5112 (2005)

Hayek,F.A.: The uses of 'Gresham's law' as an Illustration in Historical Theory **2**, 101–102 (1962)

Hayek, F.A.: Denationalisation of Money—The Argument Refined: An Analysis of the Theory and Practice of Concurrent Currencies, Third edn. The Insitute of Economic Affairs, London (1990)

Higgins, S.: IBM Reveals Proof of Concept for Blockchain-Powered Internet of Things. Coindesk, 17 Jan 2015

Jacobs, J.: Cites and the Wealth of Nations: Principles of Economic Life. Random House (1984)

Judson, R.A., Porter, R.D.: Estimating the Volume of Counterfeit U.S. Currency in Circulation Worldwide: Data and Extrapolation. J. Art Crime (2012)

Kambas, M., Grey, S.: Stelios Orphanides. Why did Cypriot banks keep buying Greek bonds? Reuters, 30 Apr 2013

Keynes, J.M.: *The* Economic Consequences of the Peace. Harcourt, Brace, and Howe (1919)

Keynes, J.M.: The General Theory of Employment, Interest, and Money. Palgrave McMillian (1961)

Knapp, G.F.: The State Theory of Money. Macmillan, London (1924)

Lamport, L., Shostok, R., Pease, M.: The Byzntine generals problem. ACM Trans. Programm. Lang. Syst. **4**(3), 382–401 (1982)

Lengwiler, Y.: A model of money counterfeits. J. Econ. 123–132 (1996)

Lerner, A.P.: Money as a creature of the state. American Economic Review: Papers and Proceedings, pp. 312–317, May 1947

Margeirsson, O.: Free cash for Iceland, but it pays to keep cool about Auroracoin. The Conversation, 11 Feb 2014

Menger, C.: On the origin of money. Econ. J. **2**, 239–255 (1892)

Moore, T., Christin, N.: Beware the middleman: empirical analysis of Bitcoin-exchange risk. In: Financial Cryptography and Data Security, pp. 25–33. Springer (2013)

Mundell, R.: Uses and abuses of Gresham's law in the history of money. Zagreb Journal of Economics **2**(2), 57–72 (1998)

Paolera, G.D., Taylor, A.M.: Straining at the Anchor: The Argentine Currency Board and the Search for Macroeconomic Stability, 1880–1935. Chicago University Press, Chicago (2001)

Peebles, G.: Inverting the panopticon: money and the nationalization of the future. Public Cult. **20** (2), 233–265 (2008)

Popper, N.:Digital Gold. Harper Collins (2015)

Porter, R.D., Judson, R.C.: The location of U.S. currency: how much is abroad? Bull. Fed. Res. Board, 883–903, Oct 1996

Rabinovitch, S.: China rides rollercoaster love affair with Bitcoin. Financ. Times, 22 Nov 2013

Ritter, G. Which Industries are Uber-Vulnerable for Cloud Disruption. Forbes, 13 Mar 2015

Samuelson, P.: An exact consumption-loan model with or without the social contrivance of money. J. Polit. Econ. 467–482 (1958)

Sargent, T., Velde, F.: The Big Problem of Small Change. Princenton University Press (2002)

Stalnaker, S.: Bitcoin, Ven and the End of Currency. http://techcrunch.com/2011/05/20/bitcoin-ven-and-the-end-of-currency/, 20 May 2011

Steil, B.: The end of national currency. Foreign Affairs (2007)

Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly, Sebastopol, CA (2015)

Treasury, U.S. The Use and Counterfeiting of United States Currency Abroad, Part 3 (2006)

Tasca, P.:Digital Currencies: Principles, Trends, Opportunities, and Risks. Bundesbank (2015)

## Author Biographies

**Dr. Richard Porter** is an empirical economist and the CEO of a payments consultancy specializing in virtual currencies such as Bitcoin. Porter was a 43 year veteran of the Federal Reserve System. He began his career at the Board in Washington D.C. in September 1971, while he was on a leave of absence from the Ohio State University. He conducted research and policy analysis for the Board for over three decades, finishing as a senior adviser in the Division of Monetary Affairs. He then served for a decade as a Vice President and Senior Policy Advisor for payments at the Chicago FRB. At the Bank, Porter oversaw economic research and policy analysis on payments systems, participated at a senior level in the FOMC monetary policy process and served as economics editor of the Bank's in-house research and policy journal. Prior to his Federal Reserve service, Porter was an Assistant Professor of Economics at Ohio State University and earlier obtained three degrees at the University of Wisconsin at Madison.

Porter has had an active research and policy career. He has published dozens of articles in several areas of empirical economics and statistics with concentrations in monetary and payment economics and finance. His most highly cited work on asset pricing has been cited over 1,000 times and reprinted four times. His major contribution to the analysis of money and inflation was featured on the front page of the *New York Times*.

He has published a variety of research and policy articles in a number of of leading scholarly journals. These include the *American Economic Review*, *Annals of Economic and Social Measurement*, *Brookings Papers on Economic Activity*, *Carnegie Rochester Conference on Public*

*Policy*, *Econometrica*, *Economic Letters*, *Economic Modelling*, the *Journal of Economics and Business*, the *Journal of Economic Dynamics and Control*, the *Journal of Monetary Economics*, the *Journal of Money, Credit and Banking,* and the *Journal of Payment Strategy and Systems.* He has also contributed to several Federal Reserve System Publications including the Federal Reserve *Bulletin* and the Chicago Federal Reserve Bank's *Economic Perspectives*.

**Dr. Wade Rousse** began his career at Maritime Logistics, where over a decade he worked his way to becoming a partner, and eventually led a successful undertaking to sell the company. Afterwards, Wade moved into the public sector and was on staff in the Financial Markets Group at the Federal Reserve Bank of Chicago. Currently, Dr. Rousse is an Executive in Residence for the W.A. Franke College of Business at Northern Arizona University.

# How Non-banks are Boosting Financial Inclusion and Remittance

**Diana C. Biggs**

**Abstract** This chapter explores financial inclusion and economic empowerment through non-bank alternatives to traditional financial services providers such as retail banks. Specifically, we will explore two technology-based solutions for money transfer and payments: 1) mobile money: the provision of financial services via mobile phone; and 2) applications of blockchain technology and digital currency in the remittance industry. The author notes that these technologies hold the potential to significantly reduce barriers to access to financial services for under-or unbanked populations given the right conditions: consumer adoption; availability of mobile and internet connectivity; and a favorable regulatory environment.

**Keywords** Bitcoin • blockchain • mobile • mobile money • remittance • financial inclusion • inclusive finance • unbanked

## 1 The Opportunity for Non-banks in Financial Inclusion and Remittance

According to the World Bank Global Findex (2014 data), two billion people—equating to 38 % of the world's adult population—do not use formal financial services (The World Bank Group 2015). For the most part, these are poor populations who are excluded from even the most basic financial services offerings, specifically the ability to spend, the ability to store, and the ability to invest. The World Bank research estimates that 73 % of poor people are unbanked because of costs, travel distances and the often burdensome requirements involved in opening a financial account (The World Bank Group 2015).

Financial inclusion, or inclusive financing, is the delivery of financial services at affordable costs to sections of disadvantaged and low-income segments of society (Wikipedia 2015). It is generally accepted that financial access is the gateway to edu-

D.C. Biggs (✉)
Centre for Blockchain Technologies, University College London, London, UK
e-mail: diana.biggs@gmail.com

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_10

cation, health, housing and other necessities to growth and development. In addition, access to financial services is critical for access to economic opportunity, increases productive investment and consumption, and contributes to women's empowerment.

Financial inclusion has today become a particular area of focus for non-bank financial services providers, given the under-servicing of those populations to date from traditional banks. These non-bank offerings include nonprofits and NGOs, community-based institutions and cooperatives, telecommunications providers, microfinance institutions, post offices and, in recent years, some financial technology (fintech) start-ups.

Remittances, the transfer of money by migrant workers to their home countries, exceed both official development assistance and foreign direct investment (excluding China) as a source of funds for developing countries (Cook and McKay 2015). With this scope, their benefits to the recipient economies are well recognized, including aiding in the reduction of poverty, enhancing entrepreneurship, access to formal financial services, communication and information technologies, and contributing to spending on health and education.

Overall financial inclusion and remittances have been areas of focus for the application of new technology, with the aim to leverage new tech in order to improve and enhance access to such services. This chapter will examine two technology-based solutions for providing financial access to populations left outside the sphere of traditional financial services offerings, first with an overview of mobile money and secondly an introduction to non-bank remittance solutions enabled by technology such as digital currency and the blockchain.

## 2 Mobile Banking: Overview

Mobile Banking can be defined as the provision and availment of banking and financial services with the use of mobile telecommunication devices. In the broadest sense, this may include facilities to send and receive payments and, when provided by a traditional financial services provider, to conduct bank and stock market transactions, administer accounts and to access customized information (Tiwari and Buse 2006).

The increasing interest in and proliferation of mobile banking offerings around the world has been driven by several factors, including:

- Increasing penetration of mobile phones in societies across the globe: GSMA Intelligence estimates that the total number of active SIM connections at end 2013 was 6.3 billion (GSMA 2014).
- Globalization and increasing availability of mobile services have moved it from a luxury item to what is broadly viewed as a necessity (Tiwari et al. 2007).
- 18–34 year olds increasingly favor new technologies to traditional services (Canning 2013).
- Rapid technological improvements in mobile devices and networks, including increased processing power, greater battery life and dramatically improved networking speeds.

While in Western markets banks and other financial services institutions see mobile offerings as an expansion of their services, this chapter will focus on the opportunity for mobile to provide financial services to under- and unbanked populations globally, particularly in developing markets.

## *2.1 Mobile Money*

To date, the majority of mobile banking offerings are centered around mobile money programs, which allow for mobile payments, such as bills or peer-to-peer transfers. Mobile money is already a fairly mature industry, with established offerings in the majority of emerging economies (GSMA 2015).

For the purposes of this chapter, we follow the definition of mobile money of the GSMA's Mobile for Development Mobile Money Programme's 2014 State of the Industry report. Mobile money services refer to offerings which do not require a user to be banked with any financial institution and whose network transaction points lie outside of traditional bank offerings, i.e. bank branches and ATMs. These services offer an interfaces available on basic mobile phones, rather than the need for a smartphone app. This definition does not include mobile banking services where mobile is simply a channel for accessing traditional banking services (GSMA 2015).

Mobile money, being value held within the mobile phone, are typically offerings of either the Mobile Network Operators (MNOs), such as Airtel with Airtel Money or Safaricom with M-Pesa, or a collaboration between an MNO and a bank. In certain countries, these services fall under the regulatory oversight of the financial services regulatory and may require licensing.

### 2.1.1 Usage and Availability of Mobile Money

As of 2014, there were 255 mobile money services available across 89 countries worldwide, covering over 60 % of developing markets, according to the GSMA. In terms of adoption, there were 299 million registered mobile money accounts as of December 2014, which represents 8 % of mobile connections in the markets offering mobile money services, (GSMA 2015) indicating a strong growth opportunity for the usage of these services.

Geographically, usage of mobile money in Sub-Saharan Africa (SSA) surpasses other regions, accounting for 53 % of live services globally as of December 2014 (GSMA 2015). The World Bank Group's Global Financial Inclusion Report 2014 found that 12 % of adults in SSA reported having a mobile money account. Of this, half had both a mobile money account and an account at a financial institution, and half a mobile money account only. At 58 %, Kenya holds the highest share of adults with a mobile money account, followed by Somalia, Tanzania, and Uganda with approximately 35 % (Demirguc-Kunt et al. 2015).

In other regions, usage of mobile money remained much lower, with only three percent of adults with a mobile money account in South Asia, 2% in Latin America and the Caribbean, and less than one percent in all other regions (Demirguc-Kunt et al. 2015).

### 2.1.2 Mobile Money Applications

Mobile money services allow the digital storage of funds within a mobile-based account, which can then be used for a variety of goods and services including bill payment, mobile top-up of pre-paid accounts, peer-to-peer transfer, bulk disbursements (i.e. employee payments), merchant payments and receipt of international remittance. At present, domestic peer-to-peer (P2P) transfers and airtime top-ups remain the most common product offerings amongst mobile money service providers.

The majority of mobile money services remain cash-based in some way, for example the cashing out of remittances received from abroad via mobile money, or cash-in funding of accounts. For this, providers rely on physical access points, which are predominantly agent-based networks. At the end of December 2014, there were 2.3 million mobile money agent locations globally, an increase of 45.8 % from the previous year. Using bank branch data available from the IMF Financial Access Survey (FAS) Database, this indicates that mobile money agent outlets outnumber bank branches in 75 % of the 89 markets where mobile money is available today (GSMA 2015). In addition to agent networks, microfinance institutions, ATMs, bank branches, postal offices and even petrol stations also serve as access points for mobile money across various regions.

### 2.1.3 Benefits of Mobile Money

Mobile money brings several advantages both to the customer and the service provider:

- Improved efficiencies: increased speed of payments and lower costs to send and receive over traditional methods;
- Enhanced security, monitoring, and transparency, reducing opportunity for crime and fraud;
- Allows for broader geographical coverage, removing physical barriers and reducing time away from work and home to travel to a brick and mortar financial institution;
- Serves as a convenient initial entry point into the formal financial system (Demirguc-Kunt et al. 2015), both by the introduction of such services to customers via the mobile phone and in the collection of user data it allows, which can then be applied to functions such as credit-scoring.

As of 2014, in 16 countries around the world the number of mobile money accounts outnumbered the number of bank accounts (GSMA 2015). This is one indication of how mobile money promotes financial inclusion. With the convenience and increasing accessibility of mobile phones, and the behavioural familiarity of topping up a mobile phone via local agents, mobile money serves as an enabling gateway to the access of financial services.

## 2.2 Other Mobile Financial Services Offerings

**Mobile insurance**: Mobile insurance uses the mobile phone to provide microinsurance services to the underserved. The service must allow subscribers to manage risks by providing a guarantee of compensation for specified loss, damage, illness, or death.

**Mobile savings**: Mobile savings providers provide savings offerings via mobile phone. These services allow subscribers to save money in an account that provides principal security, and, in some cases, an interest rate.

**Mobile credit**: Mobile credit providers provide users with credit offerings via mobile phone. The service allow subscribers to borrow a certain amount of money that they agree to repay within a specified period of time, at an agreed amount of interest and/or fees.

**Case study: M-Shwari**

M-Shwari is a paperless banking service available in Kenya, offered through Safaricom's mobile money transfer service, M-PESA. M-Shwari offers both savings and loan products and was launched via a partnership between Safaricom and the Commercial Bank of Africa (CBA). Building off the success of M-PESA as a mobile money service in Kenya, M-Shwari extends this offering into savings and credit providing the benefits of traditional banking products, including interest on deposits, deposit insurance and access to credit to unbanked populations. For their credit offering, M-Shwari were the first large-scale loan provider to leverage data from mobile usage to provide input into credit decisions, by creating an initial credit score (Cook and McKay 2015). This use of mobile data for credit-scoring decisions is increasingly being looked at by traditional banks, credit card companies and social entrepreneurs as a means to facilitate credit offerings to previously underserved populations, who lack the necessary data for existing credit score methods.

## 2.3 New Models in Remittance

Remittances refer to earnings in the form of either cash or goods sent by migrant or overseas workers to support their families back home. The number of international migrants living outside their country of origin was an estimated 247 million in 2013 and is expected to exceed 250 million in 2015 (World Bank 2015). Money sent home by migrants now represents one of the largest foreign income inflows to developing countries and in recent years have been rising steadily, although this growth has recently slowed due to factors including the economic slowdown in Europe and the impact of declining oil prices on the Russian economy (World Bank 2015).

The majority of remittance money, circa 80–90 %, is spent on basic necessities including food, clothing, shelter, health care and education, (IFAD Remittance Factsheet 2009) thus playing a strong role in poverty reduction.

**Table 1** Estimates and projections for remittance flows to developing countries (USD BN) (World Bank 2015)

| Region | 2013 | 2014f | 2015f | 2016f |
|---|---|---|---|---|
| Developing countries | **418** | **436** | **440** | **459** |
| East Asia & Pacific | 113 | 122 | 125 | 130 |
| Europe & Central Asia | 52 | 48 | 42 | 45 |
| Latin America & Caribbean | 61 | 64 | 66 | 69 |
| Middle East & North Africa | 49 | 53 | 53 | 55 |
| South Asia | 111 | 116 | 120 | 126 |
| Sub-Saharan Africa | 32 | 33 | 33 | 34 |
| **Globally** | **557** | **583** | **586** | **610** |

According to the latest World Bank estimates, global remittance receipts, including by both developing and high-income countries, are estimated at $583 billion in 2014 and could rise to $586 billion in 2015 and $636 billion in 2017 (World Bank 2015). Top recipient countries in 2014 were India, China, Philippines and Mexico.

## 2.4 *Remittance Process*

The typical process for a remittance transaction involves three steps:

1. **On-boarding of value**: The sender pays the remittance to a remittance provider in their country of residence using cash, check, money order, credit card, or debit card, typically in-person but also a website, email or by phone.
2. **Facilitation of value transfer**: The remittance provider then facilitates the transfer of the value, informing the local counterparty of the amount to be transferred, the recipient details, and the selected method of payout.
3. **Off-boarding of value**: The local agent, for example a local bank or agent network, makes the payment to the recipient.

In the majority of cases, settlement is conducted between the sending and paying agents periodically, as agreed between the parties, through a commercial bank (Ratha 2012).

## 2.5 *Costs of Remittances*

The global average cost of sending $200 was 7.7 % in the first quarter of 2015, with a weighted average cost (by size of bilateral remittance flows) of 6 %, indicating lower costs in higher volume corridors (World Bank 2015).

**Table 2** Total avg. remittance cost by region of the world (World Bank 2015)

| Region | Q1 2013 | Q2 2013 | Q3 2013 | Q4 2013 | Q1 2014 | Q2 2014 | Q3 2014 | Q4 2014 | Q1 2015 | Q2 2015 |
|---|---|---|---|---|---|---|---|---|---|---|
| East Asia & Pacific | 8.97 | 8.88 | 9.00 | 8.28 | 8.52 | 8.38 | 7.92 | 8.12 | 8.13 | 8.11 |
| Europe & Central Asia | 6.77 | 6.70 | 6.68 | 6.29 | 6.49 | 6.35 | 6.17 | 6.22 | 6.11 | 6.02 |
| Europe & Central Asia excluding Russia | 8.43 | 8.35 | 8.41 | 7.93 | 8.18 | 7.92 | 7.67 | 7.54 | 7.20 | 7.18 |
| Latin America & Caribbean | 7.77 | 7.28 | 7.26 | 7.02 | 6.21 | 5.57 | 6.02 | 6.03 | 6.14 | 6.78 |
| Middle East & North Africa | 7.81 | 7.83 | 7.61 | 7.80 | 8.32 | 8.29 | 8.25 | 8.63 | 8.41 | 8.21 |
| South Asia | 7.16 | 7.02 | 7.12 | 6.58 | 6.56 | 6.45 | 5.97 | 5.94 | 5.96 | 5.74 |
| Sub-Saharan Africa | 12.2 | 12.1 | 12.3 | 12.6 | 11.7 | 11.6 | 11.3 | 11.5 | 10.2 | 9.74 |
| Global | 9.05 | 8.88 | 8.93 | 8.58 | 8.36 | 8.14 | 7.90 | 7.99 | 7.72 | 7.68 |

With the estimated total global remittances of $586 billion for 2015 (World Bank 2015), at the current weighted average cost of 6 %, this would mean approximately $35 billion in fees. These fees can occur at the sender side both as an upfront fee as well as a currency-conversion fee typically held within the exchange rate. Smaller money transfer operators may also charge a fee to the recipient upon collection).

As seen on the chart above, Sub-Saharan Africa remains the most expensive region to send remittances to, at 9.74 % at Q2 2015, and the South Asia region the least expensive at 5.74 %.

Remittance costs have been declining over time, partly due to advancements in technology which help to drive down costs, as well as increasing competition.

## 2.6 *Mobile Money in Remittance*

Domestic peer-to-peer remittances are recognized as an opportunity by mobile network operators (MNOs) to leverage their platforms and distribution networks to capture international remittance flows. The majority of mobile money international remittance service offerings on the market cater to ‘North-South’ flows, in which money is onboarded in a developed market and sent to the mobile wallet of a recipient in a developing market. According to the GSMA, there are over 60 partnerships between mobile money operators (MMOs) and money transfer organisations (MTOs) (Scharwatt and Williamson 2015). Globally recognized MTOs include Western Union, WorldRemit, Ria and MoneyGram.

International remittances via mobile money increased significantly in 2014 alone, as the market opened up both due to favorable commercial opportunities, such as the opportunity for cost reduction via mobile and digital technologies, and the removal of regulatory barriers in certain geographies.

In most instances, senders submit their payment at a physical agent in their local market, although online channels are increasing in use. These partnerships, however, have yet to gain significant traction as a remittance channel. At the end of 2014, only 164,000 cash-to-wallet and web-to-wallet international transfers were received monthly in mobile money accounts globally, according to GMSA estimates (Scharwatt and Williamson 2015).

In addition to North-South flows, MNOs are beginning to realize the importance of South-South flows, namely intra-African remittance. This can be accomplished via creating interoperability between country mobile money systems. At present, only four countries globally—Indonesia, Tanzania, Sri Lanka, Pakistan—have launched domestic interoperability between mobile money providers (GSMA 2015).

## *2.7 Bitcoin Remittance*

Proponents of the digital currency space have been optimistic about the potential for bitcoin, as a means of cross-border value transfer, to transform the remittances industry.

In the remittance use case, sending money across long distances, borders, or even across the world, bitcoin and blockchain technology offers potential benefits across the value chain over existing money transfer solutions.

As a decentralized peer-to-peer system, the bitcoin blockchain is able to replace traditional financial services providers for the transfer of value, leveraging a global network of actors, called "nodes" which serve to process and confirm the transactions 24 h a day, seven days a week. These transfer values through the system are done in real-time, currently with a typical transaction confirmation time of 10 minutes. The system is essentially "trustless", as no central authority has power over the network, and transactions are publically and immutably recorded on a digital ledger, the blockchain itself. All of this happens at near zero-cost, at typically only 0.0001 bitcoin (BTC) per transaction (Bitcoin Wiki 2015).

These properties represent significant efficiencies and cost-savings over traditional methods of value transfer led by financial services institutions, by the nature of the technology itself as well as the removal of slow and costly third parties.

### 2.7.1 Flow of Funds in Bitcoin Remittance

There are three options for the operational flow of funds in bitcoin remittance solutions:

1. Bitcoin-only onboarding and offboarding
2. Bitcoin-only onboarding and both fiat and bitcoin offboarding
3. Onboarding and offboarding in both fiat and bitcoin

In each of these cases, the bitcoin blockchain is used for the intermediary transfer of value and in options 2 and 3 the service provider, either at one or both ends of the value chain, is responsible for the conversion of fiat to bitcoin.

On the sender side, in each option the sender typically has the option to send value directly as bitcoin, using their own bitcoin holdings as purchased at a bitcoin exchange, ATM or through an individual seller.

In option 3, the remittance service provider accepts another form of payment, i.e. via credit or debit card payment, bank transfer, or cash. The service provider then uses that payment to purchase an equivalent amount of bitcoin from their bitcoin exchange of choice.

The bitcoin is then sent to the recipient for offboarding, handled either via the service's local entity, a local partner, or received directly as bitcoin.

Integrations between sending and receiving channels are typically done via API calls between the systems involved.

While an informed public are growing increasingly aware of bitcoin, its use as a currency and payment method remains relatively limited. As well, for users of remittance solutions, trust is typically a paramount factor in selecting a provider, and bitcoin's at times negative image in the press may be a deterrent from services which are outwardly promoting its integration. Therefore, for reasons of brand, utility and adoption, an increasing number of service providers are using the bitcoin blockchain merely as the rails upon which value is sent and working with partners, including traditional payment methods and value stores, for on- and offboarding.

### 2.7.2 Commercial Model

Traditional providers argue that the high costs of existing remittance offerings are not simply imposed by the market out of greed or legacy transfer systems, but rather are predominantly due to costs relating to the regulation and compliance imposed on the industry by governments and financial regulating bodies. Others attribute some of this cost to the operational costs associated with the on and offboarding of value in developing markets, where infrastructure and servicing may be limited.

The majority, if not all, bitcoin remittance solution providers subject themselves to the same, if not greater, Know Your Customer (KYC) and Anti-Money Laundering (AML) KYC and AML policy requirements as financial institutions. This is necessary both as a requirement by their own financial institutions servicing them as a company, as well as a pre-emptive move should regulatory bodies in the countries in which they operate require it in the future. Therefore, they are also subject to the costs of compliance, albeit they may be more likely to look to and benefit from new fintech solutions in the area of compliance management, which may also reduce costs and increase efficiency.

Looking across the value chain, the majority of bitcoin-based remittance solutions utilize a web-based platform for the onboarding of value. This online workflow keeps costs low while also enabling broader geographical coverage and 24/7 services. Depending on the provide, the sender may be required to pay an upfront fee or to purchase the currency at a rate with some markup to provide revenue to the service provider, which may vary as per the selected method of offboarding.

The majority of the cost-savings and efficiencies of bitcoin-based remittance solutions comes in using the blockchain as the international payments engine facilitating the value transfer across geographies. This eliminates the need for banks to serve as intermediaries, which both slows timings and increases costs. The value can reach the destination country within a typical transaction time of 10 mintues.

Once received by the recipient operations, the bitcoin value is typically sold as quickly as possible, given the ongoing volatility of the bitcoin price, to lock in the value of the transfer. This is also frequently the source of revenue for the provider, benefiting from gains in the foreign exchange transactions. The local sale of bitcoin also provides the necessary liquidity for the offboarding. Therefore, for this model to work, a bitcoin exchange with the necessary amount of bitcoin liquidity must exist for the receiving country's market and currency. This proves to be a challenge in numerous geographies where low-cost remittance solutions would be welcome.

The bitcoin remittance service provider must then have a method to transfer the local value to the recipient. This is sometimes referred to as the "last mile", meaning the transfer of goods and services from a hub or provider to reach a final destination, typically the end-user or retail customers. The term now is applied across supply chain management, particularly in the context of developing markets, with "last mile problem" representing the challenges in getting goods and services to the end user in many of these markets, given logistical, geographical, political and other complexities.

Given these potential complexities, this is typically where the majority of costs lie for these service providers. For the value to reach local end recipients, bitcoin remittance service providers must either create a local agent network or develop partnerships with existing networks and money service providers, such as ATM networks, mobile mobile offerings, traditional banks, and cash transfer providers, which then require their own fees.

The argument which many of the bitcoin focused remittance startups make, that the overarching cost of remittances is predominantly due to the providers overcharging and the legacy infrastructure, is deemed incorrect by competitors in the space. Those arguing against feel that those costs are actually due to the last mile problem, the cost of actually getting that money into the hands of those who need it, given the costs related to logistics, geographical challenges, technology (or lack thereof) and regulation and compliance.

In addition, marketing is a massive spend area for remittance companies, particularly those who do not yet have an established brand, and this would exist for bitcoin remittance companies as for any other service provider.

Also, despite the potential cost savings using the blockchain rails, certain remittance corridors are simply too efficient, as a result of extremely high demand and market forces, to have costs driven any lower, except by players willing to take a hit in order to capture that market share. For start-ups, this typically would not be an option, at least not for the long-term.

**Case study: The Philippines**

The Philippines has been one of the most successful recipient countries to date for bitcoin-based remittance service providers. The Philippines is consistently one of the top four recipient countries of overall remittances globally, due to the country's high number of overseas workers, who send portions of their wages to family back home. The Philippines is also a country that has been at the forefront of digital financial services, partly attributed both to the country's high mobile penetration rate and a progressive regulatory environment (GSMA Mobile Money for the Unbanked 2012). In fact, in 2014, Filipino lawmaker Rep. Kimi S. Cojuangco filed a bill creating electronic money, called the E-peso, as a medium of exchange for use on the Internet and to be recognized as legal electronic tender. The Bangko Sentral ng Pilipinas (BSP) said it would study the use of bitcoin and other cryptocurrencies in order to decide on a technology to use for the E-peso (Media Relations Service-PRIB 2014).

The Philippines market has two main bitcoin service providers, Coins.ph and Rebit.ph, as well as several smaller active bitcoin remittance service providers. The presence of two strong offerings within the market, both of which engage in marketing campaigns, dialogue with regulators, and general education of the market, has helped to strengthen the demand for the services and supported the growth of the ecosystem. To what extent these services will be able to continue to capture market share of remittance to the Philippines remains to be seen.

### 2.7.3 Regulatory Environment

While initially bitcoin-related companies were able to remain under the radar of regulatory agencies, they are increasingly taking notice. For the remittance use-case in particular, given that it involves the transfer of value from one country to another, despite the fact that bitcoin itself may not be regulated, certain jurisdictions deem these businesses to fall under the regulation pertaining to money transfer. In other countries where regulatory bodies may not yet have taken a stance, many players are choosing to actively engage with policy makers to mitigate potential issues in the future and lobby for progressive policies around the technology.

There are several reasons regulatory bodies would want to maintain close watch over the space, including the potential risk for money laundering, the potential risk of circumvention of capital controls in relevant jurisdictions, and the need for consumer protection.

In the US, all businesses engaged in remittance activities, including those using bitcoin or blockchain, must hold a Money Service Business or Money Transmitter license. For many other countries, a Money Transfer Operator (MTO) license is required.

As with other consumer financial services offerings, regulators also require that proper compliance policies and procedures, covering Know Your Customer (KYC) and Anti-Money Laundering (AML), be in place.

The cost of these licenses and on-going compliance requirements can be quite onerous for smaller start-ups but are a necessary cost of doing business in the space.

### 2.7.4 Players in the Bitcoin-Enabled Remittance Space

Despite an ongoing number of entrants in this space, it is difficult to say whether any are making substantial traction to date for their intended use case, in terms of volumes and repeat users. Also listed here are a number of operations cited online which appear to no longer be in operation.

**Remittances to Asia**

- Coins.ph
- Rebit.ph
- Remitty
- Abra
- Bitspark
- CoinPip
- ZipZap
- CoinPlug
- Palarin
- Korbit
- Bitcoin India
- igot
- Gatecoin
- Zinger
- Bitcoin Vietnam
- Bitcoin Indonesia

**Remittances to Europe**

- Bit2Me
- Cashila

**Remittances to Latin America & Caribbean**

- Bitt
- HelloBit
- LibertyX
- Aircoinz

- Volabit
- SatoshiTango
- Bitso
- SurBTC
- MondoMe

**Remittances to Africa**

- Bitpesa
- Bitsoko
- Bitmari

**Global/platform offerings**

- Align Commerce
- BitX
- Stellar
- CoinJar
- Bitrefill
- BlinkTrade

**Pivoted or Closed offerings**

- Romit (pivoted to merchant payments)
- Coincove (pivoted from remittance due to regulatory burdens in the US)
- Beam (closed)
- 37Coins (closed)
- Moneero (closed)
- Buttercoin (closed)
- Bitstake (closed)
- Rebittance.org (comparison site; closed)
- Coinbatch (unknown)
- ArtaBit (unknown)

**Peer-to-peer model**
From 2014 onwards, we have seen a number of players come into the market with a service offering of peer-to-peer remittance. Sometimes referred to as an "Uber of remittance", these players provide person to person transfers without the use of a bank or third party intermediary. Sometimes referred to as a "Human ATM network", individuals can cash out money sent from other users via blockchain technology.

**Case study: Abra**
Abra is a mobile phone app, available on iPhone and Android, which allows both cash-in and cash-out via registered individuals or businesses, called Abra Tellers, who facilitate the buying and selling of digital cash and receive a small fee, which they themselves set, in return for the service. The mobile app is initially launching in the US and Philippines, with more countries to follow (Abra 2015). Deposited currency is transferred immediately to bitcoin, which is held on the individual's

smartphone. By holding value in bitcoin, the company currently avoids any regulatory requirements for transmitting payments. To users, this use of bitcoin is hidden.

**Global/Platform offerings**

In addition to consumer-facing bitcoin and blockchain-based remittance services, two entrants in the space are designed as platforms with open APIs to serve as rails for other businesses, non-profits and developers in the space.

One such example is Stellar. Stellar is an open source protocol for value exchange supported by a nonprofit, the Stellar Development Foundation. Servers run a software implementation of the protocol, using the internet to connect to and communicate with other Stellar servers and a consensus algorithm to confirm transactions, thus forming a global value exchange network (Wikipedia 2015). A decentralized protocol, it can be used to send and receive money in any pair of currencies (Stellar FAQ 2015). It allows for near instant transactions and seamless international payments at a very low cost. According to Wikipedia, two real-world applications of the Stellar protocol include Oradian, a cloud-based banking software company, which plans to use the Stellar network to connect microfinance institutions in Nigeria, and the Praekelt Foundation, which plans to integrate Stellar into Vumi, an open-source messaging app providing young women in Sub-Saharan Africa to save money in airtime credits.

## 3 Conclusion

While it is still early in the development and adoption lifecycle of both mobile money and, to a greater extent, bitcoin and blockchain based remittance offerings, the potential impact on the ability for financial services to reach those without access to traditional banking is clear. These technologies represent significant cost reductions, reduce the barriers of geography and enable new channels and pathways for interoperability of services and product offerings. The growth and evolution of these services will depend on a number of factors, including interest and adoption by the markets they are addressing, regulatory enablement and investment, and collaboration across both industry and policy markets, to help ensure accessibility, ensure trust and security and reduce costs.

## References

Abra: Abra announces public app launch and merchant API solution. Ratan Tata and American Express join Series A funding round (2015) http://blog.goabra.com/2015/10/22/abra-announces-public-app-launch-and-merchant-api-solution-ratan-tata-and-american-express-join-series-a-funding-round/ Accessed 19 Nov 2015

Wikipedia (2015) Financial Inclusion: Wikipedia entry. https://en.wikipedia.org/wiki/Financial_inclusion. Accessed 6 Dec 2015

Bitcoin Wiki (2015) https://en.bitcoin.it/wiki/Transaction_fees. Accessed 8 Dec 2015

Canning, J (2013) The Full Value of Mobile in Financial Services. https://www.thinkwithgoogle.com/articles/full-value-mobile-financial-services.html. Accessed 23 November 2015

Stellar FAQ, https://stellarorg.zendesk.com/hc/en-us/articles/201788459-What-is-Stellar, Accessed 29 Nov 2015

Cook, T., McKay, C.: How M-Shwari Works: the story so far. Forum 10. CGAP and FSD Kenya, Washington, D.C. License: Creative Commons Attribution CC BY 3.0. http://www.cgap.org/sites/default/files/Forum-How-M-Shwari-Works-Apr-2015.pdf. Accessed 10 Jan 2016

Demirguc-Kunt, A., Leora K., Dorothe S., Van Oudheusden, P.: The Global Findex Database 2014: Measuring Financial Inclusion around the World. Policy Research Working Paper 7255, World Bank, Washington, DC (2015)

IFAD Remittance Factsheet (2009). http://www.ifad.org/pub/factsheet/remittances/e.pdf. Accessed 20 Nov 2015

GSMA (2014) The Mobile Economy 2014, http://www.gsmamobileeconomy.com/GSMA_ME_Report_2014_R2_WEB.pdf. Accessed 5 January 2016

GSMA (2015) 2014 State of the Industry: Mobile Financial Services for the Unbanked, http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/03/SOTIR_2014.pdf. Accessed 26 Nov 2015

GSMA Mobile Money for the Unbanked (2012) Mobile Money in the Philippines—The Market, the Models and Regulation, http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/Philippines-Case-Study-v-X21-21.pdf. Accessed 3 Mar 2016

Media Relations Service-PRIB (2014) Bill creates E-money as medium of payment for Internet, http://congress.gov.ph/press/details.php?pressid=8212. Accessed 7 Mar 2016

Ratha, D.: Remittances: funds for the folks back home. IMF Finance & Development (2012). http://www.imf.org/external/pubs/ft/fandd/basics/remitt.htm Accessed 28 Nov. 2015

Scharwatt, C., Williamson, C.: Mobile Money Crosses Borders: New remittance models in West Africa. GSMA, London (2015)

The World Bank Group: Financial Inclusion Homepage (2015). http://www.worldbank.org/en/topic/financialinclusion/overview#GFindex Accessed 20 Feb 2016

Tiwari, R., Buse, S.: The Mobile Banking Prospects: A Strategic Analysis of Mobile Commerce Opportunities in the Banking Sector. Hamburg University Press, Hamburg (2006)

Tiwari, R., Buse, S., Herstatt, C.: Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage. Proceedings of the International Research Conference on Quality, pp. 886–894. Innovation and Knowledge Management, New Delhi (2007)

Wikipedia, the free encyclopedia (2015) Stellar (payment network), https://en.wikipedia.org/wiki/Stellar_(payment_network) Accessed 29 Nov 2015

World Bank (2015) Migration and development brief #24, 13 Apr 2015 http://siteresources.worldbank.org/INTPROSPECTS/Resources/334934-1288990760745/MigrationandDevelopmentBrief24.pdf. Accessed 28 Nov 2015

World Bank (2015) Remittance Prices Worldwide Issue No. 14, June 2015 https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2015.pdf Accessed 24 Nov 2015

## Author Biography

**Diana C. Biggs** is an advisor and executive based in London, UK where she consults on strategy and innovation in financial services and technology, with a focus on digital currency and financial inclusion. Prior to launching her consultancy, Diana was Chief Strategy Officer for Soko, a Kenya-based mobile technology social enterprise revolutionizing models of international trade. Her work in global development and finance spans more than ten years and five continents, including roles at Oliver Wyman Financial Services, the International Institute for Environment and Development (IIED) and Kiva.org. Diana was recently named one of the top 25 Fintech Influencers in the UK.

# Scalability and Egalitarianism in Peer-to-Peer Networks

**Fabio Caccioli, Giacomo Livan and Tomaso Aste**

**Abstract** Many information-technology innovations are driven, in their early stages, by an egalitarian ethos that empowers individuals through dis-intermediation. Bitcoin and peer to peer financial systems were inspired by these egalitarian ambitions. However, in bitcoin we have recently witnessed a strong centralization around a few large mining pools, which puts control of most of the system in the hands of a few. In this chapter we investigate the physical limits of distributed consensus mechanisms over networks, and discuss whether there are scalability and efficiency reasons that incentivize centralization. We compute the time to reach majority consensus in a variety of settings, comparing egalitarian networks with centralized networks, and quantifying the effect of network topology on the propagation of information.

**Keywords** Majority consensus mechanism on networks · Bitcoin network · Egalitarianism and scalability

## 1 Introduction

We are currently witnessing the rise of a new form of distributed economy, which emerges from the combination of digital communication infrastructures and the big data revolution. Peer-to-peer decentralized economies and finance have the potential

F. Caccioli · G. Livan · T. Aste (✉)
Department of Computer Science, University College London, Gower Street, WC1E 6BT, London, UK
e-mail: t.aste@ucl.ac.uk

F. Caccioli
e-mail: f.caccioli@ucl.ac.uk

G. Livan
e-mail: g.livan@ucl.ac.uk

F. Caccioli · G. Livan · T. Aste
Systemic Risk Centre, London School of Economics and Political Sciences, WC2A2AE, London, UK

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_11

to provide citizens with direct control over their activities, by removing intermediation layers and fostering inclusion. Blockchain is providing the technology to make this happen in a secure and reliable way. Distributed systems are being constructed around an egalitarian ethos according to which "peers" freely exchange goods and information without the need of a central authority to establish trust, verify identity, or enforce commitments. Yet, we are witnessing that many of such idealistic egalitarian forms of economic organization are changing their nature as they evolve. In fact, these systems show a strong tendency to naturally evolve towards structures where a small portion of nodes has a large influence over the whole system. This has been for instance observed in the evolution of the mining pools in bitcoin, where the system has evolved form a fairly egalitarian network of miners, in which individuals were able to mine their coins at home, to highly specialized and concentrated industrial-scale mining activities. A similar evolution has been observed in the world wide web, which started from a distributed community of people and companies, and evolved into a highly centralized system where. For instance, Facebook owns 1.49 billion active users profiles (2015) and 99.9 % of web searches in US are run through 5 search engines only, with Google accounting for over 64 % (2015) of them. This concentration is due to simple economic rules that demand greater efficiency and lower costs. This return-to-scale economic law introduces however new forms of information asymmetry (Garcia 2014) and new kinds of risk related to the presence of very large quantities of personal information held in a few places only. Within the context of distributed systems that generate consensus with majority vote, such tendency towards concentration can be very dangerous.

In this chapter we discuss the relation between the structure of communication network and the functional properties of peer-to-peer systems. In particular, we discuss the relation between level of equality between nodes in the network, and efficiency and scalability.

The chapter is structured as follows: we present in Sect. 2 a short introduction to complex networks, and we discuss in Sect. 3 how the properties of information spreading processes depend on the network topology. We then present in Sect. 4 an application to bitcoin blockchain, and we study in particular how the occurrence of blockchain forks is related with the properties of the underlying network. In Chap. 4 we present conclusions.

## 2 A Brief Introduction to Complex Networks

Networks are the most general way to represent systems made of several entities characterized by pairwise interactions. A network is defined in terms of a set of nodes $\{1, 2, \ldots, N\}$ and a set of links $\{e_1, e_2, \ldots, e_M\}$, where each link connects a pair of nodes. Nodes connected by a link are said to be *neighbors*, and the number of neighbors of a node is the node's *degree*. A convenient way of representing a network is in terms of its adjacency matrix $\mathbf{A}$, whose element $A_{ij}$ is 1 if node $i$ is connected to node $j$, and zero otherwise. Each node in a network can interact with its neighbors, that are the nodes connected to it through links.

Several dynamical processes take place on networks. Certain processes, such as searches on the Internet or propagation in power grids, happen on physical networks. Other processes are mediated by non-physical network structures, such as, e.g., the spreading of epidemics or the word of mouth diffusion of information in a social system. In both cases the topological properties and the heterogeneity of the underlying networks play a crucial role in driving the evolution and, possibly, determining the outcome of the dynamics at hand. Countless network topology models, and their impact on dynamical processes, have been studied in the dedicated literature (see for instance Albert and Barabási 2002; Sergey 2008; Oxford University Press 2010; Alain Barrat et al. 2008). In the following, we outline the properties of the two most common *random* network classes. In this context, random does not mean chaotic or disorganized. On the contrary, we shall focus on ensembles whose individual realizations all share a number of well defined *statistical* properties. In particular, it has been shown that the degree distribution $P(k)$ of a network, that defines the probability of a node to have degree $k$, strongly affects the dynamical properties of processes taking place on networks (Alain Barrat et al. 2008; Bianconi 2002; De Martino et al. 2009). Here we are interested in exploring the effect of the network structure on its capability to efficiently propagate information, which is at the basis of the validation mechanism in blockchain systems and is directly related with efficiency and egalitarianism. We will therefore focus on two classes of networks with very different degree distributions: the Poisson distribution, that is rather equalitarian, and the power-law distribution, that is dis-equalitarian, being characterized by a few hub nodes with very large degrees, and a multitude of other nodes with small degree.

## 2.1 Erdős-Rényi Networks

The Erdős-Rényi (ER) random network model was devised in the late fifties, and it represents the most popular benchmark model for networks featuring *mild heterogeneity*. It consists of $N$ nodes, and each of the $N(N-1)/2$ pairs of nodes in the network have a fixed probability $p$ to be connected. Clearly, this formation scheme creates, on average, a total number of $pN(N-1)/2$ links, with an average degree of $\langle k\rangle = p(N-1)$.

What about individual nodes? The probability that a given node $i$ will be connected to exactly $k$ neighbors (in network jargon this is referred to as node $i$ having degree $k_i = k$) is proportional to the probability of independently "hitting" $k$ nodes (each with probability $p$) and "missing" the other $N-k-1$, which is a bimodal distribution:

$$\text{Prob}(k_i = k) = \binom{N-1}{k} p^k (1-p)^{N-k-1}. \tag{1}$$

From the above equation it is straightforward to compute that the probability of hitting a fraction $\alpha N$ of nodes becomes exponentially small in $N$ when $\alpha \to 1$, i.e. $\text{Prob}(k_i = \alpha N) \propto \exp(\alpha N \log p)$. Taking the large $N$ approximation of Eq. (1), one can also show that the degree distribution of a large network is very well approximated by a Poisson distribution

$$P(k) = \frac{(pN)^k}{k!} e^{-pN} . \tag{2}$$

The above result means that both the average and the variance of the ER model's degree distribution are given by $pN$. All in all, these results justify the previous hint at mild heterogeneity or, in other words, egalitarianism: in the ER model there are no nodes that dominate the network by linking to a disproportionately large fraction of peers, and the Poisson degree distribution (2) concentrates most of the probability within a limited set of degrees around the average.

Processes on ER networks can reach the entirety of the network by starting form a single node in a number of steps that is proportional to the logarithm of the total number of nodes $N$. This is called the *small world* effect. Intuitively, given that each node has on average $pN$ neighbors, one expects the number of nodes at a distance $d$ from a given node $i$ to scale as $(pN)^d$: on average, node $i$ has $pN$ neighbors, and so do they and the nodes higher upstream from $i$. For sufficiently large values of $d$, the number of nodes found at distance $d$ from $i$ is a finite fraction of all nodes in the network. From this consideration, one finds that the average distance between pairs of nodes in an ER network scales as

$$d \simeq \frac{\log N}{\log(pN)} \simeq \frac{\log N}{\log \langle k \rangle} . \tag{3}$$

Therefore a process evolving on the network form any given node will reach any other node in average after a number $d \propto \log N$ of steps.

## 2.2 *Scale-Free Networks*

Many real-life networks are not egalitarian, and are dominated by a small fraction of hubs connected to a substantial fraction of nodes. In mathematical terms, this is best described in terms of a power law, hence scale-free, distribution of the degrees, i.e.

$$P(k) \sim k^{-\gamma} , \tag{4}$$

the tail index $\gamma > 0$ is a very important parameter. Networks with smaller values of $\gamma$ have larger hubs and are less egalitarian as we shall see shortly.

Quite interestingly, modeling the topology of scale-free networks requires describing their growth and evolution, in a way which is quite revealing about the mechanisms leading to the emergence of dominant nodes. Such description is provided by the Barabasi-Albert model of *preferential attachment* (Barabási and Albert 1999). Starting from a small group of nodes, the network is built by adding nodes one at a time, and each newcomer connects to one of the already existing nodes. In particular, the new node connects to a given node $i$ with a degree-dependent probability $\pi$ that reads

$$\pi(k_i) = \frac{k_i}{\sum_{j=1}^{M} k_j}, \tag{5}$$

where $k_i$ is node $i$'s degree, and $M$ is the number of nodes present in the network. The preferential attachment growth rule (5) gives a competitive advantage to nodes that already have a high degree, in a rich-get-richer fashion. This mechanism indeed gives rise (for large $N$) to a power law degree distribution (4), with a tail exponent $\gamma = 3$. Exponents $\gamma$ with values other than three can be achieved with generalizations of the preferential attachment rule (5) (see, e.g., Paul 2000).

## *2.3 Network Egalitarianism*

The egalitarianism, or lack thereof, of a network can be measured directly from its degree sequence in terms of Gini coefficient, i.e. the most popular measure of inequality in a population. Despite having been originally intended and still being mostly used as a measure of wealth inequality, the Gini coefficient can be used to assess how unevenly a generic quantity is distributed across a given population. Let us then consider the sequence $k_i$, $i = 1, \ldots, N$, of degrees in a network. The Gini index $G$ of the sequence is defined as

$$G = \frac{\sum_{i<j} |k_i - k_j|}{N \sum_{i=1}^{N} k_i}. \tag{6}$$

The above expression can be easily manipulated to show that it corresponds to half the average absolute difference between degrees (normalized to the average degree in the network), i.e. $G = \langle |k_i - k_j| \rangle / (2\langle k \rangle)$. The Gini coefficient is bounded between zero, which is achieved under complete equality $(k_i = k, \forall\, i)$, and one, which is achieved asymptotically under complete concentration on one node (formally $k_i = k$ for a given node $i$ and $k_j = 0$, for all other nodes $j \neq i$, even though this does not correspond to a feasible degree sequence).

An alternative inequality measure is represented by the Theil index, which is akin to an entropy measure and is also bounded between zero (complete equality) and one (complete concentration on one node). It reads

$$T = \frac{1}{N \log N} \sum_{i=1}^{N} \frac{k_i}{\langle k \rangle} \log \frac{k_i}{\langle k \rangle}. \tag{7}$$

In Fig. 1 we show the average behavior of the Gini and Theil indices computed from networks with degree sequences distributed according to Eq. (4).

As Fig. 1 reveals, networks with extremely heavy tailed degree sequences $(\gamma \simeq 1.25)$ show very large Gini coefficient values $(G \sim 0.65)$, comparable to those

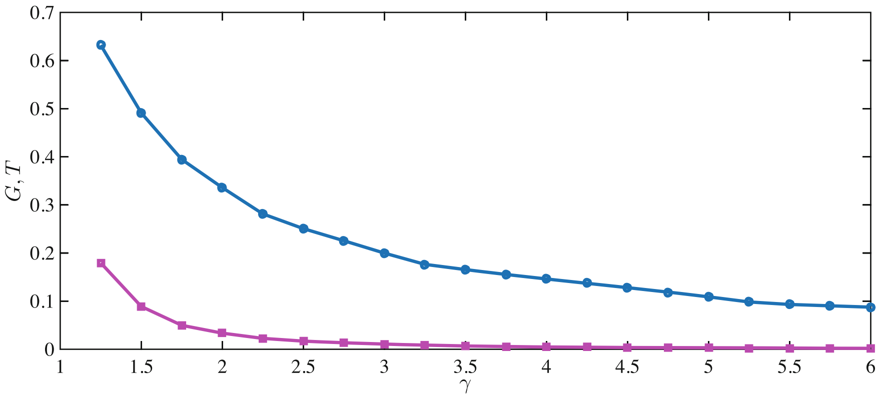


**Fig. 1** Gini (*blue circles*) and Theil (*purple squares*) indices as a function of the tail exponent $\gamma$ of a power law distributed degree sequence (4). For each value of $\gamma$ results are obtained by averaging over 100 networks made of $10^4$ nodes, with a fixed average degree $\langle k \rangle = 8$ (the value does not affect the behavior of the Gini coefficient)

measured, e.g., for individual wealth distribution in those countries with the highest observed wealth inequality levels. This reflects the strong centralization induced by the degree distribution (5) for low values of $\gamma$, which generates a few hubs with $\mathcal{O}(N)$ links, and leaves the vast majority of the nodes with a few connections only. Increasing the tail exponent reduces centralization, which is very well captured by the corresponding monotonic decrease of the Gini coefficient shown in Fig. 1. When the tail exponent is large enough to ensure the convergence of the first few moments (i.e. $\gamma \gtrsim 3.5$), the network degree distribution is de facto egalitarian, despite still being power law, as the Gini coefficient is quite close to zero and well within ranges that are naturally observed in systems characterized by mild heterogeneity. For instance an Erdős-Rényi network with $\langle k \rangle = 8$, as the one used in the example in Fig. 1, has a Gini coefficient around 0.08. Similar considerations can be made from the behavior of the Theil index, which also decays to values very close to zero for $\gamma \gtrsim 3.5$.

The presence of heavily connected hubs in scale-free networks improves the communication between nodes by providing additional paths with respect to more homogeneous topologies, e.g., ER networks. In fact, for $\gamma \geq 3$, the average distance between nodes in scale-free networks scales logarithmically in $N$, as in (3), but it is systematically smaller than that of ER networks when comparing systems with the same average degree (see Albert and Barabási 2002). When $2 < \gamma < 3$ the distance between nodes scales as $\log \log N$ and when $\gamma \leq 2$ the distance becomes a few steps only independently from the size of the network (Oxford University Press 2010).

Facilitated communication between nodes comes at a price, as scale-free networks are much less resilient than their more egalitarian counterparts. Attacks aimed at destroying hubs can have severely disruptive effects on the transport properties. On the other hand, ER networks are more resilient to targeted attacks, as no node (or group of nodes) is particularly central in the topology.

### 2.4 Collective Properties of Networks

The topology of networks strongly affects their collective properties. For instance, the threshold for the emergence of a giant component is very different in ER versus scale-free networks. A network of $N$ nodes has a giant component if the size $S$ of its largest connected component (a connected component is a set of nodes such that any pair amongst them is connected by at least one path) is formed by an extensive number of nodes, i.e. $\lim_{N\to\infty} S/N > 0$. For uncorrelated networks (i.e. networks with no correlations between degrees of neighboring nodes), it is possible to show (2008) that a giant component is present if

$$\frac{\langle k^2 \rangle}{\langle k \rangle} > 2, \tag{8}$$

where $\langle k \rangle$ and $\langle k^2 \rangle$ are the first and second moments of the degree distribution. From the above criterion, it follows that ER networks always have a giant component if $\langle k \rangle > 1$, whereas scale-free networks display a giant component if $\gamma \leq 3$.

Similarly, it is possible to show that disease spreading processes on scale-free networks always lead to an epidemic outbreak whenever $\gamma \leq 3$, while on ER networks this does not happen if the rate of contagion is low enough (Pastor-Satorras and Vespignani 2001).

In the following section, we consider a simple model of information spreading, and we discuss how this process is affected by the structure of the network.

## 3 A Network Model of Blockchain Forks: Efficiency and Egalitarianism

In the context of bitcoin (Nakamoto 2008), each node is a server that keeps a ledger containing a record of all past transactions. Different ledgers are synchronized at regular intervals by broadcasting a block created by one node. A block contains all transaction that have been recorded by a node since the last block was broadcasted and verified by all nodes in the system. When a new block, $A$, is found by a node, the node will broadcast it to its neighbors, these in turn will broadcast it to their neighbors, and so on. A conflict may arise if an alternative block $B$ is independently discovered by a node before the block $A$ has reached all nodes in the system. Such a conflict is called *fork*. Blockchain forks should be avoided because they effectively amount to inconsistencies in the system. In the following, we consider the model introduced in (Christian Decker and Roger Wattenhofer. Information propagation in the bitcoin network. In Peer-to-Peer Computing (P2P) 2013) to show how the structural properties of networks affect the propagation of information through the network.

We consider a model in which we have a network of $N$ nodes. Each node is endowed with an integer variable $\sigma_i \in \{-1, 0, 1\}$. When $\sigma_i = 0$ no new block has been discovered or verified by node $i$ since the previous synchronization, while states $\pm 1$ represent two conflicting blocks. We consider a very simple dynamics in which at time $t = 0$ all nodes are in state 0 except a randomly chosen fraction, which are in state 1. The dynamics then runs as follows: at rate $\beta$, a node $i$ in state $+1$ will broadcast its block to its neighbors in state 0, while potentially conflicting blocks can be discovered by any node in state 0 with rate $\eta$. Whenever a conflicting block is found, the node responsible for its discovery switches to state $-1$ and starts propagating to its neighbors in state 0 at rate $\beta$.

In the following, we will present an analytical description of the model for Erdős-Rényi random networks, for which we will compute the probability of observing a fork as a function of the average degree of the network, its size (i.e. the number of nodes), as well as the fraction of nodes to which the block has been broadcasted. We will then present a comparison between the performance of Erdős-Rényi and scale-free networks.

## 3.1 Erdős-Rényi Networks

We are interested in computing the probability that the initial block is broadcasted to a fraction $n^*$ of nodes in the system before an alternative block is discovered. Until no new blocks are discovered, the dynamics of the system is equivalent to that of a Susceptible-Infected (SI) process (Alain Barrat et al. 2008). The SI model on an Erdős-Rényi random network can be described in terms of the following rate equation:

$$\frac{dn_A(t)}{dt} = \beta n_A(t)(1 - n_A(t)) \; , \tag{9}$$

where $n_A(t)$ is the fraction of nodes to which block $A$ has been broadcasted to (informed nodes), and $\beta$ is the rate at which the signal coming from an informed node reaches one of its uninformed neighbors. For Erdős-Rényi networks we can write $\beta = \langle k \rangle c p_0 / \langle l \rangle$, where $c$ is the speed at which the signal travels, $\langle l \rangle$ is the average distance between two nodes, and $p_0$ the rate at which the informed node sends the signal. Equation (9) can be intuitively understood as follows: In a time interval of length $dt$ each node in state $+1$ will broadcast the block $B$ to its neighbors with probability $\beta dt$, hence the term $\beta n_A(t)$ in the equation. A node that is broadcasting will propagate the block to its neighbors that have not been yet informed, whose number can be approximated as $\langle k \rangle (1 - n_A(t))$, i.e. the average number of neighbors of a node times the probability that a node is in state 0.

The solution of Eq. (9) is given by (see for instance Alain Barrat et al. 2008)

$$n_A(t) = \frac{n_A(0)e^{\beta t}}{1 + n_A(0)(e^{\beta t} - 1)} \; . \tag{10}$$

If $n_A(0)$ is the fraction of nodes that know the block $A$ at time zero, we can compute the time $T(n^*)$ needed for block $A$ to be broadcasted to a fraction $n^* \in [n_A(0), 1 - 1/N]$ of the system. This time can be computed by solving the equation $n_A(T(n^*)) = n^*$, which gives

$$T(n^*) = \beta^{-1} \log\left(\frac{n^*(1 - n_A(0))}{n_A(0)(1 - n^*)}\right) \; . \tag{11}$$

From this equation we can compute the time needed for a block to be broadcasted to 50 % of the nodes without alternative blocks being discovered. If we assume the process to start from a single informed node (i.e. $n_A(0) = 1/N$) we have

$$T(50\,\%) \simeq \frac{\log N}{\beta} \; . \tag{12}$$

From this we see that the time needed for information to be propagated in the network increases logarithmically with the size of the network and it is inversely proportional to $\beta = \langle k \rangle c p_0 / \langle l \rangle$.[1] Therefore, propagation speed can be increased by increasing the average connectivity.

Equation (11) can be calibrated to obtain an estimate for the minimum time $T_{\mathrm{m}in}(50\,\%)$ needed for a block to reach 50 % in a realistic situation. A rough estimate of $T_{\mathrm{m}in}(50\,\%)$ can be given as follows: Let us consider $N$ nodes that are randomly placed on a spherical surface of radius $R_0$, the radius of the Earth. The average distance between these nodes is $\pi R_0/2$. Since information cannot propagate faster than light, we have that the minimum average time for a block to be propagated between two nodes is $\frac{\pi R_0}{2c}$ and therefore the minimum time to reach 50 % of the nodes in the network is

$$T_{\mathrm{m}in}(50\,\%) \; = \; \frac{\pi R_0 \log N}{2c\langle k \rangle} \approx 0.033 \frac{\log N}{\langle k \rangle} \mathrm{s} \tag{13}$$

considering that in the blockchain there are $N \approx 6000$ nodes, and $\langle k \rangle \approx 10$ we have $T_{\mathrm{m}in}(50\,\%) \; \simeq$ 30ms. From this result we note that in a network with $\langle k \rangle > \log N$ the average time to reach 50 % of the nodes can be faster than the time needed in

[1] More in general, it is possible to show that the initial phases of the propagation process are characterized by an exponential behavior for the fraction of informed nodes over time. This increases with a characteristic time $\tau = 1/\beta$,with $\beta = \frac{cp_0}{\langle l \rangle} \frac{\langle k^2 \rangle - \langle k \rangle}{\langle k \rangle}$. Note that, for a scale-free network with a tail exponent $2 < \gamma \leq 3$, if we consider the natural cut-off $N^{1/(\gamma - 1)}$ for the degree distribution (Sergey 2008), we find that $\beta$ scales as $\beta \sim \langle k^2 \rangle / \langle k \rangle \sim N^{1/(\gamma - 1)}$ for large values of $N$. This would alter the dependence of $T(0.5)$ on $N$ in Eq. (12), speeding up the propagation.

average to reach all the neighbors of a given node. This is not a contradiction, and it is due to the fact that the first neighbors to be informed start broadcasting the information to their neighbors, and, among these, those which receive the information start broadcasting it to their neighbors, and so on.

From Eq. (11) we can also compute the probability that, given a discovering rate $\eta$, no new block is discovered before block $A$ has been broadcasted to a fraction $n^*$ of the system. In the continuous time limit we have that

$$q(n^*) = 1 - (1-\eta)^{N\int_0^{T(n^*)}(1-n_A(t))dt}. \tag{14}$$

Plugging Eq. (11) into Eq. (14), we can write $q(n^*)$ as

$$q(n^*) = 1 - (1-\eta)^{Nf(n^*,\beta)}, \tag{15}$$

where

$$f(n^*, \beta, n_A(0)) = \beta^{-1}\log\left(\frac{n^*}{n_A(0)}\right), \tag{16}$$

from which we easily find that

$$\begin{aligned} q(n^*) &= 1 - (1-\eta)^{\beta N \log(n^*/n_A(0))} \\ &= 1 - \left(\frac{n^*}{n_A(0)}\right)^{\beta N \log(1-\eta)}. \end{aligned} \tag{17}$$

Equations (15) and (16) can be used to characterize the performance of the network as a function of all its structural parameters, such as its average degree and size. In the following, we will measure the efficiency of a network in terms of the probability $q(50\,\%)$ that block $A$ reaches $50\,\%$ of the network before block $B$ is discovered. Other metrics could be used, for instance the fork probability can be computed from the above equations as the probability that the block $A$ is broadcasted to $N-1$ nodes before an alternative block is found.[2]

In Figs. 2 and 3 we show the behavior of $q(50\,\%)$ as a function of the average degree of the network and its size. In both cases there is very good agreement between numerical simulations and analytical results from Eq. (17). Figure 2 highlights the role played by the network's *density*, as measured by the average degree. In fact, an increase in density (at fixed $N$) corresponds to an increase in the average number of connections each node can exploit to broadcast a newly discovered block, therefore speeding up the overall propagation process and ensuring a fast convergence to consensus. On the other hand, very sparse networks are rather

[2] Note here that the analytical equations are not defined for $n^* = 1$.

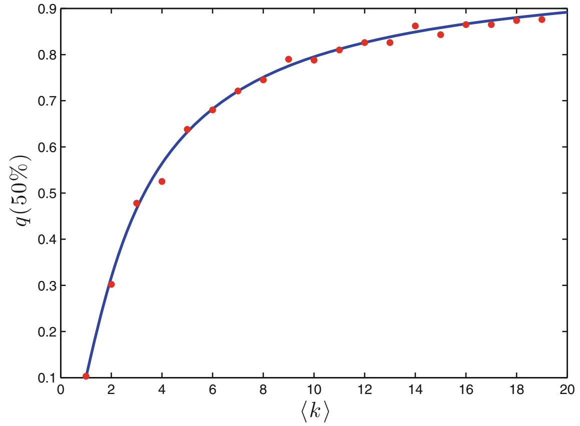


**Fig. 2** Effect of connectivity on block propagation: Probability of reaching 50 % of the network before a conflicting block is discovered as a function of the network's average degree $\langle k \rangle$ for a system with $N = 1000$, $\eta = 10^{-3}$, and $n_A(0) = 0.1$. *Dots*: results from numerical simulations. *Solid line*: analytical result from Eq. 17. There is an overall good match between analytical and numerical results, which show that an increase in connectivity is beneficial to the network's efficiency

inefficient, as low connectivity practically corresponds to low average numbers of paths connecting distant nodes, i.e. to the de facto separation between different regions of the network.

Figure 3 shows instead that network expansion at fixed density has adverse effects on the efficiency of block propagation, as the presence of larger numbers of nodes increases the likelihood of discovering conflicting blocks.

Lastly, Fig. 4 shows the probability of informing 50 % of the network (at fixed density and number of nodes) conditional on having already informed a fraction $n_A(0)$ of nodes at an initial time $t = 0$. As one would expect intuitively, efficiency increases monotonically with $n_A(0)$. However, let us note that there are remarkable marginal gains in efficiency for relatively small increases of the initially informed fraction of nodes. This is shown in the inset in Fig. 4, where we plot the discrete derivative of $q(50\,\%)$ that corresponds to incrementing the number of initially informed nodes by one node at a time.

### *3.2 Comparing the Performance of Different Networks: Erdős-Rényi Versus Scale-Free Networks*

In the previous section we have seen how properties such as the size of an Erdős-Rényi network and its average degree affect the probability that a block reaches the majority of the system before a conflict occurs. We now turn to the

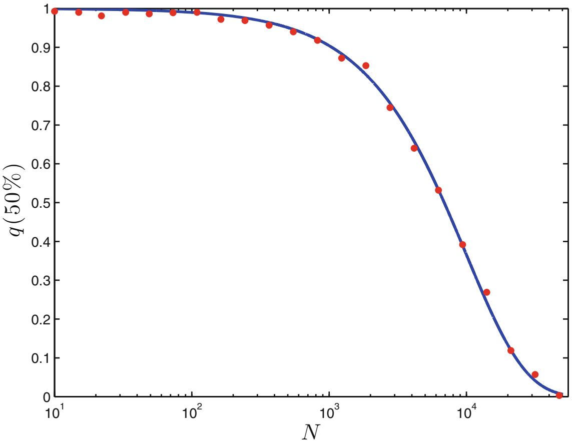


**Fig. 3** Scalability with respect to network size: Probability of reaching 50 % of the network before a conflict as a function of network size for a system with $\langle k \rangle = 7$, $\eta = 10^{-3}$, and $n_A(0) = 0.1$. *Dots*: results from numerical simulations. *Solid line*: analytical results from Eq. 17. As can be seen, there is a very good agreement between analytical and numerical results, which show that network expansion at fixed densities, i.e. at fixed average degree $\langle k \rangle$, increasingly prevents the likelihood of reaching consensus in the system

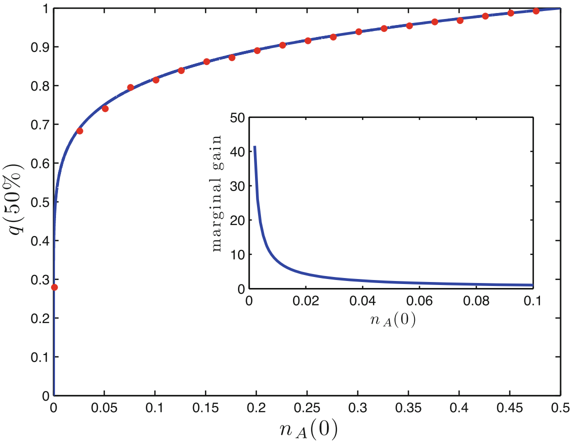


**Fig. 4** Dependence on initial condition: Probability of reaching 50 % of the network conditional on a given fraction $n_A(0)$ of nodes being already informed for a system with $\langle k \rangle = 7$, $\eta = 10^{-3}$, and $N = 1000$. *Dots*: results from numerical simulations. *Solid line*: analytical results from Eq. 17. Inset: zoom in the region of small $n_A(0)$. Controlling 5 % of the system allows to reach the majority of the system without observing conflicts in about 70 % of the cases

comparison of the performance of Erdős-Rényi with respect to that of scale-free networks. To this end we resort to numerical simulations, because there is no analytical solution for the case of scale-free networks. For scale-free networks, we

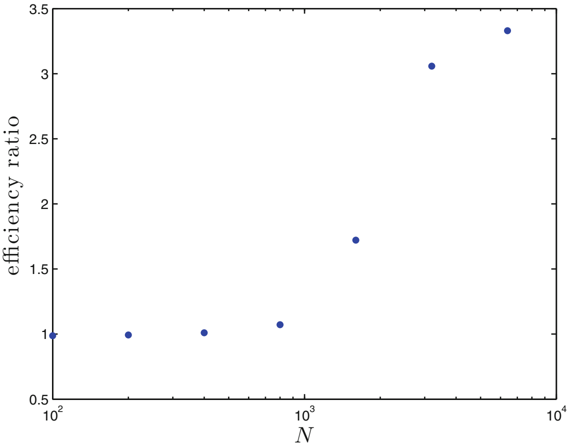


**Fig. 5** Scalability of Erdős-Rényi versus scale-free networks: Ratio between the probability of reaching 50 % of the networks before a new block is discovered on scale-free over Erdős-Rényi networks with the same average degree $\langle k \rangle = 8$ as a function of the network size. As the size increases scale-free networks become more efficient than Erdős-Rényi networks

consider networks generated through a linear preferential attachment rule (Barabási and Albert 1999). This mechanism generates networks whose degree distribution has a tail exponent equal to $\gamma = 3$. This is a rather common exponent value for real networks (Oxford University Press 2010). In Fig. 5 we plot the ratio between the probability of reaching the majority of the network before a conflict in scale-free vs. Erdős-Rényi networks with the same average degree $\langle k \rangle = 8$, and for different values of $N$. From the plot, we see that networks generated through preferential attachment become more efficient as $N$ increases. The increased efficiency of scale-free networks is due to the presence of hubs, that connect most of the nodes in the network through short paths. However, the presence of hubs also increases the fragility of the network with respect to targeted attacks. In fact, it has been shown (Oxford University Press 2010) that an attack protocol that seeks to remove nodes starting from those with the highest degree quickly breaks a scale-free networks into disconnected components. For instance, the fraction of nodes that need to be removed for the giant component to disappear is, in the case of scale-free networks, typically of a few percent (Cohen et al. 2001; Sergey 2001). Although the scale-free networks we have used in our simulations have a tail exponent $\gamma = 3$, we expect the higher efficiency of scale-free networks to hold also for smaller values of $\gamma$, as lowering the tail exponent increases the probability of having hubs in the system.

## 4 Conclusion

Topology strongly affects the behavior of dynamical processes taking place on networks. In this chapter we have shown how egalitarianism is in conflict with efficiency. This was shown by reviewing the main features of two common ensembles of random networks, Erdős-Rényi and scale-free. Erdős-Rényi networks have a Poisson degree distribution, while scale-free networks have a power-law degree distribution. The latter implies the existence of hubs in the network, i.e. nodes with significantly more connections than the average degree, that are not present in Erdős-Rényi networks. Therefore, as suggested by the Gini coefficient associated with the degree distribution of these network ensembles, the two can be considered as prototypical examples of egalitarian and non-egalitarian networks.

We have discussed that the difference in the degree distributions of these two classes of networks has profound consequences on their behavior, for instance regarding the emergence of a giant component of connected nodes, or the propagation speed of signals in the network. The focus of this chapter was to understand how the propagation of information on networks is affected by their topology. In particular, we have considered a stylized model of block-propagation in the blockchain. In the model, we assume that a new block has been discovered and has to be propagated to the whole network before an alternative block is found, leading to a conflict. Two competing processes take therefore place in the network. On one hand, nodes that have been informed about the new block broadcast it to their neighbors, on the other hand nodes that have not yet been informed can find an alternative block.

We have provided an analytical formula for the probability that a conflict arises in an Erdős-Rényi network, and we have characterized its dependence on the size of the network and its average degree. By means of numerical simulations, we have compared the performance of Erdős-Rényi and scale-free networks, and we have shown that the latter perform better as the size of the network increases. This finding suggests the existence of a trade-off between efficiency and nodes' equality.

## References

http://www.comscore.com/Insights/Market Rankings/comScore-Releases-June-2015-US-Desktop-Search-Engine-Rankings, 09 2015

Albert, Réka, Barabási, Albert-László: Statistical mechanics of complex networks. Rev. Mod. Phys. **74**(1), 47 (2002)

Barrat, A., Barthelemy, M., Vespignani, A.: Dynamical Processes on Complex Networks. Cambridge University Press (2008)

Barabási, Albert-László, Albert, Réka: Emergence of scaling in random networks. Science **286** (5439), 509–512 (1999)

Bianconi, Ginestra: Mean field solution of the Ising model on a Barabási-Albert network. Phys. Lett. A **303**(2), 166–168 (2002)

Cohen, Reuven, Erez, Keren, Ben-Avraham, Daniel, Havlin, Shlomo: Breakdown of the internet under intentional attack. Phys. Rev. Lett. **86**(16), 3682 (2001)

Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P), 2013, pp. 1–10. IEEE (2013)

De Martino, Daniele, Dall'Asta, Luca, Bianconi, Ginestra, Marsili, Matteo: Congestion phenomena on complex networks. Phys. Rev. E **79**, 015101 (2009)

Dorogovtsev, S.N., Goltsev, A.V., Mendes, J.F.F.: Critical phenomena in complex networks. Rev. Mod. Phys. **80**(4), 1275 (2008)

Garcia, D., Tessone, C.J., Mavrodiev, P., Perony, N.: The digital traces of bubbles: feedback cycles between socio-economic signals in the bitcoin economy. J. Roy. Soc. Interface **11**(99), 20140623 (2014)

Krapivsky, P.L., Redner, S., Leyvraz, F.: Connectivity of growing random networks. Phys. Rev. Lett. **85**(21), 4629 (2000)

Nakamoto, Satoshi: Bitcoin: A peer-to-peer electronic cash system. Consulted **1**(2012), 28 (2008)

Newman, M.: Networks: An Introduction. Oxford University Press (2010)

Pastor-Satorras, Romualdo, Vespignani, Alessandro: Epidemic spreading in scale-free networks. Phys. Rev. Lett. **86**(14), 3200 (2001)

Sergey, N.: Dorogovtsev and José FF Mendes. Phys. Rev. Lett. **87**(21), 219801 (2001)

## Author Biographies

**Fabio Caccioli** is a lecturer in the Department of Computer Science at University College London. He was previously a research associate in the Centre for Risk Studies, University of Cambridge, and a postdoctoral fellow at the Santa Fe Institute (Santa Fe, US). Fabio holds a Ph.D. in Statistical Physics from the International School for Advanced Studies (Trieste, Italy).

**Giacomo Livan** is a Ph.D. in Physics from the University of Pavia (Italy). In 2011 I joined the Abdus Salam International Centre for Theoretical Physics (Trieste, Italy) as a Postdoctoral Fellow, and in 2014 I joined the Department of Computer Science of UCL as Research Associate. Since 2016 I am an EPSRC Early Career Fellow in Digital Economy.

**Tomaso Aste** is Professor of Complexity Science at UCL where he is Head of the Financial Computing & Analytics Group, co-Director of the UCL Centre for Blockchain Technologies, Director of the M.Sc. in Financial Risk Management, vice-Director of the UK Financial Computing & Analytics Doctoral Centre and a member of the Board of the LSE Systemic Risk Centre. He is recognized as a world-leading scientist in complex system studies and financial big-data analytics.

# Are Transaction Costs Drivers of Financial Institutions? Contracts Made in Heaven, Hell, and the Cloud in Between

**James Hazard, Odysseas Sclavounis and Harald Stieber**

**Abstract** In 16th century Europe, the revolution in printing technology and increasing literacy in European cities created a positive shock to capital productivity. At the same time, the spread of Protestantism in Northern Europe induced individuals to honour contracts or risk exclusion from the Kingdom of God. Max Weber would argue that the religious institution of Protestantism, by dissuading defection from agreements, had allowed a new form of almost trustless exchange with strangers. Strict self-enforcing religious rules restrained individuals from opportunistic behaviour thus lowering the cost of monitoring and enforcing contracts. This led to increasing commerce and economic growth. A better capitalized, but less strict Catholic Southern Europe was unable to exert control and reduce contracting costs in the same way leading to less exchange. We argue that peer to peer technologies, such as Bitcoin, Blockchains, smart contracts, and peer-to-peer (P2P) legal platforms recall these historical evolutions. We anticipate that these technologies will reduce the cost of contracting, specifically with regards to contract monitoring and enforcement. Trustless exchange without some of the current intermediaries specializing in monitoring and enforcement technologies will have a significant impact on the financial system and its institutional structure. Moving beyond theory, this chapter discusses some of the major manifestations of technologies capable to strongly decrease the cost of contracting, and it proposes a certain class of models to explore how P2P technologies, and the concomitant reduction in transaction costs they will cause, can be expected to affect financial exchange.

**Keywords** Transaction costs • Property rights • Transactional relationships • Contracts and reputation • Networks

J. Hazard
CommonAccord, Founder, Silicon Valley, San Francisco, USA
e-mail: james.g.hazard@gmail.com

O. Sclavounis (✉)
Oxford Internet Institute, Oxford, UK
e-mail: odysseas.sclavounis@gmail.com

H. Stieber
European Commission, Brussels, Belgium
e-mail: harald.stieber@ec.europa.eu

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_12

# 1 Introduction

> *"It took some early adopters with enough faith to actually spend real money to purchase some bitcoins to start to give it a value."* Gavin Andresen, Chief Scientist at the Bitcoin Foundation, during a keynote at Princeton University, 27 March 2014

In 16th century Europe two parallel developments were unfolding that would help bring down the cost of contracting. The first was the development of the printing press and concomitant increases in literacy rates which increased the stock of human capital. This decreased the cost of defining and monitoring property rights. The second was the spread of various forms of Protestantism, instructing adhering individuals to honor contractual obligations or risk exclusion from the Kingdom of God. This had the effect of decreasing enforcement costs as agreements became largely self-enforcing. Several centuries later, Weber argued that this religious institution had allowed a new form of (almost) trustless exchange between complete strangers and led to an era of international commerce creating substantial wealth. Although both the technological and institutional developments were key to reducing the cost of contracting, the development of a religious institution was found to be decisive in promoting self-enforcing contracts linked to higher economic growth rates. The decentralization of the function of monitoring and enforcement of contracts led to greater capital productivity.

We argue that the transaction cost approach used to understand the changes in behavior, contracting, and institutions in 16–18th century Europe, can similarly be applied to understanding current technological developments in P2P technologies. P2P technologies such as Bitcoin and other Blockchain-enabled technologies have changed the nature of contracting (definition, monitoring, and enforcement) especially as it relates to the enforcement function. Specifically, we argue that these technologies have the potential to drastically reduce and, more importantly, restructure the transaction costs associated with contracting. This reduction and restructuring of transaction costs allows for 'hub less' contracting, significantly reducing counter-party risk. This chapter brings this insight to bear in understanding the potential for change in the financial system.

In thinking about the future of money and banking, we argue that transaction costs could play a pivotal role with respect to new financial technologies' capacity to dislocate or disrupt existing institutions and organizations such as cash, or universal banking. We do not argue that transaction costs are the only determining factor. Rather we think that they are among those factors that we can actually understand quite well *ex ante*, i.e. before the actual adoption of new technologies in time and space will provide the ultimate answers.

At the start of our reflection it is necessary to analyze how successful *current* financial institutions have been in reducing transaction costs. For both money and banks, the *centralization* of control seems to have played a crucial role. In the case of money, fiat money has regularly led to inflation and abandon were it not for strong and *credible* central control of the money supply (examples are the early Chinese experiments with paper money or the U.S. free banking system with decentralized creation of private moneys). Banking organizations, in their current form, have some of the most rigid and hierarchical internal control structures in the sense of Coase

(1937) within the universe of firms across all industry sectors. Centralization in finance reflects the broader trend exhibited in history where centralized societies had competitive advantages, notably advanced technology, in the accumulation of resources and increase in population relative to less centralized societies (Diamond 1997).

Both cash and banks have been successful in reducing transactions costs from the point of view of an individual transaction. Cash that is legal tender is guaranteed to be accepted in payment of debts towards the state. This ensures the use value of modern cash that is only a symbol or token and cannot be consumed (Kyotaki and Wright 1989). Cash has reduced the need for parties to a transaction to spend time and effort to inquire about the acceptability of a means of payment and store of value.

The case of banks is more complicated. On the one hand, banks are highly sophisticated, internally diversified firms that carry out a myriad of financial services and transactions inside their business control structure (Diamond 1984). They also interact with markets at many different points during this process. In the early days of banking their positive effect on transactions costs was quite obvious as communication and search was prohibitively expensive for an investor seeking alternative business opportunities beyond her local area (of residence, or existing economic activity). Banks were centralizing, matching, netting funding, and investment already when Marco Polo returned from his excursion to China with first specimens of paper (fiat) money. They have done so ever since, and their business model has not changed too much between the Italian banks of the 1400s and commercial banks of the 1930s.

In the meantime, elements such as deposit insurance, lender of last resort funding by central banks (i.e. the government just as in the case of deposit insurance), and more recently the acknowledgement that some financial institutions are too big to fail have complicated the assessment (Philippon 2012; Bai et al. 2014). While the marginal transaction may still benefit from the capacity of modern banks to bundle complicated financial services for a client, it is less certain that the net benefit for society is positive under all circumstances. Indeed, Davies and Tracey (2014) find that once implicit subsidies are taken into account, economies of scale largely disappear, i.e. a bigger balance sheet is no longer associated with lower costs of financial intermediation. As a starting point for our discussion we can take it for granted that these implicit subsidies exist and are substantial.[1]

The development of FinTech and, more generally, P2P technologies intended to simplify the financial system, particularly Blockchain technology and associated smart contracts, have the potential to reshape the costs of transacting in the financial system. Moreover, the development of *a P2P legal contracting system*, backed by a combination of Blockchain and smart contracts can dramatically change how all the stages of

[1] It is noteworthy, while we do not discuss market structure here, that implicit subsidies lead to falling average costs in a large portion of banks' production function. On those portions new entrants will not only face the hurdle of getting new ways of doing things accepted, but they may actually be unable to compete with the incumbent once the latter has eliminated, after some initial successes and growing market share of the newcomers, inefficiencies that may have accumulated over the years (Roberts 2004).

contracting would happen, and can be expected to have the potential to disrupt the current business model of some of the most profitable and established financial services firms including in areas such as investment banking, clearing and settlement, accounting, auditing, etc. Such a restructuring of transaction costs by P2P technologies would recall the effects that the printing press and self-enforcing Protestantism had on trade and economic growth in 16–18th century Europe. In the present chapter, we try to explore the potential effect of P2P financial technologies on the financial system using this historical precedent to structure our mostly theoretical discussion.

Our discussion proceeds as follows:

In the Sect. 1, we review the literature on institutions reducing transaction costs as an input for economic development. As part of this review we consider an original Weberian contribution to this literature: Blum and Dudley (2001) suggest that a strong negative shock to the cost of contract enforcement in the Protestant parts of Europe between 1500 and 1750 can explain the otherwise counterintuitive acceleration of economic growth in Northern Europe compared to a better capitalized Southern Europe.

In Sect. 2, we discuss how Bitcoin and Blockchain-based transaction technologies, and more generally a legal system designed for the Internet, could alter transaction costs. It is true that many activities attached to financial contracts have not seen falling transactions costs, quite the contrary: legal advice, clearing and netting of contracts, disclosure of contractual information, auditing of contracts, legal reporting requirements are areas where costs have stayed steady despite significant progress in ICT's. Some authors go even further suggesting that transaction costs per unit output of the financial sector have actually increased (Philippon 2012), and that using the financial system has become more expensive over time even if overall informational efficiency has increased over the last half century (Bai et al. 2014).

In Sect. 3, we discuss how a stepwise agent-based modeling approach could be developed based of a model by Kiyotaki and Wright (1989) where a medium of exchange emerges endogenously and is held in equilibrium mostly due to its favorable impact on transactions cost. The model is simple, elegant, and a good point of departure for thinking about financial institutions from a transaction cost perspective. A modeling strategy for future agent-based models could then consist in relaxing step-by-step the strong rationality assumptions in analytically solvable models with two or three representative agents; more granular, bottom-up agent-based models could be particularly helpful to better understand the impact of P2P transaction technologies.

A couple of points should also be made with respect to the analytical strategy that is used in this chapter and how we perceive the relative roles played by financial firms, trust and transaction costs. Financial firms revolve around and depend on the concept of trust.[2] Trust comes in many different forms: trust in the persistence of the status quo, trust that contracts will be honored in different contexts with either the third party being a frequent partner in the exchange or a

[2] Duffie (2010) argues that the failure mechanics in a banking crisis are all the more non-linear since large banks will use way beyond any point of ex-post optimal behaviour all the flexibility they have within their group's internal control structure to protect their reputational capital.

complete stranger involved in a one-off transaction, etc. What type of contractual relationships and their degree of enforceability will be reflected in a particular level of trust? What kind of social, political, or economic institutions have come to embody varying levels of trust?

Transaction costs could provide a link between these questions: transaction costs can help quantify the required level of trust for a particular financing operation. Transaction costs can help to compare different forms of contracting, a comparison that would otherwise remain largely phrased in qualitative terms. Transaction costs can help explain a substitution of a prevailing set of institutions by new ones especially if it can be shown that these new institutions bring about a reduction in transaction costs for at least certain types of transactions.

We will thus apply the following logic in what follows: trust can be constructed in various ways, in financial transactions it lowers, *ceteris paribus*, the cost of transacting. Transaction costs can be higher or lower for a variety of reasons, including available technology. Lower transaction costs increase the likelihood of a transaction taking place in the same way as higher levels of trust do. To assist our reflection on the future of money and banking we are thus looking for models that aim to explain the evolution of financial transactions via different levels of trust. Alternatively, we are looking for models that explain the adoption or the emergence of financial institutions via differences in transaction costs.

## 2 Institutional Theory

Modern economic theory has often worked with models of a frictionless world with zero transaction costs. In reality, transaction costs are substantial, and societies have struggled to bring these down. Ultimately, various institutions emerged (including financial institutions) to bring down transaction costs with differing levels of efficiency. Institutions are “the rules of the game in a society or, more formally, are the humanly devised constraints that shape human interaction” and they have the effect of “structuring incentives in human exchange, whether political, social or economic” (North 1990: 3). By limiting the range of human behavior they reduce uncertainty and therefore the cost of interaction, or transaction costs. How exactly institutions reduce these costs is very important to the ultimate efficiency of institutions in providing a framework to structured exchange. This requires a look at the nature of transaction costs and how they relate to property rights.

### *2.1 Property Right Regimes*

Property rights are key to the functioning of an economic system as they represent “the rights individuals appropriate over their own labor and the goods and services they possess” (North 1990: 33). For exchange to take place “individuals potentially interested in the asset must possess full knowledge of its valued attributes" (Barzel 1997: 7). However, due to the complexity of the environment and the cognitive limitations of individuals, it is costly to ascertain and document the actual value of the resource. In short, there are transaction costs associated with altering *and* maintaining the integrity of property rights. Formally, transaction costs are defined as the "costs associated with the transfer, capture and protection of rights" (Barzel 1997: 4). If the transaction costs are too high "exchanges that otherwise would be attractive may be forsaken" (Barzel 1997: 5)

There are three dimensions to transaction costs: (1) definition and manufacturing, (2) monitoring and (3) enforcement of contracts. These dimensions exhibit a close analogy to the three stages in modern financial banking intermediation as they roughly correspond to (1) underwriting and manufacturing of financial instruments, (2) monitoring and screening credit and market risks to the value of contracts, and (3) enforcement/execution of (financial) contracts.

*Defining* property rights is the first step to exchange and is necessary to know the "value of the different attributes lumped into the good or service" (North 1990: 29). Finding the value is itself a costly process which is never perfectly defined, because of the diminishing returns to being fully informed. In the case of certain assets, for example personal information, establishing the exact value of the asset is made more difficult because of its intangible nature.

*Monitoring* the asset is important as an individual only owns the right to a resource to "the extent to which an owner's decision about how a resources will be used actually determines the use" (Alchian and Demsetz 1973: 17). If some of the valued attributes of the asset can be exploited by others, the owner has a decreased incentive to invest further, thus decreasing the productive capacity of the asset.

The final part of transaction costs is *enforcement* which is important as a deterrent and a means of restitution if the rights of the owner are violated. Enforcement is of crucial importance to the operation of a stable and functional property rights system. In the absence of fair, transparent, rule-driven and consistent enforcement, an individual would have little reason to think that the other party to an exchange would not renege on their contract, thus discouraging exchange.

So institutions are efficient at providing a framework for cooperation and coordination to the extent that they are able to reduce the transaction costs associated with either defining, monitoring, or enforcing property rights.

## *2.2 The Enforcement Mechanism*

The precise nature of the enforcement mechanism is of particular importance. It defines how credibly the institutional arrangement can ensure compliance and commitment. The enforcement mechanism does this by raising the cost of defection which can be either pecuniary or psychological, or a mix of both as in the case of insolvency proceedings that imply a gradual and increasingly severe restriction of the property rights of one party to an exchange.[3] Institutions can be separated into two categories according to the structure of their enforcement mechanism, informal institutions that are “not sanctioned by formal mechanisms” (Kasper and Streit 1998: 106) and formal institutions whose “sanctions are implemented in an organized manner by some member of society” (Kasper and Streit 1998: 106).

Before going on to analyze how these institutions function, it is important to note that the definition, monitoring and especially enforcement of property rights all display the characteristics of a public good. Public goods, as argued are typically underprovided because of the collective action problem (Olson 1965). This is instructive in understanding how societies evolve from being governed primarily by informal institutions before shifting to formal institutions.

## *2.3 Informal Institutions*

Most human interaction is governed by informal institutions. Informal institutions are the sum of “socially transmitted information and are part of the heritage we call culture” (North 1990: 37), ranging from codes of conduct to norms of behavior. Enforcement in informal institutions can be either self enforcing or enforced via a decentralized mechanism.

Self-enforcing informal institutions can be broken down into two categories. The first are those rules that are self-enforcing because they are in alignment with individual self interest. Individuals follow the rules of the road in the interest of self preservation. Informal institutions can also be self-enforcing when they have been internalized by individuals to form part of their utility function. Religion, culture, and values are informal institutions, which, if deviated from, impose a psychological or social cost on the individual. Shared, internalized informal institutions reduce uncertainty by making individual behavior predictable. This decreases transaction costs and increases the likelihood of cooperation.[4]

Informal institutions can be enforced by decentralized acts that arise spontaneously from members of a group (Greif 1993). It is not the task of a specific actor but instead is assumed on an ad hoc basis by random members of the group. The rationale behind individuals spontaneously taking it upon themselves to define, monitor and enforce rights, is their interest in preventing the erosion of their

[3] Martin Shubik once compared the restrictiveness of bankruptcy rules to the gas throttle of the economy, a less restrictive bankruptcy rule allows more risk taking, but will eventually hurt overall trust in (asset) valuations; Diamond (1984) discusses the role of bankruptcy in conjunction with debt contracts as an effective means to enforce contracts within the financial sector, and Myers (1977) has argued that a growing discomfort of management to face insolvency proceedings puts an upper bound on the firm’s financial leverage.

[4] As Coase (1960) famously observed, in the complete absence of transaction costs, all beneficial exchanges would take place irrespective of the allocation of property rights; this famous link between institutions and transaction costs has certainly been one of the reasons why Coase’s article is by a very large margin the most cited economic theory paper of all times.

institutions which provide a basis for cooperation. Integral to these informal institutions are reputation systems and social knowledge. In groups, individuals have information about the other members of the group based on past interactions. The smaller, denser and more homogenous the group, the faster information related to reputation travels. This enables individuals to ascertain the risk of dealing with another individual. Defection from the accepted institution is dis-incentivized by damaging the reputation of the offender (thus making it harder for her to find other trading partners) and by the resultant ostracism from other members.

However, when a society grows in size and complexity, informal institutions are less effective at providing a framework for cooperation and coordination. Self-enforcing institutions that rely on a common culture to align expectations become weaker as the society becomes more heterogeneous, raising uncertainty. Exhibiting the characteristics of public goods, socially decentralized enforcement also begins to fail as individuals are unable to overcome the problem of collective action and free ride on the contribution of others. When systems of kinship and clan are superseded by larger more complex societies, this gives rise to impersonal exchange where "transactors are previously unacquainted, they are unlikely to transact again, and information about the activities of either is unlikely to reach others with whom they might transact in the future" (Granovetter 1985: 490).

## 2.4 Formal Institutions and Contracting

To reduce uncertainty in trustless exchange and "to capture the gains from trade in a world of impersonal exchange [institutions] must be accompanied by some kind of third party enforcement" (North 1990: 57) to overcome the collective action problem and ultimately provide a productive incentive structure. Moreover, societies "increasing complexity…. naturally raise[s] the rate of return to the formalization of constraints" (North 1990: 46) which becomes increasingly easier with technological innovations like the printing press that lower the costs of formalization.[5]

Formal institutions are rules that govern behavior that are credible because they are enforced by a third party agent. Third party agents are 'organizations' defined as "groups of individuals bound by some common purpose to achieve objectives" (North 1990: 5), which are able to overcome the problems related to collective action by better aligning the incentives of their members. Judicial systems have been important institutions for societies evolving over time from informal institutions based on culturally transmitted rules, to formal institutions where agreements are formalized using contracts enforced by the state. Societies that manage to formalize agreements via third-party enforced contracts at lower costs experience stronger economic growth.

[5] In ancient Persia, reflecting very high costs of documentation on durable storage media, famously the only written formalized agreements were peace treaties and tax rules.

Contracting in formal institutions greatly reduces uncertainty compared to the ad hoc mechanisms used in informal institutions. However, this comparative advantage depends on the third party agent reliably performing the function of enforcement. To do so effectively, it is important that the third party agent enforces and administers the rule-set impartially and consistently. Failure to do so negates the productive effects of institutions by inserting uncertainty in a crucial aspect of the institutional logic. As Escosura and Villaroya (2009) found in Argentina, when the third party arbitrarily and inconsistently enforces contracts complex exchange proves to be costlier because uncertainty over the exact outcome of contract enforcement is too high.

The risk of third party organizations being compromised and exploiting their relative position of power lies in the opportunistic nature of individuals and imperfect information about their behavior. This brings us to one of the fundamental concerns of political science, the question of "*quis custodier ipsos custodes?*" or "who will guard the guards themselves?". This is the paradox of governance—an agent intended to protect and enforce the rights of a society has to have the capacity to do so, but in doing so also has the power to violate the very rights that it is meant to protect. Formal institutions function best when there is a credible commitment that the external agent will not behave opportunistically (Weingast 1995; Cukierman 1994).

Fundamentally, the benefits of formal institutions over informal institutions, notably the potential for complex exchange via extensive contracting, are existent only to the extent that the third party agent can be *trusted* to be *fair*. If the third party abuses its position of power it will hurt the efficiency of the very institution it is meant to enforce. Informal institutions are less subject to this vulnerability, but are inefficient at providing enforcement *at scale* or in *complex exchange*, making exchange remain at comparatively simple levels of sophistication also referred to as "poverty trap" in the literature (Capra et al. 2009).

## 2.5 Technology, Transaction Costs and Institutional Change

However, technology can alter the structure of transaction costs thus altering the dynamics of the institutional matrix. The printing press, for example, decreased the cost of information search and propagation (Eisenstein 1979); so did the Internet, and both technologies decreased the cost of mobilization and coordination of actors, as well. Blockchain technologies could again alter the structures of transaction costs in a significant way along all three dimensions discussed above. This should be expected to have implications on the complementary nature of formal and informal institutions that are necessary to provide strong governance whilst reducing the potential for third party risk. Blockchain institutions provide the formalization associated with formal institutions, with the decentralization associated with informal institutions. North's typology does not entirely encompass this matrix of complementary characteristics which suggests the formation of a new type of institutions—one which could have significant impact on governance and, potentially, economic growth.

### 2.6 *Transaction Costs in History*

Blum and Dudley (2001), combining approaches from endogenous growth and evolutionary game theory, elaborate on Weber's famous argument that the "[Protestant] Reformation created the decisive momentum for economic development in northern Europe by modifying contractual relationships among believers" (Blum and Dudley 2001: 11). Catholics believed their sins could be forgiven by a priest which was reflected in their economic behavior by a greater number of defections in contracts, as the *cost of defection* was comparatively *low*. In contrast, for members of "Protestant sects, the hedonic cost of defection was high" (Blum and Dudley 2001: 2) because Protestants did not believe in the Catholic sacrament of penance effectively meaning that the cost of defection was higher. This is a good example of how internalized rules can govern behavior and reduce transaction costs.

Much in the same vein, the issue of establishing trust in a financial transaction without the intervention of a central authority is in the context of an option contract described in Christopher Marlowe's version of the Dr. Faustus theme. Writing in England at the end of the 16th century, Marlowe obliges his Dr. Faustus to pay his dues after 24 years of almost unlimited power and goes to hell *instead* of accepting the offered sacrament of penance. Marlowe's Faustus, in contrast with the German original and the much later versions by Goethe and Mann, rules out any possibility of deviation from the established contractual terms. Thanks to Faustus' self-monitoring behavior, the contract becomes quasi self-enforcing, thus reducing the cost of enforcement to zero. Dr. Faustus is of the opinion that formal contractual terms matter *more* than the social status of the contracting parties, a revolutionary idea at the time. As a result, the formal contract can establish trust vis-à-vis any (arbitrary) third party. Marlowe's option contract is nothing else but a precursor of the self-executing smart contract that will be discussed in the next section.

## 3 P2P Technology and Transaction Costs

In this section we discuss the potential impact of P2P technologies on transaction costs. We place Bitcoin and Blockchain in the context of open source technologies, including an open source approach to text, called *Common Accord*.

Newly emerging P2P technologies are innovative in combining and leveraging existing technologies such as the Internet and algorithmic encryption techniques, opening up new ways to reduce transaction costs. E-commerce and email are two Internet based applications where transactions costs have been noticeably lower than in their physical world equivalents. For instance, systems such as eBay reduce the cost of propagating information about offerings and the reputation of sellers, as well as automating many elements of the transactions (eBay also spawned a large and partially automated dispute resolution system, *Modria*.) But these systems still depend on a *hub* dominated by a single organization (eBay and Amazon for instance).

P2P technologies are transformative (in addition to innovative in a combinatorial sense à la Schumpeter) because they are "hubless," which is to say that any participant can become a hub for any activity where he/she is able to add value for other participants, while maintaining low switching costs. It is useful to mention "Git" at this point, an open source distributed version control system for the creation of software. It permits full traceability of the history of materials, flexibility to modify, and privacy of use. In its more social uses, notably as hosted by GitHub, it allows sophisticated participants to find resources, evaluate reputations and collaborate, reducing the cost of collaboration. Git has been an important factor in reducing the average size and capitalization of technology companies. We anticipate that P2P payments and a systemic approach to legal text will have similar impacts on banking and finance.

## *3.1 Bitcoin*

Even though Git allows nearly frictionless collaboration it does not solve the double-payment problem. Nor does it provide a mechanism for rewarding maintenance of the infrastructure. Bitcoin emerged as a uniquely innovative single-purpose system that solves these two issues.

Bitcoin is a system that allows users to securely store and verify information publicly in a dynamic chain of data that is distributed amongst nodes in the network. The network is secured through a competitive process called "mining", where miners are incentivized to process transactions in exchange for bitcoins, a digital token whose value has increased considerably. The system is created so that once data is embedded into the Blockchain it becomes immutable unless the actor that wants to change the Blockchain controls a majority of the processing power of the network making it resistant to change (the so-called "51 % attack" remains Bitcoin's greatest vulnerability). Any change to how the Bitcoin protocol operates must be made by consensus, meaning that a *majority* of miners must agree on the changes being put forwards. The technical breakdown of how the Blockchain functions and is secured is explained in Nakamoto (2008).

Bitcoin has limitations. First, it is a special purpose protocol. While it is successfully used to create a non-falsifiable record of a broad range of events, it's ability to automate more complex transacting is very limited. Second, it can process only a very limited number of transactions, and involves a large time latency before an event is confirmed as permanent. Third, the incentive system depends on wasting electrical energy to solve cryptographic puzzles. This waste of electricity is inherent to the system; the economic incentive is based on the cost of computing. Fourth, while the identities of persons can be masked by encryption, the validity of the transaction depends on the record being integrated into the public record which is shared by all participants. A breach in the mask reveals a person's transaction history. Fifth, a change to how the Bitcoin protocol operates must be made by consensus, meaning that a majority of miners must agree on the changes being proposed. Bitcoins' *resistance to change* can be seen from the ongoing debate relating to the scalability of the network. Despite most people being in agreement over the need for certain changes in the system to allow it to grow, certain technical and governance issues have prevented a consensus from emerging.

The most obvious use of bitcoins is as currency. Indeed, the white paper first describing the Bitcoin network that was published by the figure Satoshi Nakamoto is entitled “Bitcoin: A Peer-to-Peer Electronic Cash System” suggesting that this was the intended purpose for the system. Money is meant to have three key characteristics (1) store of value (2) unit of account and (3) medium of exchange. In this respect, the volatility of the price of bitcoin hinders its use as a medium of exchange although there has been modest improvement in this respect. Instead, bitcoins are used primarily for speculative purposes for the time being. A significant advantage of bitcoin as cash is that individuals control their own moneys. This is an important attribute in many societies where banking institutions are not trusted. However, some have argued that bitcoin as money is fundamentally flawed because of the traceability of transactions. This reduces bitcoins’ fungibility, an attribute that many deem key for the function of money. In terms of existing categories, bitcoin is clearly not a fiat money, but it does not correspond fully to commodity money either; this difficulty of agreeing on its attributes continues to make its regulation cumbersome and uneven across jurisdictions which in itself is a major obstacle for its marketability.

## *3.2 Blockchain*

At its most fundamental level, the Bitcoin Blockchain is a shared, auditable platform with formalized and unbreakable rules about how transactions must take place. This platform is open to all the parties, cannot be censored and most importantly has no need for any intermediary or third party to process and validate transactions. From a theoretical standpoint, this presents an important development. The need for third parties to provide credible enforcement has been necessary for the formalization of contracting, but the Blockchain can partly remove the need for a third party for many types of transactions thus changing how institutions function.

In the past year a cleavage has emerged within the ‘Cryptocurrency’ community regarding the function and value of ‘permissioned’ and ‘permissionless’ Blockchain’s (Swanson 2015). In the context of Bitcoin, the Blockchain is the distributed public ledger that holds a record of all the transactions that have occurred in the network and that is secured by the miners. The Blockchain is distinct from the tokens, bitcoins, that are used to incentivize the miners to participate in processing transactions. This distinction between Blockchain’s and bitcoins has led many to identify the Blockchain as the object of value in the network. The Bitcoin Blockchain is permissionless in that any entity can decide to participate in the network either as a user or as a miner. However, permissioned Blockchain’s have also been developed, sometimes called private Blockchain’s, where the creator of the Blockchain in question designates who can participate in the network and in what capacity.

When thinking about how Bitcoin and Blockchain’s could impact the financial system, this dichotomy between permissioned and permissionless Blockchain’s is important. Although there is disagreement amongst the two camps regarding the merits of the different types of Blockchains, many have argued that they serve different purposes. The Bitcoin Blockchain offers a secure ledger due to the significant hash power expended on mining but this also makes it costly to run and inflexible. On the other hand, permissioned Blockchains are less secure but are less costly to run, and can provide much more flexibility in their design. Permissioned Blockchains have been developed by various companies and several large banks are developing their own private Blockchain solutions. One notable development is the creation of a consortium of banks and the private Blockchain company R3Cev, with the aim of developing private Blockchain solutions for trading, settlement and general automation of their business processes. Another is the creation of a consortium under the Linux Foundation bringing together many major actors. Payments and transacting join Linux, Git and other codes, as part the open source dynamic. It seems likely that many different types of Blockchains will exist, with differing characteristics according to the needs of their designers and users.

As the ecosystem matures, the use cases of Blockchains continue to increase far beyond mere financial applications. Blockchain solutions are being developed in many different industries for diverse reasons ranging from fraud protection, the lowering of transaction costs and fees, or the reduction of counterparty risk. Examples of these development can be seen in the insurance industry, digital content management platforms, distributed file storage, real estate or digital identity to name but a few.

## 3.3 Smart Contracts

"Smart contracts," refer to modules of computer code that run on Blockchains. They can be programmed to transfer tokens of value, enable access to resources or otherwise automate functions based on conditions. They are self-executing, like other software code, but also shared among the parties and cryptographically verifiable. The phrase "smart contracts" has led many to confuse them with "contracts" in a legal sense. Smart contracts are *automation*, not law. They perform functions like ordering, payment and scheduling that are common on bank and merchant websites. These contracts range in complexity, from simple bets, to complex financial instruments. Smart contracts can bring much, eventually perhaps all of this supplier-dominated automation and intermediated marketplaces into the open source dynamic. Because the automation is shared, it can become harmonized and keep improving continuously. The frictionless nature of the mechanisms permits complex mechanisms to be used at almost no cost (and basically at zero *marginal* cost). These possible use cases include enforcement and governance mechanisms such as escrows, voting, and eviction. The shared nature and sharp definition will also permit rapid institutional and organizational learning about optimal contracting and transacting. The lowering of transactions costs related to the creation of complex contracts could allow for more iteration and eventually efficiency in contracting. If the logic of the previous section carries over one could also expect that many currently missing markets can be completed using appropriate automation (and its inherent standardization).

The combined use of the Blockchain and smart contracts creates a platform where individuals can exchange, manufacture and execute contracts with considerable sophistication and with little cost. This innovation could turn the economics of institutions on its head.[6] Such a system would combine characteristics of formal and informal institutions. The fact that automation can provide credible commitments to parties makes them resemble informal institutions in that no third party agent is required to provide the enforcement function. On the other hand, such systems have attributes of formal institutions, notably the formalization of contracting—the definition, monitoring and enforcement of contracts. In such systems, third party enforcement becomes largely redundant as individuals could contract with each other on a voluntary P2P basis, with an impartial and predictable enforcement technology taking away counterparty risk.

## 3.4 Inefficiencies of Legal Documents

While many kinds of high volume transacting have been *automated*, and the great majority of transacting takes place without reading a legal document, not all have been *digitized*. Most transactions are covered by documents such as "terms of use", "terms of sale" and privacy policies which are opaque to most users and invite abuse; all this legal documentation continues to run on a paper standard, or unstructured data, as opposed to a digital, or algorithmic standard that can not only be processed by machines, but allows full automation and machine interoperability. There are also important fields of transacting which take place by exchange of word processed documents.

Legal documents continue to suffer from enormous inefficiencies in their creation, review, management and enforcement. The costs of re-creating and reviewing legal texts are well documented (Wickelgren 2011). These inefficiencies are a major reason why the cost of contracting has remained stubbornly high more than two decades after the start of the ICT revolution.

Word processing in the legal industry has come to be dominated by a proprietary software solution and a complex data model. Indeed, the data model is so complex that it has proved difficult for competitors to create tools that are fully compatible. The networked nature of legal transacting means that most actors stick with the dominant solution. Of course, word processing is *incompatible* with peer-to-peer automation. Various efforts are being made to format legal documents in ways that are compatible. Worse, the word-processing data model has inhibited the kind of

[6] Curiously, extrapolating this potential, P2P technologies could bring us in a not too distant future arbitrarily close to the vision of complete markets spelled out by Arrow and Hahn (1971), the criticism of which originally led to the emergence of the institutional economics literature. A logical circle would thus be closed.

iterative improvement and sharing of knowledge and work that has made open source software drafting so successful.

## *3.5 Common Accord*

Common Accord is a system that has adapted the tools and methods of open source software development to legal documents, with the aim of codifying the documents of law into a shared code of legal transacting. These resemble wikis, can be handled in git, and can be "forked" or adapted for each jurisdiction, language or industry thus making law *modular*.

Contracts are roughly described as "the law of the parties." Legal systems broadly respect contracts as party-defined law and will interpret them to prevail over background law across a broad range of issues. The expansion of contract boilerplate over the word-processing era reflects a kind of peer-based decentralization of the law which creates considerable inefficiency when done as word-processing, but can contribute to decentralization in automated transacting.

There are advantages of an open source approach to the creation of legal texts that can even exceed those for software. Legal text is not "objective" or "deterministic." It does not "run" on a machine. It depends on language, culture, institutions, the quality of advocacy and decision-makers. Codification greatly reduces uncertainty by socializing text. It can come to have shared meaning through use, interpretation, commentary and custom. In other words, a system like Common Accord could prove a key step in making law a common good, which because of the reduction in transaction costs associated with its open source production could be more inclusive, thus gaining legitimacy.

This poses the question of the economic incentives to contribute. The search for lower transaction driving through automation happening in banks and other financial firms could also drive the digitization and codification of legal documentation. In addition, there is a long tradition and important institutions that already collaborate on legal codification: regulators writing rules, institutions dedicated to codifying the law, lawyers collaborating on model (or master) documents, or companies codifying their own practices reflecting the fact that automation and consistency advantages of a codified approach can be captured even by a single firm. The use that follows is "viral" since a firm necessarily shares its "code" with its partners (Triantis 2013). For finance, there are notable possibilities for codifying new or existing products and for codifying compliance and reporting.

For the converging peer-to-peer transacting platform, Common Accord provides a way for legal texts and the legal system to interface with smart contracts, extending the reach of automated transacting to the full range of legal relationships. In this way, peer to peer transacting platforms would not only be self-enforcing through the use of smart contracts, but also legally valid and binding.

### 3.6 Banking and the Financial System

Bitcoin has demonstrated that a transaction system does not need a hub. Whatever its future, it is a proof that solutions exist for hubless peer-based transaction systems with the following characteristics, (1) reliable shared records, (2) anti-double-spending and (3) incentives for maintaining the system.

P2P transacting platforms that incorporate Blockchains, smart contracts and open source legal text management systems could create a paradigm where contracting parties no longer need to pass through intermediaries to exchange. Blockchains would offer a secure and non corruptible platform where smart contracts could be automated and agreements entered upon. An open source legal text management protocol would ensure that these transacting platforms operate within the remit of applicable law. Such a paradigm would benefit from significantly lower transaction costs then exist today in the financial system.

The financial system and the banking system will be affected at many levels. Peer-based payments threaten many repeat revenues. Uniform interfaces and codified documents will reduce costs and transaction cycle times. They will also facilitate new entrants and allow customers to be more mobile. The improved record-keeping will make banks easier to audit. Handling text as source code will enable collective sourcing of regulatory compliance materials. It will enable regulated entities to demand consistency from regulators via shared texts.

## 4 Modeling Transaction Costs and Financial Institutions

Could we formalize these discussions in a way that would allow hypothesis testing or simulation of the impact of different technologies on society's transactions costs problem? Money as a social institution has been very difficult to integrate into the mainstream neo-classical model of (complete) competitive markets.[7] In the Arrow-Hahn (1971) formulation a good without consumption value in equilibrium is priced at zero and its stock is forced to zero as well. The model of Kyotaki and Wright (1989), hereafter KW, is a good starting point to think about such formalization. In their approach the institution of money emerges as the solution to a problem of costly search for randomly matched parties to a mutually beneficial exchange. This places their model in the realm of anonymous exchange. One the one hand, their model contains strong assumptions about enforceability of contracts (rule of law) and the role of the state (and hierarchically organized authority and/or trust more generally). On the other hand, their model is kept simple from an analytical as well as topological point of view. As a result, it blurs the distinction between transactions costs and network effects when discussing the benefits of

[7] See Shubik (2001) for an excellent, non-technical overview.

emerging or state-induced financial institutions. But it is precisely for these restrictions that it is a good starting point for our present discussion.

In KW a speculative transaction demand for money emerges in a simple setting that is characterized by a generalized absence of the double coincidence of wants. Agents have to care about two things when maximizing expected consumption: first, the likelihood of being able to trade with agents that hold their preferred consumption good, and, second, storage cost.

Total (social) transactions costs in this economy are therefore the sum of storage costs at any point in time. Thanks to differences in storage costs, there will also be trade in some cases where only one agent receives her preferred consumption good, and the other agent accepts a non-preferred good in exchange and can lower its storage costs and/or increase her likelihood to trade in her preferred consumption good in the future. In a second step, KW introduce fiat money, which simply has the dual property (1) to dominate all other goods in terms of having lower storage costs, and (2) of not being consumable. Fiat money is dropped from the proverbial helicopter, i.e. there is (implicitly) a central authority controlling the money supply.

It is worth noting that in this simple economy with three types agents and three types of consumption goods, without fiat money there are nine situations where agents are matched without trade and twelve matches with trade. With fiat money, there are nineteen matches without trade and twenty-six matches with trade. The likelihood to be in a trade increases, but fiat money does not add any further instances of a double coincidence of wants. As a result, even if the likelihood to be in a trade increases, the same cannot be said about the likelihood to consume, since part of the additional trades will only *lengthen intermediation chains*. Increasing the likelihood to trade (increase market liquidity) *and* the lengthening of intermediation chains has been a central dual feature of *financial innovation* until recently.

However, the likelihood to trade is only one element on the way to final consumption. What matters in the end if how much consumption takes place in the aggregate, i.e. the level of social well-being. Perhaps surprisingly, the introduction of fiat money in the KW model is *not* unequivocally welfare enhancing. It turns out that too much money lowers consumption. Indeed, there is an optimal amount of fiat money. Commodity monies can circulate in parallel, but they are crowded out as use of fiat money increases. As a result, the KW model points to a potential severe issue of a prisoners' dilemma: due to the favorable storage costs, it is individually optimal to accept fiat money in an intermediate exchange; if money growth is not capped, money will eventually crowd out final consumption.[8]

Let us summarize KW's results: in their search-theoretic motivation for the emergence of a means of exchange KW derive a speculative demand for both

[8] A KW economy with privately provided fiat money is inexorably driven towards its only (Nash) equilibrium in terms of individual trading strategies where no trade will take place because all trading partners have fiat money in stock to be swapped against their preferred consumption good. KW do not discuss this point, but we mention it here as a side remark and hint towards the discussion on the limited money supply in the case of the digital currency bitcoin.

commodity money and fiat money. However, even in this simple setting, agents are presumed to have substantial knowledge about the overall economy: KW presume that the distribution of agents producing a particular good is known ex-ante, a stark deviation from Adam Smith's anonymous market exchange with a spontaneous organization of the division of labor the parameters of which are ignored by individual participants. The stochastic process that matches agents (potential trading partners) is also fixed in the KW model, i.e. agents thereby know the structure of the economy, they have rational expectations. On the other hand, while knowing quite a lot, they are not given any *choice* in the presumed optimization (which is the agents' consumption technology) and thereby agents' are trapped in the prisoners' dilemma once fiat money grows beyond the socially optimal amount.

Finally, and most interestingly for the discussion in this chapter, the storage costs of the commodity moneys and of fiat money are given and not determined endogenously. But what do the two types of money do in this setting after all? Commodity money emerges endogenously; agents like to hold it because of its marketability and its convenience (such as lower storage cost). The supply of commodity money is limited by the amount of agents in the economy producing it. It has no consumption value to its holder, but it has consumption value for other agents in the economy. Now compare this to the centrally provided government fiat money. Again, it has no consumption value for its holder, but nor does it have value for any other agent. In the KW model its supply is fixed, its marketability and convenience properties are simply defined to be superior to commodity money.

To arrange our discussion and arrive at the same time at a visual representation of our argument that transaction cost is a crucial concept in thinking about how Internet-based technology can be expected to re-shape financial intermediation, we propose a simple, highly stylized modeling approach. It has a simple structure which through iteration allows for genuine complexity to emerge. Similar modeling approaches have been used in studying (1) the impact of additional information on agents' capacity to correctly forecast an external financial signal, or (2) how different forms of interaction between agents facing a similar learning/optimization problem allow improvements of individual and group performance. Consequently, such models have been termed "learning to forecast models". They can typically be implemented using agent-based computational modeling, or experimental economics.

Take the example of an agrarian economy where the individual agents are very small. They produce a highly standardized product (such as corn), and because they are small compared to the market the price established on the market is an external signal. The production (cost) function is given as well (at least in the short run), and hence the only variable that will determine if our agent can achieve an excess over (production) costs is the deviation from the expected price at which she will be able to sell her output. Early financial technology will likely consist of a set of rules of thumbs, or, if there are historical or seasonal patterns in the data, a slightly more sophisticated time series model (calendars established over long periods of time and used in agriculture are exactly that).

Once agents start using different financial technologies, they create track records of how successful they were in guessing the external signal. The ensuing capacity to consume can typically be observed by their peers. The variance that is now observable allows for a further development of financial technology. An agent can exploit the variance of individual strategies and their associated consumption streams and provide model-based forecasts of the external signal. If the data-generating process that governs the magnitude and variance of the external signal is sufficiently stable, such a model-based analysis can outperform the rules of thumb based on agents' own experience or that of their immediate neighbors. The agent using the statistical model may choose to provide a financial service to other agents but its capacity to do so is strictly limited by a number of cost factors.

The signal to be guessed could be quite frequent in this case, e.g. a broad index of the U.S. equity market like the S&P 500. Switching costs are likely modest, but it remains non-trivial to determine when it actually makes sense to switch the forecasting strategy. The example could also represent a commodity futures market situation. Here, the cost of observing the evolution of prices takes center stage as the market is already locking in the price of the commodity at a specific future date. The farmer at the start of our example can now decide how much to produce and substantially reduce (expected) costs.

### *4.1 A Step-by-Step Modeling Strategy to Explore the Relative Importance of Transactions Costs for the Emergence of Financial Institutions*

The discussion of the KW model motivates the need to go to a bottom-up approach (De Grauwe 2010) and let institutions that can reduce transactions costs emerge (and disappear) as a (historical) result of economic exchange (the trodden path mechanics). In a first version of such a bottom-up modeling approach agents could have only local knowledge about consumption as they can observe their own consumption as well as consumption of a limited number of neighbors (in a physical space). Using simple heuristics to forecast a crucial economic signal (such as aggregate consumption opportunities (GDP) or any proxy for it which could be the weather in an agrarian economy (amount of rainfall, etc.) agents try to improve their well-being by keeping forecast errors within an acceptable range. They can copy heuristics of their neighbors once it is observed that a neighbor fared better, on average, using a different heuristics (rule of thumb). If transactions costs allow, an agent who has been relatively successful (and as a result her forecast heuristics has been adopted by a number of other agents (a number to be defined, implies assumptions about available communication technology) can decide to produce a centrally provided forecast.

In such a first variant of an agent-based computational model, the consumption history of the central agent could be observed by all other agents in the economy simultaneously. Depending on the frequency of the signal this situation could correspond to various technology shocks: printed documents that can be transported and/or reproduced at low cost, international sea trade, the arrival of the transatlantic cable, modern exchanges for stocks, commodities, and financial derivatives, etc.

What is crucial here is absence of a peer-to-peer network since there exists a local shared knowledge about the forecasting technology, but this knowledge remains local.

The central agent has to bear some fixed cost (fees for being listed on a central exchange, hosting fee for a website, etc.). The more agents become her customers the cheaper she can offer the forecast for the next round. Agents do not change anything on their side in terms of behavior. The falling average cost curve produces some lock-in as customer agents will forego some of the locally provided superior heuristics due to the small fee they have to pay to the central agent. This cost advantage is remindful of the problematic feature of fiat money in the KW model, however, we have much more realistic assumptions concerning agents' available choices as well as their knowledge about the structure of the aggregate economy.

There can be a large number of agents in the economy as a whole, but every agent has a small fixed number of immediate neighbors. Similar to the KW model, agents have an initial endowment (which can be interpreted as a piece of agricultural land or a financial asset) that can be consumed in the next period. Consumption depends on the precision by which an external signal is forecast (the external signal can be interpreted to be weather conditions, the future price of the commodity produced, or the rate of return on financial assets). To produce the forecast agents, have at their disposal a number of simple heuristics that include simple time series models such as moving averages, random walks with or without drift, etc. Alternatively, agents can observe their immediate neighbors' consumption histories. If they observe that a neighbor was more successful than themselves, they will enter into conversation and may copy the neighbor's rule of thumb. It is not central to our argument how exactly this process takes place. What matters is that it will take some time and effort, (transactions) costs that ultimately reduce consumption.

Typically, in this kind of setting agents will be characterized by bounded rationality in the sense of limited, or costly, memory. E.g., they can observe only a relatively small number of periods of their own forecast and consumption history. As long as consumption of the agent does not fall below a certain threshold level, whatever behavior the agent has applied during the last period will be applied in the next period. This behavior is not only realistic in a highly decentralized setting where the agents can be thought of as retail customer or private households (or even small and medium sized firms), it has also been shown to be a very successful strategy in game-theoretic terms once games are played with a spatial dimension such as a grid or a graph (Nowak et al. 1994; Nowak and Sigmund 1993; Watts 1999: 204ff.). To allow for the emergence of financial institutions, once an agent is being copied by more than half of its neighbors, the agent can render her consumption history visible to all agents in the economy and offer the information on her model used to forecast the aggregate signal in exchange for a fee. The fee corresponds to a simple swap of individual search costs with a fee for the centrally produced forecast.

The more agents "buy" the rule that has produced the centrally visible stream of consumption, the lower the fee s will become. The central agent has will not go out of business as long as at least the initial number agents/neighbors is willing to acquire the forecast model which defines the fixed cost to be financed which can be thought of as the hosting costs of a website. The model enters the next round: any agent (i) first decides (automatically) based on the consumption threshold level and based on the last outcome to either enter into a search or not. If the answer is no, the model in store is used to compute the forecast and the agent will receive the resulting stream of consumption (and may or may not make a payment to a central agent). If the answer is yes, the agents will look to their neighbors' consumption history as well as to the Internet to see if any central agents are around. If a neighbor is more successful, agents will enter into a conversation and spend the effort and copy the heuristics. If none of the neighbors is more successful, agents will compare the consumption histories of the central agents (e.g. via their websites or their consumption histories recorded elsewhere). A first selection will be to only keep the central agents that show higher consumption. Among the latter the agents will engage into a contractual relationship where they pay a fee that is strictly smaller than the effort to engage with neighbors and use the centrally provided forecast. After this decision consumption is computed and the model goes into the next round.

This first variant of the model could be analyzed in terms of the pattern it produces depending on the cost parameters used. There is the cost of local search; then there is the fixed cost of hosting the website of the central agent.

Another output of such a model will be a measure how social welfare compares to individual loss due to lock-in. Social welfare can be expected to increase with the emergence of central agents due to the beneficial effects on costs. Similar to fiat money in the KW model, these benefits can outweigh some of the losses at the level of individual agents as the latter stick to the centrally provided forecast too long, i.e. the local agents switch too late.

A first evolution of the model could lift the restriction on memory of agents. Thanks to technology, agents can observe their entire history of consumption (marginal storage costs are zero) and they can test alternative heuristics on the entire history of the external signal. Longer memory can be expected to reduce volatility. As a result, agents will look less frequently for alternative heuristics. The ex-ante effect on social welfare and lock-in appears to be ambiguous. While longer memory should, ceteris paribus, lead to a slower adoption of alternative heuristics (recall that all agents start using own heuristics that are costless) including the emergence of central agents and the use of their forecasts, once a large number of agents have bought into centrally provided forecasts the lock-in would be more permanent as well. In any case, lower storage costs make society more (model) conservative.

We think this model corresponds well to the first generation of the Internet with storage costs falling over time. What agents pay in the aggregate for local search can be expected to fall quite dramatically over time as histories get longer and local search will provide almost all observations for the same cost. As a consequence, agents will spend less on strategies that look promising on the basis of a short memory test, but do not produce sufficiently different results over the longer term. (In the aggregate convergence on the true data generating process should be faster with longer memory.)

A third variant of the model could then relax the technological constraint on the cost side that distinguishes the central agent from the local agent. In terms of our cost parameters this corresponds to a situation where both the cost of local search and the (fixed) cost of setting up the central agent's office become very small and thus very similar in size (amazon web services base packages may differ insignificantly from costs of an individual local search in many cases). Lock-in should be much lower in this situation which is clearly welfare enhancing. Agents will switch strategy more easily which is welfare enhancing; given the small difference between costs of local and global searches only a few (very large?) central agents can be expected to prevail over longer stretches producing a limited amount of lock-in.

Finally, in a fourth variant, one could relax the restriction on local agents in terms of access to other agents' histories and heuristics. This would then correspond to an open data (histories), open source (heuristics), P2P finance setting. This could correspond to the transition from the first Internet to the relational web. Each agent could carry out the computation that corresponds to the knowledge of a central agent having all other agents in the economy as clients. However, there is no lock-in. It is another corner solution to our model producing the maximum amount of welfare in our economy. Note, however, that there is not credit in this model, no room for a financial cycle, asset price bubbles, etc.

How general the situation of the described agent is becoming clearer once we reconsider the balance sheet of a typical household. The household is required to correctly understand a number of external signals and trends such as the evolution of life expectancy, health risks, how the market value of his educational status evolves; moreover, a number of macroeconomic variables and trends need to monitored: economic growth, employment and investment opportunities, and inflation. However, for our reflection it is sufficient to illustrate that households face a very complex monitoring problem and that monitoring costs are high (Diamond 1984). On the other hand, these monitoring costs are subject to important economies of scale and scope. These economies form the basis of a highly diversified financial services industry which has banks (monetary financial institutions) at its center.

What then if, one by one, these monitoring costs could be reduced to close to zero? The advent of big data, advanced data analytics, abundant open data, cheap computing power, the mobile Internet, Blockchain technologies, smart contracts and open source management of legal text; all these factors point to the potential of a significant reduction in monitoring and enforcement costs. A revolution similar to the one described by Marlowe and Weber in the context of Protestant culture's impact on transaction costs could be under way in this case.

# 5 Conclusion

This chapter's theoretical discussion explored the argument that the formal institutions needed for complex contracting need third party enforcement to be credible. The peer to peer technologies described subsequently show how monitoring and enforcement of contracts in the context of financial transactions could become significantly less costly. A peer to peer transaction system that leverages the security of Blockchain's, with the automation and self-enforcement of smart contracts with the concomitant legal text interfacing with the system, would dramatically lower the costs of monitoring and enforcement in financial systems. Clearing houses, stock markets, equity funding, insurance could all be to a certain extent automated and operate in a peer to peer manner rather then with a central administrator. This would likely upend the financial system as it functions today. Financial services companies will have to reconsider their value propositions on a fundamental level as their role as intermediaries is made redundant.

# References

Alchian, A., Demsetz, H.: The property rights paradigm. J. Econ. Hist. **33**(1), 16–27 (1973)

Arrow, K.J., Hahn, F.: General Competitive Analysis. Holden-Day, San Francisco (1971)

Bai, J., Philippon, T., Savov, A.: Have Financial Markets Become More Informative? Working Paper, NYU Stern Business School, April (2014)

Barzel, Y.: Economic Analysis of Property Rights, 2nd edn. Cambridge University Press (1997)

Blum, U., Dudley, L.: Religion and economic growth: was weber right? J. Evol. Econ. **11**(2), 207–230 (2001)

Capra, M.C., Tanaka, T., Camerer, C.F., Feiler, L., Sovero, V., Noussair, C.N.: The impact of simple institutions in experimental economies with poverty traps. Econ. J. **119**, 977–1009 (2009)

Coase, R.: The nature of the firm. Economica **4**, 386–405 (1937)

Coase, R.: The problem of social cost. J. Law Econ. **3**, 1–44 (1960)

Cukierman, A.: Central bank independence and monetary control. Econ. J. 1437–1448 (1994)

Eisenstein E.: The Printing Press As an Agent of Change. Cambridge University Press (1979)

Escosura, L., Villarroya, I.: Contract enforcement and argentina's long run decline. Cliometrica **3** (1), 1–26 (2009). Working paper in Economic History

Davies, R., Tracey, B.: Too big to be efficient? The impact of implicit subsidies on estimates of scale economies for banks. J. Money Credit Banking **46**(s1), 219253 (2014)

De Grauwe, P.: Top-down versus bottom-up macroeconomics. CESifo Econ. Stud. **56**, 465–497 (2010)

Diamond, D.W.: Financial intermediation and delegated monitoring. Rev. Econ. Stud. **51**, 393–414 (1984)

Diamond, J., Guns, G.: Steel: The Fates of Human Societies. W.W. Norton, New York (1997)

Duffie, D.: The failure mechanics of dealer banks. J. Econ. Perspect. **24**(1), 51–72 (2010)

Granovetter, M.: Economic action and social structure: the problem of embeddedness. Am. J. Sociol. **91**(3), 481–510 (1985)

Greif, A.: Contract enforceability and economic institutions in early trade: the Maghribi traders. Am. Econ. Rev. **83**(3), 525–548 (1993)

Kasper, W., Streit, M.: Institutional Economics. Edward Elgar, Cheltenham (1998)

Kiyotaki, N., Wright, R.: On money as a medium of exchange. J. Polit. Econ. 927–954 (1989)
Marlowe, C.: The Tragical History of Dr. Faustus. Routledge (2005, first published 1604)
Myers, S.C.: Determinants of corporate borrowing. J. Financ. Econ. **5**(2), 147–175 (1977)
Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Consulted **1**(2012), 28 (2008)
North, C.D.: Institutions, Institutional Change and Economic Performance. Cambridge University Press, Cambridge (1990)
Nowak, M.A., Sigmund, K.: A strategy of win-stay-lose-shift that outperforms tit-for-tat in the prisoner's dilemma game. Nature **364**, 56–58 (1993)
Nowak, M.A., Bonhoeffer, S., May, R.M.: More spatial games. Int. J. Bifurcat. Chaos **4**(1), 33–56 (1994)
Olson, M.: The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press, Cambridge (1965)
Philippon, T.: Has the U.S. Finance Industry Become Less Efficient? On the Theory and Measurement of Financial Intermediation, Working Paper, New York University (2012)
Roberts, J.: The Modern Firm: Organizational Design for Performance and Growth. Oxford University Press (2004)
Rodrik, D., Subramanian, A., Trebbi, F.: Institutions Rule: The Primacy of Institutions Over Geography and Integration in Economic Development National Bureau of Economic Research (2002)
Shubik, M.: On understanding money. World Econ. **2**, 95–120 (2001)
Swanson, T.: Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, pp. 1–66 (2015)
Triantis, G.: Improving Contract Quality: Modularity, Technology, and Innovation in Contract Design, p. 450. JL Bus. & Fin, Stan (2013)
Watts, D.: Small Worlds. Princeton University Press (1999)
Weingast, B.: The economic role of political institutions: market-preserving federalism and economic development. J. Law, Econ. Organ. **11**(1), 1–31 (1995)
Wickelgren, A.L.: Standardization as a solution to the reading costs of form contracts. J. Inst. Theor. Econ. **167**, 30–39 (2011)

## Author Biographies

**James Hazard** is the founder of CommonAccord.org, a project to open source legal documents. He is graduate of Brown University and Cornell Law School, and has practiced law in Boston and Paris.

**Odysseas Sclavounis** is a graduate of King's College London. He is currently completing his Master's degree at the University of Oxford before beginning his Doctorate at the Alan Turing Institute and the Oxford Internet Institute. He is interested in institutional theory and governance, particularly of distributed systems such as Bitcoin and Blockchains.

**Harald Stieber** works in the department for economic analysis and evaluation at DG FISMA, European Commission, Brussels, Belgium. DG FISMA puts forward and monitors regulation for the entire financial sector in the European Union including financial institutions and financial markets, as well as corporate governance, rating agencies and financial accounting. His current interests include capital structure choices of non-financial companies, methodological issues in financial integration (e.g. measuring the size of the financial sector), network and agent-based models, theories of money, big data, and new instruments and markets for consumption risk sharing at the level of the private household. As part of his professional assignments, he follows data and modelling for policy issues in collaboration with the digital science department in the Commission, as well as data format and aggregation issues in financial markets regulation. Before joining the European Commission, he was responsible for macroeconomic modelling in the Austrian Federal Ministry of Finance and worked on issues related to fiscal federalism; from 2002 to 2007 he was a member of the OECD's Working Party No 1 on structural economic policies; between 2007 and 2012 he has worked on policy conditionality of macro-financial assistance programs. Harald has some background in engineering (TU Graz), received his master's degree in economics from the University of Vienna and his doctorate in economics from WU Vienna University of Economics and Business.

**Disclaimer for Harald Stieber** The views expressed in thischapter are my own and may not, under any circumstances, beinterpreted as stating an official position of the European Commission.

# Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money

**Gareth W. Peters and Efstathios Panayi**

**Abstract** In this chapter we provide an overview of the concept of blockchain technology and its potential to disrupt the world of banking through facilitating global money remittance, smart contracts, automated banking ledgers and digital assets. In this regard, we first provide a brief overview of the core aspects of this technology, as well as the second-generation contract-based developments. From there we discuss key issues that must be considered in developing such ledger based technologies in a banking context.

**Keywords** Blockchain · Smart contracts · Banking ledgers · Data integrity · Data security · Exchange clearing

G.W. Peters (✉)
Department of Statistical Science, University College London, London, UK
e-mail: garethpeters78@gmail.com

G.W. Peters
Department of Statistical Science, Oxford Mann Institute, Oxford University, Oxford, UK

G.W. Peters · E. Panayi
Systemic Risk Center, London School of Economics, London, UK
e-mail: stathi.panayi@gmail.com

E. Panayi
Department of Computer Science, UCL, London, UK

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_13

# 1 Introduction

Throughout this book, the reader has observed how blockchain technologies have enabled the creation of crypto-currencies, and their rise has been documented widely documented.[1] The use of these currencies has prompted wide discussions on the merits (or lack thereof) of decentralisation, disintermediation,anonymity and censorship resistance in this setting, aspects which we discuss in this chapter also. One cannot, however, dispute their potential to disrupt areas such as the global remittance industry, by facilitating near-instantaneous global remittance with very low transaction fees.

In more recent times, blockchain applications have appeared to go far beyond their first application domains in virtual currencies, for instance they are now important in fields such as domain registration, crowdfunding, prediction markets and even gambling. Second generation blockchain technologies enable not only the execution of simple transactions, but the carrying out of computation on a network, where e.g. payments become conditional on the state of some internal or external variables (much the same way as financial derivatives have a payout that is a function of an underlying financial instrument). This is the basis for 'smart contract' technologies, which we shall see can be important building blocks for these new application areas. As a consequence of these second generation technologies, a number of developments in this field have begun to appear which include third party data ledgers (Devanbu et al. 2001), e-contracts/smart contracts and virtual contracts (Buterin 2014b; Kosba et al. 2015; Swan 2015), e-assets or remote asset title transfers (Halevi et al. 2011) and further applications, discussed in Czepluch et al. (2015).

One can imagine that different applications require different blockchain structures or architectures, and our first contribution is in describing the differences (from both a theoretic and practical standpoint) between permissionless and permissioned blockchains in this context. As blockchains require nodes to act as verifiers for the network, permissionless blockchains allow for anyone to join as a verifier, while prior authorisation from a centralised authority or consortium is required in a permissioned blockchain. These blockchain types therefore require different approaches to achieving consensus, as well as incentivising verification activity on the network. In this context, one of our contributions in discussing these frameworks focuses on the significance of data integrity protocols, which can be incorporated with blockchain technologies to achieve different levels of permissioning, data integrity and data security.

While the potential for smart contracts to operate on these blockchains is very promising, it is not without its pitfalls. Notably, current blockchain structures,

[1] Nakamoto (2008) introduced the first decentralised crypto-currency called Bitcoin, and related technology startups have already attracted more than $1 billion in funding. The currency has been the subject of academic considerations in topics such as privacy (Reid and Harrigan 2013), security Barber et al. (2012), regulation (Peters et al. 2014) and monetary policy (Peters et al. 2015).

requiring the repetition of computation on all network nodes, will rapidly run into scalability issues, and this will require consideration before mass adoption becomes possible. Blockchain technology has the potential to revolutionize contract law and processing via self-enforcing digital contracts, whose execution does not require any human intervention. However, where automated smart contracts have a real-world counterpart, one has to understand both the legal and technical ramifications, particularly in the case of disagreements between the two, which is what we aim to analyze.

In addition to these innovations in financial transactions and contract law, it is also recognised that such technologies can contribute significantly to other aspects of the financial industry, e.g. related to regulation and taxation. Importantly for this chapter, we envisage a banking and insurance environment in which blockhain technologies are utilised in banking ledger records and other banking and insurance records, such as loss databases and claims record databases. In this regard, we will discuss aspects that must be considered when developing such technologies for banking applications, notably loss reporting, recording and provisioning in order to be consistent with modern regulations such as Basel III/IV, Solvency II and IFRS 9.

We also discuss how blockchain technology offers the potential for the development of new approaches to governance systems with the ability to decentralize many processes and thereby provide perhaps more democratic inclusive decision-making processes. Indeed there are some attempts to develop second generation blockchain architectures that are specifically designed for board rooms and automated structuring of governance frameworks for corporations. It is important to note what we refer to as decentralization in this context, see for instance the definition provided in Benkler (2006).

> Decentralization describes conditions under which the actions of many agents cohere and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action.

Another area we explore in the context of blockchain technologies is that of clearing and settlement of financial assets. Several markets have experienced benefits in reducing counterparty and settlement risks in shortening the settlement cycle from 3 days to 2 days, and blockchain technologies have the potential to lead to near-instantaneous settlement. Because of the ability of blockchain to serve as an alternative for structures featuring centralised bodies for verification, we present the possible blockchain structures which would facilitate this, as well as initial industry attempts at pursuing this field.

This chapter is topical, as it extends previous work regarding the real-world considerations that banks and other financial institutions would have, if they were to consider handling crypto-currency transactions (see, e.g. Peters et al. (2014) for a discussion of operational risk considerations, and Peters et al. (2015) for a monetary policy perspective). In particular, it shifts the discussion to the underlying blockchain technology, which has a much broader scope for entering the banking sector and the regulatory space.

The remainder of the chapter is structured as follows: Sect. 2 details the differences between the permissionless and permissioned blockchain types, it describes the advantages blockchains hold over databases and introduces smart contracts and their possible applications. Section 3 discusses existing notions of security, confidentiality, availability and integrity and how it applies to enterprise data, giving examples of blockchain structures which can preserve these features. Section 4 proposes usecases for blockchain technology for government cash management through administering Treasury Single Accounts, as well as improving on the commercial bank ledger structures. Section 5 describes the current state of the clearing and settlement system and proposes blockchain approaches to reduce the inefficiencies. In Sect. 7 some conclusions are drawn.

## 2 Blockchain Technology Emerges

The emergence of blockchain technology is inextricably linked to the introduction of Bitcoin, the decentralised crypto-currency for the internet. Nakamoto (2008) described how a network of users could engage in secure peer-to-peer financial transactions, eliminating the need for financial intermediaries and reducing the cost of overseas payments. In so doing, however, Nakamoto described a structure, termed the blockchain, along with a communication protocol, which essentially solved the Byzantine Generals' Problem[2] and thus enabled the network to achieve consensus without requiring knowledge of users' identities, or trust relationships.

So what is a blockchain and what are the different types of blockchain technology arising? In its most crude form, a blockchain may be considered a ledger or, more simply, a chronological database of transactions recorded by a network of computers. The term 'blockchain' refers to these transactions being grouped in blocks, and the chain of these blocks forms the accepted history of transactions since the inception of the blockchain. On such a blockchain, anyone can attempt to provide an update to the blockchain ledger with a new record or amendment, which they sign with their own private cryptographic key.

To ensure that only legitimate transactions are recorded into a blockchain, the network confirms that new transactions are valid, given the history of transactions recorded in previous blocks. A new block of data will be appended to the end of the blockchain only after the computers on the network reach consensus as to the validity of all the transactions that constitute it. Thus the transaction only becomes valid ('confirmed') once it is included in a block and published to the network. In this manner the blockchain protocols are able to ensure that transactions on a

[2] In the Byzantine Generals' problem, introduced by Lamport et al. (1982), a group of Byzantine Generals are camped around an enemy city in different locations. If they all attack simultaneously, then they have superior firepower to their enemy. The problem is that they need to agree a common battle plan, so that they attack at the same time, with the additional complication that there may be a traitor amongst their ranks.

blockchain are valid and never recorded more than once, enabling people to coordinate individual transactions in a decentralized manner without the need to rely on a trusted authority to verify and clear all transactions.

## *2.1 Basics of Blockchain Technology*

Just like many other technologies for the internet, blockchains rely on public key cryptography to protect users from having unauthorised persons take control of their accounts. The private and public key pairs enable people to encrypt information to transmit to each other, where the receiving party would then be able to determine whether the message actually originated from the right person, and whether it had been tampered with. This is critical when one needs to communicate to a network that a transaction between two parties has been agreed. In addition, the presence of an ability to identify the integrity of the data is also critical for applications we will consider, as discussed further below. We don't enter into a detailed discussion here on the basic details of crytographic properties of blockchain and its construction via hash functions as the reader can find this detail in other chapters in this book. We note that detailed discussions on the different types of hash function may be found in the overview of Carter and Wegman (1977).

We note that within the blockchain structure there is also included information related to the digital time stamp, which records the temporal existence of a particular blockchain ledger item at a given instance in time. It could be utilised to symbolise that a contract between two agents is initiated or completed, that transactions of some form materialized or that payments/e-property were transferred ownership etc. Typically a digital time stamp also contains information relating to the hash created from the activity of securing the particular data/information entered into the ledger. This allows time stamping to occur with an element of privacy for the data being secured and entered on the blockchain ledger. In addition, just recording the hash is a more parsimonious representation of the information being secured or recorded.

There exist parties such as Time-Stamping Authorities (TSA) that can provide a trusted third party arrangement to provide a secure and safe cold or secured live storage of information relating to the blockchain ledger recording. This digital notary signs with a private key for this data to be recorded and the time when this data was communicated to the authority. Then the signature address would be sent back to the original owner of the data. This simplified form is often performed in blockchain technologies using more advanced approaches such as a TSA collecting and securing in encrypted storage several agents data sets from within a fixed time period, then taking all data from this period and providing a time stamp, and hashing all this data together via a method such as a Merkle tree, see (Merkle 1979, 1980; Devanbu et al. 2001). Then the resulting hash, for instance the root of the Merkle tree would be hashed together with the final hash of the previous time period and then published in the blockchain ledger.

## *2.2 Permissionless and Permissioned Blockchains*

There are various (often conflicting) categorisations of blockchain types, and for the purposes of this chapter we will focus on the different types of blockchain according to whether authorisation is required for network nodes which act as verifiers, and whether access to the blockchain data itself is public or private.[3] For the first categorisation we have:

- *Permissionless* blockchains, where anyone can participate in the verification process, i.e. no prior authorisation is required and a user can contribute his/her computational power, usually in return for a monetary reward.
- *Permissioned* blockchains, where verification nodes are preselected by a central authority or consortium.

For the second categorisation we have:

- *Public* blockchains, where anyone can read and submit transactions to the blockchain.
- *Private* blockchains, where this permission is restricted to users within an organisation or group of organisations.

In reality, most permissionless blockchains feature public access, while the intention of most permissioned blockchains is to restrict data access to the company or consortium of companies that operate the blockchain. For this reason, we collapse the categorisation into two types, permissioned and permissionless blockchains, and we elaborate the distinction between them in the following section.

### 2.2.1 Permissionless Blockchains

In the prototypical example of a blockchain, the Bitcoin network, the blockchain used is 'permissionless'. Permission refers to the authorisation for verification, and anybody can join the network to be a verifier without obtaining any prior permission to perform such network tasks. Because these verifiers are vital to the operation of the network, their participation is encouraged (and indeed incentivised) through the issuance of new currency that is paid to them once they have verified a block of transactions, the so called 'Proof-of-Work' concept to be discussed below.

Consensus within the network is achieved through different voting mechanisms, the most common of which is Proof-of-Work, which depends on the amount of processing power donated to the network. The notion of Proof-of-Work allows the network to secure against malicious attempts to tamper with the blockchain structure due to the computational power that has already been applied to create the blockchain ledger entries. If an attacker wished to tamper with the blockchain, they would have to commit a computational effort equivalent or greater than all the power spent

[3] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

from the reference point they wished to alter to the present time. In addition, they would have to achieve this at a faster pace than the current legitimate network processing of new blockchain entries. Proof-of-work concepts can come in many forms, for instance they may rely on solutions to a computationally hard problem, a memory intensive problem or a problem that may require user interventions. To be practically useful for a blockchain technology, such problems must be computational challenging to solve, but efficient to verify a solution once obtained. Although these algorithms are vital in ensuring the security of the network, they are also very costly in terms of computation, and thus electricity usage also.

A permissionless blockchain is advantageous in that it can Swanson (2015) both accommodate anonymous or 'pseudonymous' actors and protect against a Sybil (i.e. identity-forging) attack Douceur (2002). On the other hand, the incentive mechanism has to be carefully developed in order to ensure that verifiers are incentivised to participate. In Bitcoin, for example, verifiers receive an amount for verifying each transaction, as well as for publishing a block of transactions. However, the latter is 2 orders of magnitude higher than the former. Since the incentive for publishing transactions of blocks decreases according to a predefined schedule, means that verifiers will at some point need to increase the amount they will require to process individual transactions, which makes it more costly to transact in Bitcoin.

Besides Bitcoin, examples of permissionless blockchains include Ethereum,[4] the platform that is intended to provide access to smart contracts on the blockchain, as well as offer blockchain as a service.

### 2.2.2 Permissioned Blockchains

This is not the only possible configuration of a blockchain, however, and the discussion is increasingly moving towards private, permissioned blockchains for specific usecases. Permissioned blockchains have a set of trusted parties to carry out verification, and additional verifiers can be added with the agreement of the current members or a central authority. Such a configuration is more similar to a traditional finance setting, which operates a Know Your Business (KYB) or Know Your Client (KYC) procedure to whitelist users that are allowed to undertake operations in a particular space. Swanson (2015) finds that permissionless and permissioned blockchains are fundamentally different in both their operation and the range of activities that they enable, some of which we review here.

Permissioned blockchains are intended to be purpose-built, and can thus be created to maintain compatibility with existing applications (financial or otherwise). They can be fully private (i.e. where write permissions are kept within an organisation), or consortium blockchains (where the consensus process is controlled by a pre-selected set of nodes).[5] Because the actors on the network are named, the

[4] https://www.ethereum.org.

[5] https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.

intention is that they are also legally accountable for their activity. In terms of the transactions these blockchains handle, it will be predominantly off-chain assets (such as digital representations of securities, fiat currencies and titles of ownership), rather than on-chain assets, such as virtual currency tokens Swanson (2015).

An advantage of a permissioned blockchain is scalability. In a permissionless blockchain, the data is stored on every computer in the network, and all nodes verify all transactions. It is obvious that once the number of transactions increases substantially, the users that are able to perform this type of processing and verification will decrease, leading to more centralisation. In a permissioned blockchain, only a smaller number of preselected participants will need to operate, and if these come from large institutions they will be able to scale their computing power in line with the increase in number of transactions.

However, because of the smaller number of participants, it is much easier for a group of users to collaborate and alter the rules, or revert transactions. In addition, it is easy for them to reject transactions and in this sense it is not 'censorship resistant' as a permissionless blockchain would be. Examples of permissioned blockchains include Eris,[6] Hyperledger,[7] Ripple[8] and others.

### 2.2.3 Smart Contracts

In recent times, industry interest has increasingly moved to second generation blockhain applications, including digitising asset ownership, intellectual property and smart contracts. The latter usecase is particularly interesting, as one can encode the rules of a contract in computer code, which is replicated and executed across the blockchain's nodes. Such a contract can be self-enforcing, monitoring external inputs from trusted sources (e.g. the meteorological service, or a financial exchange) in order to settle according to the contract's stipulations.

The concept of smart contracts has been considered as early as 20 years ago by Szabo (1997), although we have only recently had concrete blockchain-based implementations. These blockchains extend the functionality of the network, enabling it to move from achieving consensus on data streams, to achieving consensus on computation (Kosba et al. 2015). An example is Ethereum, which intends to provide 'built-in blockchain with a fully fledged Turing-complete programming language' (Buterin 2014b).

To understand how this extends the functionality of the Bitcoin blockchain, for example, let us consider a Bitcoin transaction as a very simple contract for the transfer of a certain amount of crypto-currency from one account to another. In a smart contract, this transfer could be made depending on some condition, for example: 'Transfer x amount of y currency from Alice to Bob if the temperature in

[6] https://erisindustries.com/.

[7] http://hyperledger.com/.

[8] https://ripple.com/.

Devon is below 0 degrees Celsius on at least 20 of the next 30 days'. Smart contracts can feature loops and have internal state, so a much richer array of transactions becomes possible. In addition, they are permanent (i.e. they remain on the blockchain unless they are instructed to self-destroy), and are able to be reused as building blocks for a more complex service.

Ethereum can be seen as a platform for deployment of internet services, for which such smart contracts are the building blocks. Because of the Turing-completeness of the in-built contract programming language, and the fact that computation is executed on every network node, it could have been possible for one to create an infinite loop, i.e. a contract that never terminates, which could bring down the network. To protect against this, programmable computation in Ethereum is funded by fees, termed 'gas', and a transaction is considered invalid if a user's balance is insufficient to perform the associated computation (Wood 2014).

There are still potential issues to be resolved, however, before smart contracts can reach widespread adoption. One is scalability, as it is infeasible to expect that as the number of contracts and users grows, every single node has to process every transaction. The second is code correctness, as both the developers and users of the smart contracts have to be confident that the contract performs its intended use, and does not entail excessive fees due to unnecessary computations. Finally, there is the issue of the relationship between an electronic smart contract and its legal counterpart. For example, performing court enforced legally binding contracts on a distributed and decentralized system potentially over multiple legal jurisdictions.

Thus far, smart contracts are not legally enforceable, although there have been efforts in the direction. Eris industries have recently proposed the idea of dual integration, or 'ensuring a real world legal contract overlay fused onto a specific smart contract'.[9] Other initiatives include CommonAccord,[10] which attempts to create templates of legal texts and thus create contracts in a modular fashion. The objective is to remove ambiguity as much as possible, having the smart contract accurately reflect the written legal contract, so that it can be actionable in the real world.[11]

## 2.3 Differences Between Blockchains and Databases

In terms of applications of blockchain technology, one could argue that we are still in the exploration phase. It is prudent to be cautious about claims that this technology, particularly in its 'permissioned blockchain' form could disrupt fields as diverse as banking, insurance, accounting etc. In particular, it would be useful to explore exactly what advantages blockchains have compared to well-understood transaction recording technologies, such as databases.

[9] https://erisindustries.com/components/erislegal/.

[10] http://www.commonaccord.org/.

[11] http://p2pfoundation.net/Legal_Framework_For_Crypto-Ledger_Transactions.

To start with, we provide a short description about the types and capabilities of modern databases. Depending on the nature of the data one is storing, there are five genres of databases (Redmond and Wilson 2012):

- Relational databases, such as SQL and variants, which are based on set theory and implemented as two-dimensional tables;
- Key-value stores, which store pairs of keys and values for fast retrieval;
- Columnar databases, which store data in columns, and can have more efficient representations of sparse tables compared to relational databases;
- Document databases;
- Graph databases, which model data as nodes and relationships.

Databases can be centralised (residing at a single site) or distributed over many sites and connected by a computer network. We will focus on the latter, given the closer proximity to the blockchain concept. The objective of a distributed database is to partition larger information retrieval and processing problems into smaller ones, in order to be able to solve them more efficiently. In such databases, a user does not, as a general rule, need to be aware of the database network topology or the distribution of data across the different nodes. It should also be noted that in a distributed database, the connected nodes need not be homogeneous, in terms of the data that they store (Elmasri and Navathe 2014).

Because of the design of these databases and the replication of data across different nodes, such a database has several advantages (Elmasri and Navathe 2014, p. 882):

- Better reliability and availability, where localised faults do not make the system unavailable;
- Improved performance/throughput;
- Easier expansion.

In every distributed database, however, there is the issue of how modifications to the databases are propagated to the various nodes that should hold that data. The traditional approach is a 'master-slave' relationship, where updates to a master database are then propagated to the various slaves. However, this means that the master database can become a bottleneck for performance. In multi-master replication[12] modifications can be made to any copy of the data, and then propagated to the others. There is a problem in this case also, when two copies of the data get modified by different write commands simultaneously.

A blockchain could be seen as a new type of distributed database which can help prevent such conflicts. In the same way that the Bitcoin network will reject a transaction where the Bitcoin balance to be transferred has already been 'spent', a blockchain can extend the operation of distributed databases by rejecting transactions which, e.g. delete a row that has already been deleted by a previous transaction (where a modification is a deletion, followed by the creation of a new row).

[12] http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/.

A second difference between blockchains and distributed databases lies in the ability to create self-enforcing contracts that will modify the blockchain's data. Many permissioned blockchains have a built-in virtual machine, such that one can execute pieces of computer code on the network. If this virtual machine is Turing-complete, this means that the machine can potentially solve a very large set of problems, which is very useful for executing more complex transactions on the network, possibly conditional on the state of certain off-chain variables.

The proliferation of databases as data stores has spawned considerations regarding data-related aspects, such as security, confidentiality and integrity. We argue that discussions around these issues will be important for blockchain technologies too, if they are to be successful in a business enterprise setting. In the following section we discuss these security aspects in depth and comment on blockchain attributes with regard to them.

## 3 Data Security, Confidentiality, Availability and Integrity on the Blockchain

Companies and organizations use the data they collect to personalize services, optimize the corporate decision making process, predict future trends and more. If one is to consider how to incorporate such records onto a blockchain there are fundamental issues to be considered. Within banking and financial services, for example, they must first of all adhere to different adopted best practices with regard to data confidentiality, availability and integrity. These concepts are related but distinct, and vital for data security within an organisation. We briefly discuss the first two, before exploring the latter in depth in the context of the blockchain.

Confidentiality involves the protection of data from unauthorised disclosure, either by direct retrieval or by indirect logical inference. Confidentiality considerations can also involve the possibility that information may be disclosed by legitimate users acting as an information channel, passing secret information to unauthorised users. Within a blockchain, the choice of a permissioned or permissionless structure will define whether data will be made available to the public, or only within an organisation. Permissionless blockchains also enable carrying out transactions without the disclosure of private information. Because the operation of these blockchains rests on public key cryptography, securing users' private keys is critical, and indeed, this is one of the main source of operational risks in this area (Peters et al. 2014).

Ensuring high availability means that data is accessible to authorised users. Availability is very closely related to integrity because service denial may cause or be caused by integrity violations. In blockchains, because data is replicated across many different nodes, availability should always be high. The catastrophic failure of a number of nodes should not cause any availability problems, although the network will experience a reduction in security proportional to the computational power of the missing nodes.

### 3.1 Data Integrity

Maintaining the integrity of data entails its protection from invalid modification, insertion or deletion, thereby preserving the accuracy, consistency and validity of data over its life cycle. Ensuring this integrity is important for the recoverability and searchability, as well as the traceability and connectivity of financial data records. This process usually requires a set of constraints or rules that define the correct states of a database or data set, and maintain correctness under operation. While the wider area of data security is often discussed in the context of cryptography considerations around blockchain technology, data integrity preservation in a blockchain structure has received comparatively little attention.

When we discuss data integrity in this section we are referring to the accuracy and consistency or validity of data over its life cycle. In general, when discussing data integrity it may take one of two meanings, either referring to a state of the data or a to a process performed relating to the data. Data integrity in the context of a state specification defines a data set that is both valid and accurate, whereas data integrity as a process, describes protocols adopted to preserve validity and accuracy of a data set.

In this section we argue that blockchain technologies can be structured to be consistent with best practices currently adopted with regard to data integrity, and indeed such considerations are only just starting to find their way into second generation blockchain technologies, with projects such as Enigma in MIT, see Zyskind et al. (2015). The first aspect of data integrity we consider relates to the state of the data. In this context the state specification of the blockchain data records would be defined such that the data is valid and accurate or that the smart contracts operating on the blockchain are valid and accurate.

The second aspect of data integrity relates to the transformation processes, which in this case would be operating on either data recorded or linked to the blockchain or to smart contracts operating on data on the blockchain. As with all applications in which data is a key ingredient, the data in its raw form is often not directly utilised for decision making and interpretation within the application. It must first undergo a variety of modifications and be put through different internal processes to transform the raw data forms to more usable formats that are practical for identifying relationships and facilitating informed decisions. Data integrity is then critical in ensuring that these transformations preserve the validity of the data set. Modern enterprises reliant on data, such as financial institutions, need to have confidence in the validity of their data, therefore they need to ensure both the provenance of the data and the preservation of integrity through transformation. Such transformations may also be included as part of smart contract structures in second generation blockchain applications.

Another way of conceptualising data integrity notions is to consider its function in preventing data modification by unauthorized parties, and maintaining internal and external consistency in the data set. If data is compromised then its utility to business practice and its informative nature may rapidly diminish. There are numerous places where such corruptions of data integrity may arise, for instance during replication or transfer or the execution of a smart contract that operates on a dataset to make contractual decisions.

One can minimise such issues through the adoption of error checking methods. In a blockchain, these methods are inbuilt. The hash of each block of transactions is linked to the next, thus forming a chain. Transactions that are present in these blocks cannot be altered, unless one generates all blocks from that point onwards, which requires immense computational power. However, error checking for second generation blockchain structures, where smart contracts contain computer code, will be more involved.

Causes of corruption of data integrity include human error, which may or may not be intentional, code errors, viruses/malware, hacking, and other cyber threats, compromised hardware, such as a device or disk crash and the physical compromise to devices. From this list we see that some of these issues with preservation of data integrity rely on data security, whilst others are non-resolved when it comes to security solutions. We can easily see that data integrity and data security are related, and that data security refers to the protection of data against unauthorized access or corruption and is necessary to ensure data integrity. Hence, we see that data security is one of several measures which can be employed to maintain data integrity, as unauthorized access to sensitive data can lead to corruption or modification of records and data loss.

In addition to security considerations, it is also clear that to achieve data integrity there is a strong case for data backup/redundancy/duplication. Practically, there are adopted best practices that remove the other data integrity concerns, such as input validation to preclude the entering of invalid data, error detection/data validation to identify errors in data transmission, and security measures such as data loss prevention, access control, data encryption.

We have already discussed the advantages that distributed databases bring in resolving a number of these issues. A blockchain additionally brings cryptographic security, a solution to the multi-master replication problem, and facilitates more complex transactions through enabling smart contracts.

Ge et al. (2004) note the following aspects of integrity for data stored in databases which we believe would similarly apply to blockchain structures and architectures, as well as to perhaps different smart contract structures that are designed to operate on blockchain backbone networks:

- Integrity and consistency should involve semantic integrity constraints which are rules defining the correct states of the system during operation. Such semantic constraints are present to ensure a level of automated protection against malicious or accidental modification of data, and ensure the logical consistency of data. Rules can be defined on the static state of the database, or on transitions (as conditions to be verified before data is modified). In the context of blockchains, such rules would need to be applied at different levels, to the raw processing of data and in addition, to the functioning of smart contracts or secondary processes/transformations on blockchain related data records.

- Identification, Authentication, Audit. Before accessing a system, every user is identified and authenticated, both for the audit trail and for access permission. Auditing is the process of examining all security relevant events. Such features can be incorporated into blockchains either publicly through colouring mechanisms on the blockchain records (see overview in Rosenfeld 2012) or through blockchain architectures such as permissioned blockchains.
- Authorisation (access control). Authorisation applies a set of rules that defines who has and what type of access to which information. Access control policies govern the disclosure and modification of information. In the context of requirement engineering, security aspects should not be afterthoughts of the database design process and likewise should be included in many applications in the blockchain settings. Authorisations that are of relevance in blockchain settings can range from who can append data and what type of them to the blockchain, who can verify blockchain transactions, who can perform or execute smart contracts, view existing properties of smart contracts or initiate such smart contracts.

In fact, the specification of protocols for preservation of data integrity in general governance structures has been a research topic since the early 70's and several different approaches have been proposed which include (not an exhaustive list):

1. The Bell LaPadula model (Bell and LaPadula 1973);
2. Discretionary Access Control protocols;
3. The Graham-Denning model (Denning 1976) and its extension the Harrison-Ruzzo-Ullman model (Tripunitara and Li 2013). Note, the Graham-Denning Model is a computer security model that shows how subjects and objects should be securely created and deleted. It also addresses how to assign specific access rights. It is mainly used in access control mechanisms for distributed systems
4. Mandatory Access Control. Note, MAC often refers to an access control in which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target.
5. Multilevel security. Note, MLS usually involves the application of a computer system to process information with different security levels, and prevents users from obtaining access to information for which they lack authorization. MLS is typically adopted in one of two settings, the first is to refer to a system that is adequate to protect itself from subversion and has robust mechanisms to separate information domains. The second context is to refer to an application of a computer that will require the computer to be strong enough to protect itself from subversion and possess adequate mechanisms to separate information domains, i.e. a trusted system third party.
6. The take-grant protection model. Note, this is a formal graphical model structure and protocol to establish or disprove the safety of a given computer system that follows specific rules.
7. The Clark-Wilson model (Clark and Wilson 1987).

We briefly highlight a few examples of these data integrity frameworks mentioned and then comment on the ability to develop such frameworks within the context of a blockchain network. We specifically choose two frameworks: the Clark-Wilson model and the Biba model, as variants of them have wide spread uptake for the types of applications we will discuss.

### *3.2 Clark-Wilson Model for Data Integrity*

We provide a brief review of the concepts behind the Clark-Wilson (CW) model which has been adopted in business and industry processes. Clark and Wilson (1987) argued the case for consideration of control over data integrity and not just considerations over control of disclosure. The Clark-Wilson model consists of subject/program/object triples and rules about data and application programs. The core of the CW model specification involves two key components: the notion of a transaction, which is characterized by a series of operations that transition a system from one consistent state to another consistent state; and the separation of duty (in banking settings often forming part of governance structures).

In the case of blockchain settings, one may think the first component denoted the ‘transaction’ as any function operating on the blockchain, such as addition of data to the blockchain, the verification of the blockchain transactions or a smart contract that reads or modifies the blockchain ‘state’. The second component involving separation of duty involves consideration of who may perform verification, who may view or alter data on the blockchain or attached to the blockchain, or who may view or execute or initiate such smart contracts.

In the CW model all data to be considered is partitioned into two sets termed Constrained Data Items (CDIs) and Unconstrained Data Items (UDIs). Then in addition, there are subjects which are entities that can apply transformation processes to data items to take CDIs from one valid state to another. The term ‘transformational procedure’ makes it clear that the program has integrity-relevance because it modifies or transforms data according to a rule or procedure. In addition, there are integrity validation procedures which confirm that all CDIs in a system satisfy a specified integrity scope. Data that transformational procedures modify are called CDIs because they are constrained, in the sense that only transformational procedures may modify them and that integrity verification procedures exercise constraints on them to ensure that they have certain properties, of which consistency and conformance to the real world are two of the most significant. Then UDI’s represent all other data, such as the keyed input to transformational procedures.

Given these structures, the CW model then specifies 6 basic rules that must be adhered to in order to maintain integrity of a system. We provide these below, along with a description of how these pertain to a blockchain structure.

- The application of a transformation process to any CDI must maintain the integrity of the CDI and it may only be changed by a transformation process.

  **Comment**: A transformation process is a transaction, and transactions on blockchains are unitary—it is impossible for one side of the transaction to happen without the other. Permissionless blockchains, such as Bitcoin, feature eventual consistency, in the sense that there may be some period of time for which the system is in an inconsistent state (e.g. due to a fork), but it is guaranteed to return to a consistent state eventually. However, this does require consideration for structuring of smart contract and blockchain specific secondary application functions.

In permissioned/private blockchains, it is of possible to have near-instantaneous consistency.

- Only certain subjects can perform transformation processes on prespecified CDI's. This prespecification restriction must reflect governance enforced true separation of duties. The principle of separation of duty requires the certifier of a transaction and the implementer to be different entities.;

  **Comment**: In any blockchain, subjects (users) are only enabled to transact with the tokens belonging to them, and no other user is able to access these without knowledge of their private key. Verifiers (miners) only ascertain whether transactions are valid. If however smart contracts have access to such information or data pertaining to users, this must be considered in their development on blockchain technology.

- All subjects in the system must be authenticated.;

  **Comment**: This is the case in blockchain through public key cryptography.

- There must be a single written audit file that records all the transaction processes.;

  **Comment**: Clearly this exists in the case of blockchain. An advantage of the blockchain is that it can provide guarantee of absence of modification. In the context of ownership, the blockchain proves that an asset has been transferred to somebody, and has not been transferred to somebody else subsequently. Because transactions can only be found on the blockchain, if a transaction is not found there, from the blockchain's perspective it does not exist.[13]

[13] Factom whitepaper, available at https://raw.githubusercontent.com/FactomProject/FactomDocs/master/Factom_Whitepaper.pdf.

- It must be possible to upgrade some UDI’s to CDI’s through the application of a transaction process.;
- Only a privileged subject in the system can alter the authorisations of subjects.

  **Comment**: In the case of permissioned blockchains, there may be a consortium which may determine whether another node can enter the network.

In most cases of blockchain architectures so seen far, the blockchains do not have hierarchies of authorisations for “read” and “write” access. The data model differs from that envisioned by Clark and Wilson, as there are as many copies of the data as there are verifiers on the blockchain. Anybody can change their own data unilaterally, but for this to become the accepted history of the data, consensus has to be reached about the veracity of the new data. However, as people consider data integrity issues, there are emerging forms of blockchain architecture that will consider such features, such as the Enigma system developed in MIT, which will be discussed in this section.

Under the CW model, once subjects have been constrained so that they can gain access to objects only through specified transformational procedures, the transformational procedures can be embedded with whatever logic is needed to effect limitation of privilege and separation of duties. The transformational procedures can themselves control access of subjects to objects at a level of granularity finer than that available to the system. What is more, they can exercise finer controls (e.g., reasonableness and consistency checks on unconstrained data items) for such purposes as double-entry bookkeeping, thus making sure that whatever is subtracted from one account is added to another so that assets are conserved in transactions.

## *3.3 Biba Models for Data Integrity*

There are alternative approaches to considering data integrity, we also mention a second one that is an important contrast to the CW framework described above. The Biba models‘ (Biba 1977) conceptual framework deals primarily with integrity instead of confidentiality, with its key premise being that confidentiality and integrity are in concept the dual of each other, whereby confidentiality is a constraint on who can read a message, while conversely integrity is a constraint on who may have written or altered it. The design of this data integrity model is characterized by the phrase: ‘no read down, no write up’. Hence, in the Biba model, users can only create content at or below their own integrity level. Conversely, users can only view content at or above their own integrity level. This is in contrast to other integrity models, such as the Bell-LaPadula model, which is characterized by the phrase ‘no write down, no read up’. Extensions of the Biba model structure have also been explored in the Bell LaPadula frameworks, see for instance discussions on such lattice model structures in Sandhu (1993) and Ge et al. (2004).

The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt objects in a level ranked higher than the subject, or be corrupted by objects from a lower level than the subject. Many applications therefore consider such models for data integrity as useful in instance for banking classification systems, in order to prevent the untrusted modification of information and the tainting of information at higher classification levels.

The Biba model is summarised by the following three simple components:

- The subject should be able to read an object only if they have a higher or equal security status than the object. This is known as the Simple Integrity Axiom and stated in another manner it says that a subject at a given level of integrity must not read an object at a lower integrity level (no read down).;
- The subject should be able to write an object only if they have a lower or equal security protocol than the object they write too. This is known as the Star Integrity Axiom and when stated in another manner it says that a subject at a given level of integrity must not write to any object at a higher level of integrity (no write up).;
- The final component is the Invocation Property which states that a process from a lower integrity level can not request higher integrity level access. In otherwords it can only interface with subjects at an equal or lower level of integrity status.

### *3.4 Integrity Considerations in Financial Applications*

There are blockchain technologies starting to emerge for financial applications which try to incorporate these notions of data integrity, security and confidentiality into their designs. A few examples, are provided though our coverage is by no means exhaustive in this rapidly growing field.

For instance in the case of crypto currency applications in blockchain technologies there is ‘cryptoassets.core’ which includes ‘defensive programming principles to mitigate developer human error, data integrity and security issues’. In particular, in this context the irreversibility of the blockchain structure means one must be particularly cautious in financial processes to ensure that there are protocols to mitigate against human-errors by the developers and external attackers trying to exploit issues in the financial code. In this context, the following list of potential data integrity issues for cryptoasset services is provided[14]:

- Race conditions allowing over-balance withdrawals or account balance mix up (data integrity issues);
- Double transaction broadcasts doing double withdrawals from hot wallet;
- Partially lost data on unclean service shutdown;
- Partially lost data when having Internet connectivity issues;

[14] http://cryptoassetscore.readthedocs.org/en/latest/integrity.html.

- Database damage with bad migration;
- Improper cold wallet handling increases the risk of losing customer assets;

In the developments considered in cryptoassets.core, it is possible to overcome issues such as race conditions through partitioned serialized transactions isolations. That is, the database transactions are performed in a complete isolation, one after each another, and thus there cannot be race conditions. If the database detects transactions touching the same data, only one of conflicting transactions may pass through and the others are aborted with application-level exception. In addition, they build in features such as allowing each crypto currency/asset to obtain its own collection of database tables which contain "static-typing like limits making it less likely for a developer to accidentally mix and match wrong…(assets)''. In addition they argue it is prudent to record in the blockchain transaction level time stamps for when it was broadcast to a network for verification or processing and a time stamp when this was completed, which a default of empty should it fail to complete. This allows for rapid verification and audit process for the blockchain to find non-processed transactions and then to recommit them for processing if they fail.

One of the disadvantages of using a blockchain as a data store in financial settings is that for the different verifying nodes to be able to agree on the blockchain's history, they have to store all of it locally in many blockchain architectures. While replication has benefits in increasing the resilience of the network against attacks, when the blockchain is predominantly used as a data store, it becomes more difficult to increase the storage capacity of all nodes as the amount of data increases.

One solution to this, which maintains the cryptographic security of the data store has been proposed by MIT and their Enigma project (Zyskind et al. 2015). This initiative has developed a decentralized blockchain-like framework utilizing three components: a blockchain, which records a complete history in append-only fashion, an off-chain distributed hash-table (DHT), which is accessible through the blockchain, and which stores references to the data, but not the data themselves, and a secure Multi Party Computation (MPC) component. Then any private data is encrypted on the client-side, before storage and access-control protocols are programmed into the blockchain.

Effectively, through this architecture the Enigma blockchain architecture provides a decentralized computation platform with guaranteed privacy that does not require a trusted third party's intervention. It achieves this through the use of secure multi-party computation and it ensures that data queries are computed in a distributed way, without a trusted third party. The actual data is partitioned over different nodes in the network, and they compute functions together without leaking information to other nodes. Therefore, unlike blockchain approaches such as those created for Bitcoin, this blockchain has no network members ever having access to data in its entirety, on the contrary each member has a seemingly meaningless chunk of the overall data. In addition, this lack of complete replication and reduction in redundancy can provide greater scalability features for the network and it can improve the speed. As noted in Zyskind et al. (2015) the 'key new utility Enigma brings to the table is the ability to run computations on data, without having access to the raw data itself'. Clearly, a useful aspect for many financial processing applications of blockchain.

Basically, one can think of attaching Enigma to a particular type of blockchain architecture, and deploying it to enforce on the blockchain a feature of data integrity and privacy. It will connect to an existing blockchain and off-load private and intensive computations to an off-chain network. All transactions are facilitated by the blockchain, which enforces access-control based on digital signatures and programmable permissions. In this architecture the code to be executed (such as a smart contract etc.) is performed both on the public blockchain and on Enigma for the private and computationally intensive components. It is argued that in this manner, Enigma can ensure both privacy and correctness. In addition, one can provide verified proofs of correctness on the blockchain for auditability purposes.

Unlike blockchain approaches such as those underpinning bitcoin, in which execution in blockchains is decentralized but not distributed, meaning that every node redundantly executes common code and maintains a common state, in Enigma, the computational work is efficiently distributed across the network.

As detailed in Zyskind et al. (2015), the off-chain network they develop in Enigma overcomes data integrity based issues that blockchain technology alone cannot handle as follows:

- The DHT, which is accessible through the blockchain, stores references to the data but not the data themselves. Private data is encrypted on the client-side before storage and access-control protocols are programmed into the blockchain.
- It utilises privacy-enforcing computation in Enigma's network, in order to execute code without leaking the raw data to any of the nodes, while ensuring correct execution. This is key in replacing current centralised solutions and trusted overlay networks that process sensitive business logic in a way that negates the benefits of a blockchain.

## 4 Considerations in Blockchain Technology Developments for Bank Ledgers and Financial Accounting

In this section we discuss items that may be of relevance in the banking and insurance sectors that could benefit from the developments of blockchain technologies. Industry publications, such as the recent Euro Banking Association report[15] argue for the potential of blockchain technology to partly replace trusted third parties, commonly employed in many roles in finance as custodians, payment providers, poolers of risk and in insurance settings. Remember that the primary

[15] Cryptotechnologies, a major IT innovation and catalyst for change, available at https://www.abe-eba.eu/downloads/knowledge-and-research/EBA_20150511_EBA_Cryptotechnologies_a_major_IT_innovation_v1_0.pdf.

roles of such trusted third parties is to provide functionality such as: validation of trade transactions; prevention of duplicated transactions, the so-called ‘double-spending’ issue; recording of transactions in the event of disputes over contract settlements or deliverables etc.; and acting as agents on behalf of associates or members. The blockchain can provide alternative solutions to fulfil these roles through the provision of a verifiable public record of all transactions which is distributed and can be decentralised in its administration.

In thinking about the possibilities of blockchain functionality within the banking sector, there are a range of different potential avenues to explore that move beyond the typical discussion on remittance services. Banking systems are large and complex, including a range of features such as back-end bookkeeping systems, which record customer account details, transaction processing systems, such as cash machine networks, all the way through to trading and sales, over the counter trades and interbank money transfer systems. Today, we are however unaware of any papers that go beyond this high level discussion and detail exactly how and what form blockchain technology may provide benefit in these aspects in banking settings.

In this work we will aim to provide a greater detail to these possible applications of blockchain technology. In particular we will discuss things related primarily to a few important unexplored areas:

- Government cash management the central bank and treasury accounts in particular the Treasure Single Account (TSA) of (Pessoa and Williams 2013);
- automation, decentralised and distributed banking ledgers;
- automated and distributed Over The Counter (OTC) contracts/products and clearing and settlement;
- automated client account reconciliations; and
- automated, distributed loss data reporting.

One of the potential incentives for financial institutions, banks, insurers and banking regulators for the development of distributed blockchain technologies for these types of applications involves the reduction of overhead and costs associated with audit and regulation. In addition, more automation and efficiency in transaction processing, clearing and reconciliation can help to reduce counterparty credit risks.

Before entering into specific examples, we outline some core features that blockchain approaches share which can be both beneficial and detrimental. These require careful consideration when developing the applications to be discussed, as we have seen in previous discussions above on data integrity preservation.

- Immutability of itemized components in the blockchain. A blockchain is effectively a distributed transaction database or ledger that is immutable, in that data stored in the blockchain cannot be changed, i.e. deleted or modified. However, some versions of blockchain frameworks are starting to emerge that alter the perception of immutability, such as the Enigma project discussed above. This approaches the irreversibility of the standard blockchain framework by only allowing access to data for secure computations in reversible and controllable manners. In particular they also ensure that no one but the original data owner(s) ever see the raw data.

- Transparency of information presented on the blockchain. Many blockchains being created are publicly accessible by anyone with an internet connection and are replicated countless times on participating nodes in the network, though private versions or restricted blockchain networks are emerging also, as discussed previously. The question is to what extent the application requires private versus public components. In modern regulatory changes on banking and financial institutions there are numerous competing constraints which emphasize both the importance of financial disclosure, such as Pillar III of Basel III banking regulations, requiring financial institutions to demonstrate transparency in their reporting and their relationship with regulators, and on the other side there are also fiduciary duties that institutions maintain in upholding data privacy on behalf of their customers. Therefore, alternative approaches to private versus publick blockchain networks are also being explored where instead the data on a public ledger may have different levels of data integrity structure protocols which implement possibilities such as encryption of data stored in blockchains, see project Enigma for example (Zyskind et al. 2015).

## *4.1 Possible Roles for Blockchain Technology Developments for Government Cash Management: Treasury Single Accounts*

To understand how blockchain technology may benefit this application area to Government cash management we first need to describe briefly the concept of the treasury single account (TSA) . The concept of TSA was first established widely in the consultative and technical notes of the authors based in the International Monetary Fund (IMF) by Yaker and Pattanayak (2012).[16]

The efficient functioning of a country or sovereign state hinges upon the efficiency of the government accounts. In this regard, government banking arrangements represent an important factor for efficient management and control of governments cash resources. Therefore, the governments, central banks and countries treasury arrangements should be designed in such a fashion as to minimize the cost of government borrowing and maximize the opportunity cost of cash resources. The relationship between the treasury and the central bank is a core aspect of most financial policies in a country and is multifaceted in its components and working parts. A streamlined and coherent monetary policy structure in alignment with government financing policies and fiscal policy is a cornerstone of efficient macroeconomic strategy. One core principle to achieve this involves the

[16] Note: the technical note is not representing the direct views of the IMF.

basic step of ensuring that all cash received for projects operated or approved by government functions is available in a timely fashion for carrying out government's expenditure programs and making payments as required. It is particularly in this feature that we argue that blockchain architectures would benefit this application domain.

In this regard, a TSA is a single checking account for government funds from domestic revenue and some foreign funds (together called treasury funds) which are deposited and from which required money can be disbursed in timely fashion. It is a unified structure of government bank accounts that provides a consolidation of government cash resources in a common ledger. It was proposed to act as an essential tool for consolidating and managing governments cash resources, and in doing so it provided a means to reduce borrowing costs. This is particularly useful in countries with banking structures which are not well organised, fragmented and inefficient. Many countries have successfully established such TSA structure for their government accounts. Since the TSA structure is based on the principle of Pessoa and Williams (2013) 'unity of cash and the unity of treasury, a TSA is a bank account or a set of linked accounts through which the government transacts all its receipts and payments. The principle of unity follows from the fungibility of all cash irrespective of its end use'.

Several case studies now exist demonstrating the potential of such TSA account structures to improve the situation that many emerging market and low-income countries face relating to the fragmentation of their banking systems responsible for handling of government receipts and payments. Typically, in such countries that have not instigated such a TSA structure, there are significant challenges in the banking structures since the treasury may often lack governance and may not even possess a centralized control over the ruling government's cash resources. Consequently this can result in cash being idle or unavailable when required to fund core infrastructure projects or expenditure programs for development of the economy. It also extenuates the debt for such countries since the available cash for expenditures is laying idle for extended periods in numerous bank accounts that are fragmented and dispersed over different spending agencies, while in the meantime the government will be borrowing additional funds and increasing debt in order to mistakenly fund such projects and execute its budget plans.

As detailed in Pessoa and Williams (2013) if a country's government has such inefficiencies by lacking effective control over its cash resources there can be numerous consequences:

- Idle cash balances in bank accounts often fail to earn market-related remuneration.
- The government, being unaware of these resources, incurs unnecessary borrowing costs on raising funds to cover a perceived cash shortage.
- Idle government cash balances in the commercial banking sector are not idle for the banks themselves, and can be used to extend credit. Draining this extra liquidity through open market operations also imposes costs on the central bank.

Clearly such inefficiencies can be improved with an automated trusted third party system such as that offered by some permission style blockchain technologies working as a ledger for such accounts under the auspice of a TSA structure.

Furthermore, one can argue for the TSA type structure since such a "financial pool'' example is a concept that segregates two important aspects of this process, the separation of the finance function and the service delivery functions of sector offices and departments of regions, cantons and zones. We have seen that establishing such a feature in a blockchain would require application of data integrity functions. In concept such segregation of duties, is important as it allows public bodies to focus on their core responsibilities whilst financial execution such as control of cash, payments, accounting, reporting can be handled on their behalf by a pool of professionals or as we propose here, the automation by a privacy preserving, permissioned, distributed blockchain structure. Clearly in such a structure, public bodies still define and authorise their budgets and expenditures within these budgets.

### 4.1.1 A Complete Treasury Single Account Structure

Here we recall the definition provided in Pessoa and Williams (2013) for a complete TSA structure which they argue has three core components:

1. Unification of the governments banking structure which will enable the treasury to have oversight of government cash flows in and out of these bank accounts and fungibility of all cash resources. Note particularly in a blockchain type extension can include a real-time electronic banking component and can also be private but remove the need for a single central oversight component in a government, instead replacing it with a distributed verification system.
2. In traditional TSA structures there would be no other government agency operating bank accounts outside the oversight of the treasury. In general the design of the TSA and access to the TSA will depend on the banking structures in place in a given country. In this regard, there are numerous different blockchain architectures that will be suitable for the blockchain version of the TSA.
3. All government cash resources, both budgetary and extra-budgetary, should be included in the consolidated TSA account and the "cash balance in the TSA main account is maintained at a level sufficient to meet the daily operational requirements of the government (sometimes together with an optional contingency, or buffer/reserve to meet unexpected fiscal volatility).'' (Pessoa and Williams 2013). Such features could be automated in blockchain versions of such an account through smart contract structures running on the blockchain TSA ledger. The minimum accounts that should be included in the TSA should cover all central government entities and their transactions. These include:

- accounts managed by social security funds and other trust funds;
- extra-budgetary funds (EBFs);
- autonomous government entities;

- loans from multilateral institutions;
- donor aid resources;

The structure of the TSA ledger should contain accounts which include:

- The treasury account, sometimes know as the TSA central account, which consolidates the governments cash position.
- TSA subsidiary accounts, which are netted off with the TSA main account, and which are typically created for accounting purposes in order aggregate a set of transactions whilst allowing the government to maintain the distinct accounting identity or ledger of its budget ministries and agencies.
- Transaction accounts for retail transaction banking operations which facilitate access indirectly to the TSA for different government projects. Typically such accounts are either imprest accounts (accounts with a cash balance which is capped) or zero balance meaning that their cash balances are aggregated back to the TSA main account on a regular schedule, such as daily. Such zero balance accounts are advantageous as they do not interact with interbank settlement processes for each transaction, further improving efficiency and access to funds.
- Transit accounts for flows of cash into and out of the TSA main account.
- Correspondent accounts. The development of daily clearing/netting can be automated with smart contract structures on a TSA banking ledger blockchain.

### 4.1.2 Possible Blockchain Architectures for a Complete TSA

Note in a standard TSA banking structure there are numerous possibilities relating to where the TSA account should be maintained. That is in which institution, in most cases it is argued that the Central bank of the country may be the appropriate venue for such an account. However, all cases require a trusted third party to administer and provide governance and oversight of this critical consolidated account. One potential advantage of a TSA account placed under a blockchain structure with access through private key permissions and smart contracts is that when it is placed under a private network, there would not need to be a single point of administration, it would be a trusted closed network which has been effectively decentralized. We argue that this could have the potential to remove issues that may arise with governance and oversight when entrusting such key accounts to one single institution, especially in a fragmented banking and institutional structure.

In addition, as noted in Pessoa and Williams (2013), one can establish the TSA banking structure with ledger sub-accounts in a single banking institution (not necessarily a central bank), and can accommodate external zero balance accounts (ZBAs) in a number of commercial banks. This can still be achieved in a blockchain framework in several different architectures. One of which may involve separate ZBA's maintained as internal blockchain ledgers in each commercial bank in the network, followed by a linking of these blockchains to the main TSA blockchain ledger account, with links being executed for transactions based on smart contract technology.

There are two main categories for architecture for a TSA banking account which align well with different architectural decisions for the blockchain version of the TSA, these involve either a centralized or a distributed architecture. In the centralized structure, all revenue and expenditures of the government are on a single ledger which is administered by a single trusted third party such as the central bank, whereas, in the distributed TSA structure there will be a hierarchy of organizational structures each with their own separate transaction accounts in the banking system, but still a single TSA account that contains all balances by close of business each day. As detailed in Pessoa and Williams (2013), the Sweedish TSA structure involves zero balance accounts in the central bank which are authorised by the minister for finance and available for individual spending agencies. In this case, money is transferred from the TSA to such accounts for payment of authorised project expenditures as required. All these accounts are cleared/reconciled with the TSA account daily.

In addition to understanding the network structure and components of the TSA account, there is also the aspect of revenue collection, remittance, payments and processing under the TSA account to be discussed and to consider how blockchain technology can facilitate the functioning, automation and decentralization of such important components. In traditional TSA structures there are two possibilities as detailed in (Pessoa and Williams 2013, Section II Part A) where they describe either centralized transaction processing or decentralized approaches. Under the blockchain version of such a TSA structure, all transactions processing and remittance could be performed in a decentralized manner which would not require oversight of a particular trusted third party network member, as all transaction processing would be automated on the blockchain.

Futhermore, such automation of these processes into the blockchain structure would be more efficient and less costly than existing practices. Currently the best practice adopted for TSA account processing is to utilise the commercial banking network. That is, it is common to contract the commercial banks for revenue collection purposes, these commercial banks transfer revenues collected to the TSA main account daily (so as to avoid float or need of imprest cash amounts). As noted in Pessoa and Williams (2013) such a system, though widely utilised, involves a remuneration system which "…is not transparent and does not clearly indicate the cost of revenue collection services provided by banks. The banks use the free float to invest in interest-bearing securities. This process clearly distorts the TSA structure and concept''.

In this manner one could argue that the blockchain version of the TSA account structure can further reduce costs associated with remittance services and revenue collection services currently charged to the government on a fixed contractual basis. It is currently the case that such remittance services, when provided in a blockchain structure such as in the bitcoin network, can be orders of magnitude cheaper than those offered by traditional remittance providers in financial services industries.

### 4.2 Possible Roles for Blockchain Technology Developments for Commercial Bank Ledgers

Here we discuss considerations around blockchain technologies when they are utilised for retail and investment banking account ledgers. If one is to develop blockchain technologies for ledgers in banks, it is first important to understand some primary components of typical ledgers that will need to be hashed into the blockchain structure and considered in designing the blockchain architectures and the data integrity and governance functions. Hence, we provide a simple overview of the basic structure of a banking ledger in a modern large scale retail bank. One can think of the ledger accounts of a business as the main source of information used to prepare all their financial statements and reporting. In standard practice, if a business were to update their ledgers each time a transaction occurred, the ledger accounts would quickly become cluttered and errors might be made. This would also be a very time consuming process, but this may change with the new potential of blockchain technologies. Before considerations of this nature, we overview the standard approach and then discuss some aspects.

A typical banking system has a range of different structures, including the account master file containing all customers' current account balances together with previous transactions for a specified period, such as 90 days.; a number of ledgers in place to track cash and assets through the processing system; a variety of journals to hold transactions that have been received from a range of different sources not yet entered in ledgers; and an audit trail which records who did what, when they did it and where they did it regarding transaction processing. There will also be a suite of processing software that will operate on this data for overnight batch processing to apply transactions from journals to various ledgers and account master file updating. In addition, there are audit processes in place to scrutinize the functioning of all these systems. In automated systems there are different approaches, one developed in 1987 and widely adopted is the Clarke-Wilson Security Policy Model, see details in Clark and Wilson (1987) and the brief description made above in the section on data integrity. Such an approach sets out how the data items in the system should be kept valid from one state of the system to the next and specifies the capabilities of various principals in the system.

In addition to the component structures in the banking ledgers, there are also processes to understand in how these ledgers are utilised. Therefore, to understand the ledger process better we must first recall some basics of the financial reporting cycle. In the case of the financial cycle, the accounting system records two economic events: the acquisition of capital from creditors and owners and the use of that capital to acquire property to generate revenue. This cycle performs also a third function—the financial reporting function.

We first note that the word 'ledger' refers to a book or set of records. In general, when working towards construction of the banking ledger, initially all transactions are recorded in what are known as the books/ledgers of prime entry. These are records of the transaction, the relevant customer/supplier and the amount of the transaction, which is essentially a daily list of transactions. There are a range of different prime entry books which typically consist of different types of transactions:

- Sales day book which records credit sales;
- Purchase day book which records credit purchases;
- Sales returns day book which records returns of goods sold on credit;
- Purchase returns day book which records goods returned bought on credit;
- Cash book which records all bank transactions;
- Petty cash book which records all small cash transactions; and the
- Journal which records all transactions not already recorded.

In general, the prime entry books/ledgers serve to 'capture' transactions as soon as possible so that they are not subsequently lost or forgotten about. The cash book and the petty cash book are part of the double entry system and record cash coming in and going out. Note, double entry accounting systems are just those that record transactions in two different separate books, as a credit in one and a debit in the other. However, the day books and journal are not part of the double entry system, and entries are made from there to the ledgers. Then all these prime entry books are summarised and the total of the daily transactions is recorded in the accounting ledgers of the company, which is done in the standard 'double entry' format.

After the prime entry books/ledgers there are other key elements of the double entry system in financial accounting. This system consists of the three basic components: the general ledger, the cash book and the petty cash book. In addition, there are the receivables and payables ledgers to be considered which provide details of the total receivables and payables that are recorded in the nominal ledger.

The general or nominal ledger is responsible for the recording of all accounts such as wages, sales, purchases, electricity, travel, advertising, rent, insurance, repairs, receivables, payables and non-current assets. In addition, one typically in principle considers the cash and bank accounts as forming part of this ledger, however they are typically physically recorded in a separate book since the number of such transactions is usually very large for some businesses.

The total amounts owed to suppliers and to whom it is owed is recorded in the payables ledger. Typically, there would be a separate account maintained in the ledger for each individual supplier. Generally, the aggregate total of the outstanding amounts owed in the payable ledger should reconcile with the payables balance in the general ledger. Conversely, to record the total amount owed to the business by customers there is the analogous ledger often called the receivables book. It provides details of exactly what is owed and from whom, as with the payables ledger, it is common practice to have a separate account for each customer. Again, there should be a reconciliation between the total amounts owing in the receivables ledger and the receivables balance in the general ledger.

In the context of a banking financial institution, there is a primary concern regarding the debt and equity capital records. These are the sources of such an organization capital which includes its creditors and owners. Such institutions typically distinguish three forms of capital transactions:

1. Bank Loans which are reported in the Notes Payable account and are to be utilised for short, medium or long term financing and typically asset backed. The Notes Payable Ledgers record outstanding notes and include aspects such as the identifier for the note, its holder, its maturity and current interest rate, and the original and current balance.
2. Bond Issuances are summarized in the Bonds Payable balance sheet item and specific details of each issuance are detailed in a journal entry record for each with individual separate long-term liability accounts. Such issuances allow financial institutions to obtain medium and long term capital, but they create a contractual obligation to pay a fixed amount of interest at specified intervals in the future.
3. Stock Issues are recorded as par or stated value for issued shares in Common Stock and Preferred Stock account ledger. Typically, a corporation will use different Capital Stock accounts for each class of stock.

Apart from the debt and equity capital recording ledgers, there are also other key ledgers to consider such as the Property and Systems records. These keep track of all depreciating property, plant and equipment. Typically it would involve the recording of three primary types of transactions which include:

1. Acquisition of property where an institution would use buildings and equipment to generate revenue;
2. Depreciation of property, plant and equipment;
3. Disposition of property.

To complete the third key component of financial reporting systems we also mention the basic idea of the Journal Entry and Financial Reporting Systems where institutions are able to record transaction in the general ledger using three types of accounting entries that summarize 'High-Volume' transactions such as sales and purchases, 'Low-Volume' transactions such as changes in debt and equity capital in order to remove depreciating property etc., and closing entries.

In the standard ledger systems described above different governance structures may be put in place to resolve potential accounting malpractice and fraud from arising. This is typically achieved by separating responsibilities for the double entry process, otherwise known as dual control systems or decentralized responsibility. These are typically enactments of different data integrity processes as described previously.

We note that with the development of blockchain ledger technologies and smart contracts, many of these processes and ledgers/accounting books just described which make up the financial accounting system can be automated through a blockchain structure. Such blockchains could take many forms, they could be either distributed within an organisation or even available as a public ledger (perhaps with some form of encryption for private data) that is shared between institutions, regulators and government agencies undertaking oversight, taxation etc.

In developing blockchain ledgers, one will need to consider how often to consider constructing hash entries, i.e. how often to aggregate data together before adding a hash entry to the blockchain ledger, as described in the previous overview section. In the context of banking ledgers, this will probably depend on the types of data being placed on the ledger, for instance, one may consider such data as divided into the following components. Transaction data is one source of data that must be considered, it is the records of information about each transaction and it is expected to change regularly as transactions progress and are completed. Other less frequent data includes aspects of standing or reference or meta data which is typically for all practical purposes permanent and includes names and addresses, descriptions and prices of products. We would suggest that the blockchain hashing for such financial records and ledger creation should follow a combination of both batch processing and in some applications real-time processing.

There are a few developments of second generation blockchain ledgers being developed for such banking ledger processing. For instance Balanc3[17] is a new blockchain technology being developed based on smart contracts and a blockchain architecture with the purpose of performing accounting ledger processing, in this case as a triple entry system, rather than the double entry systems described above. It is argued that the non-repudiability and comprehensive audibility of the blockchain can be utilised to guarantee the integrity of accounting records. The blockchain architecture in this case utilises a range of different products for data integrity and security, they include EtherSign combined with an IPFS decentralized data storage platform and smart contracts enacted through Ethereum blockchain. In this way this account ledger is able to construct, store, manage, and digitally sign documents. The admissible documents in this system include features such as self-enforcing smart contracts like employment contracts or invoices, or traditional text agreements. Invoicing through smart contracts automatically processes and records payments.

Before exploring other applications of blockchain, it is worth to observe that the immutability of the blockchain record when automated for transactions must be carefully considered in some cases. For instance, the issue of loss provisioning in the ledger of a banking institution must be carefully considered. We briefly comment on this below.

### 4.2.1 Considerations of Blockchain Ledgers Regarding Automated Provisioning Processes of Losses Under IFRS9

After the 2008 financial crisis that affected the world wide banking sector there were significant changes to banking regulations, insurance regulations and accounting standards. In particular the regulation we mention in this section that must be carefully considered in blockchain ledger applications in banks is that of the provisioning accounting standard now known as IFRS 9 Financial Instruments

[17] https://consensys.net/ventures/spokes/.

document, published in July 2014 by the International Accounting Standards Board (IASB).[18]

This standard has three core components:

- Classification and measurement. Any blockchain based ledger for banking settings must ensure that its recording and processing of losses in the ledger are compliant with the IFRS 9 standard classifications. These classifications determine how financial assets and financial liabilities are accounted for in financial statements and importantly how they are measured on an ongoing basis. This is particularly relevant in some blockchain architectures in which immutability would not allow reversal of misclassifications. Under the IFRS 9 framework, there is a logical classification structure for all financial assets which is driven by cash flow characteristics and the business model in which an asset is held. Under such a framework, it standardizes the management and reporting of such items in banking ledgers in a simplified fashion compared to those of the previous rule-based requirements that are complex and difficult to apply, and more importantly, complicated to automate into smart contract transformations on a blockchain banking ledger.
- Impairment components relate to the management of delayed recognition of credit losses on loans and other financial instruments. Under this aspect of IFRS 9, there is a new expected loss impairment model that will need to be enacted via smart contracts on the blockchain banking ledger processing system. This process would provide an automated and timely recognition of expected credit losses. The new Standard requires entities to account for expected credit losses from when financial instruments are first recognised, so this must be incorporated into the banking ledger processing and could be done in an automated manner with a model enacted via a smart contract structuring. In addition, the IFRS 9 standard makes impairment easier to deal with in an automated smart contract structure, as it is much more standardised under IFRS 9, making it also easier to develop such features in a unified fashion for all financial instruments. This standardization across all financial assets removes a source of complexity associated with previous accounting requirements.
- The third aspect of IFRS 9 relates to hedging accounting changes.

IFRS 9 applies one classification approach for all types of financial assets, including those that contain embedded derivative features, making the design of smart contracts based on such classifications much more streamlined and simpler to automate. Under IFRS 9, one has four possible classification categories for financial assets, which are now classified in their entirety rather than being subject to complex bifurcation requirements, again making things much more streamlined for smart contract based automations. The classification process can be potentially

[18] http://www.ifrs.org/current-projects/iasb-projects/financial-instruments-a-replacement-of-ias-39-financial-instruments-recognitio/Pages/Financial-Instruments-Replacement-of-IAS-39.aspx.

automated via a smart contract structure, see page 7 process model for such classification automation.[19]

In addition, the smart contract implementation would need to be developed under IFRS 9 compliance to apply two criteria to determine how financial assets should be classified and measured: the entity's business model for managing the financial assets and the contractual cash flow characteristics of the financial asset. It should be noted that unless an asset being classified meets both test requirements, then it will be recorded on the blockchain banking ledger in terms of fair value reporting in the profit and loss. If the asset passes the contractual cash flows test, the business model assessment determines how the instrument is classified. For instance, if the instrument is being held to collect contractual cash flows only then it is classified as amortized cost. However, if the instrument is to both collect contractual cash flows and potentially sell the asset, it is reported at fair value through other comprehensive income (FVOCI). Further background on the requirements of the IFRS 9 provisioning standards that blockchain ledgers and processing must adhere to can be found at IASB documents, http://www.ifrs.org.

In addition to the role of blockchain in banking ledgers, blockchain and smart contracts may also be utilised for other roles, such as the clearing and settlement processes. We briefly outline the role of settlement processes in the following section.

## 5 Blockchain Technology and the Trade Settlement Process

A banking area which has been hampered by the inefficiencies of traditional processes is that of settlement of financial assets. Major markets such as the US, Canada and Japan still have a 3-day settlement cycle (T + 3) in place, while the EU, Hong Kong and South Korea have moved to T + 2. This delay in settlement drives a number of risks, which we will discuss in the following section.

In order to understand how blockchain technology could potentially enter into this field, it is useful to overview the lifecycle of a trade. Firstly, a buyer comes to an agreement with a seller for the purchase of a security. What follows then is referred to as clearing, when the two counterparties update their accounts and arrange for the transfer of the security and the associated money. This process entails[20]:

- Trade valuation;
- Credit monitoring;
- Position management;

[19] http://www.ifrs.org/current-projects/iasb-projects/financial-instruments-a-replacement-of-ias-39-financial-instruments-recognitio/documents/ifrs-9-project-summary-july-2014.pdf.

[20] Source: Risk management issues in central counterparty series, presentation by Priyanka Malhotra at the Systemic Risk Centre at LSE.

- Member reporting;
- Risk management;
- Collateral management;
- Netting of trades to single positions;
- Tax handling;
- Failure handling.

The actual exchange of the money and securities is termed settlement, and completes the cycle—this is typically 2 or 3 days after trade execution and can involve the services of institutions, such as custodians, transfer agents, and others (Bliss and Steigerwald 2006). In a typical trading-clearing-settlement cycle, the following actors are involved:

- On the trading side
  - The investors (buyer and seller) who wish to trade.
  - Trading members (one for the buyer and one for the seller) through which the investors can place their orders on the exchange.
  - The financial exchange or multilateral trading facility, where the trading members place the trades.

- On the clearing side
  - The clearing members, who have access to the clearing house in order to settle trades. These firms are also trading members, and thus settle their own trades, but non-clearing trading members have to settle through them.
  - The clearing house/CCP, which stands between two clearing members.

- On the settlement side
  - The two custodians, who are responsible for safeguarding the investors' assets. This role may also be played by a Central Securities Depository (CSD).
  - The settlement system.

Clearing and settlement can be bilateral, i.e. settled by the parties to each contract. This of course entails that risk management practices, such as collateralisation, are also dealt with bilaterally (Bliss and Steigerwald 2006). A large number of OTC (over-the-counter) derivatives used to be settled in this way, until recent efforts by the G20 resulted in regulation to impose central clearing.[21]

In central clearing, a third actor acts as a counterparty for the two parties in the contract and is termed the central counterparty (CCP). This simplifies the risk

[21] For an example of EU regulation in this area, see http://www.fca.org.uk/firms/being-regulated/meeting-your-obligations/firm-guides/emir.

management process, as firms now have a single counterparty to their transactions. Through a process termed novation, the CCP enters into bilateral contracts with the two counterparties, and these contract essentially replace what would have been a single contract in the bilateral clearing case. This also leads to some contract standardisation. In addition, there is a general reduction in the capital required, due to multilateral netting of cash and fungible securities. Duffe and Zhu (2011) discusses the effects of introducing a CCP for a particular class of derivatives. Examples of securities that are centrally cleared include equities, commodities, bonds, swaps, repos etc.

There are two main risks that are exacerbated by a longer settlement cycle:

- Counterparty risk between trade execution and settlement, and associated margin requirements. Because of these risks, clearing members are required to maintain capital with the CCP. One can see that faster execution times would minimise this risk, and thus minimise these capital requirements. As an example of this reduction, note that a 'move from T + 3 to T + 2 implies a 15 and 24 % reduction in the average Clearing Fund amount, during the typical and high volatility periods, respectively'[22]
- Settlement risk, or 'the risk that one leg of the transaction may be completed but not the other'(Bliss and Steigerwald 2006). Certain payment methods have been proposed to combat this issue, but it is obvious that a shorter settlement cycle would mitigate this further.

The two main types of settlement instructions are Delivery vs Payment (DvP) and Free of Payment (FoP), also termed Delivery versus Free.[23] The former ensures that delivery of the assets will only occur if the associated payment occurs. The latter method is simply a free delivery of assets, i.e. it is not associated with a payment, which occurs in a separate transaction. This obviously introduces a risk of non-payment by the buyer.

We next describe the possible blockchain structures that could be used to mitigate risks and increase efficiency.

## 5.1 Blockchain in the Settlement Cycle

In most applications of the blockchain, the advantages it brings are decentralisation and disintermediation. In the case of the trading-clearing-settlement cycle, we can envision the possibility of a consortium blockchain used at every level:

- At the financial exchange/multilateral trading facility level. For example, a consortium of brokers can set up a distributed exchange, where each of them

[22] BCG, Shortening the Settlement Cycle October 2012, available at http://www.dtcc.com/media/Files/Downloads/WhitePapers/CBA_BCG_Shortening_the_Settlement_Cycle_October2012.pdf.

[23] https://www.fanniemae.com/content/fact_sheet/dvp-dvf-comparison.pdf.

operate a node to validate transactions. The investors still trade through a broker (due to naked access regulations), but the exchange fees can be drastically reduced.

- At the clearing level. A consortium of clearing members can set up a distributed clearing house, thus eliminating the need for a CCP. Clearing then becomes closer to bilateral clearing, with the difference that the contract stipulations are administered through a smart contract, and thus there is less scope for risk management issues.
- At the settlement/custodian level.

A concrete example of how the entire lifecycle of a trade would look like is as follows: A buyer submits an order to buy a particular amount of an asset, for which there is an equivalent selling interest, through his broker. The buyer's and seller's brokers then create a transaction for the transfer of that amount of the asset, which is then transmitted to the distributed exchange network and verified. Once a block of transactions is verified, it is transmitted to the decentralised clearing house, where a new transaction is created, involving the brokers' clearing members. Once this transaction is verified in the clearing house blockchain, it is then transmitted to the settlement system, where a new transaction is created involving the custodians or CSDs, and the transfer of assets occurs automatically once this transaction is confirmed.

Such a configuration would firstly increase the speed of the entire settlement cycle from days to minutes or even seconds, where we would essentially have continuous settlement. There are a number of industry initiatives already in the digital asset transfer and settlement space, and we mention indicatively R3 CEV,[24] Digital asset holdings,[25] Symbiont,[26] Chain[27] and SETL.[28] HitFin[29] has proposed an alternative approach from the one described here, where trades are cleared bilaterally on a private blockchain, in less than 17 s. Besides the fast transaction settlement and automatic settlement of contracts upon maturity, all reporting, compliance and collateral management can be handled through the blockchain, thus reducing backoffice coss (Fig. 1).

[24] http://r3cev.com.

[25] http://digitalasset.com.

[26] http://symbiont.io.

[27] http://chain.com.

[28] http://setl.io.

[29] www.hitfin.com.

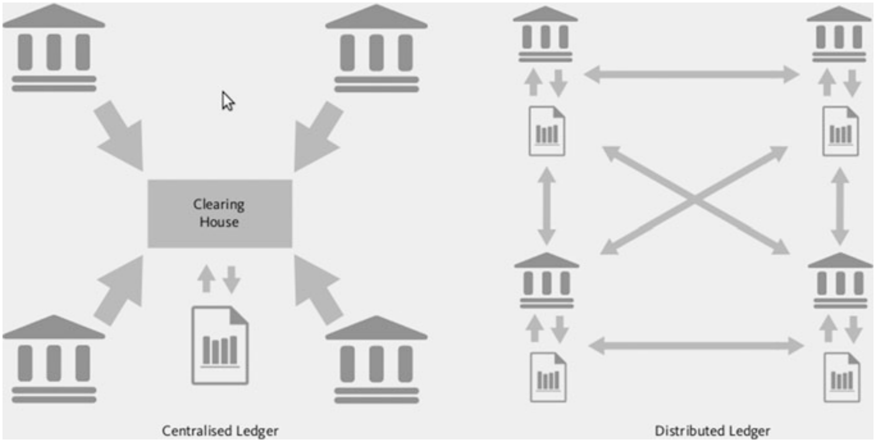


**Fig. 1** Clearing in a centralised and decentralised ledger. Image source: The Fintech 2.0 Paper: rebooting financial services, available at http://www.finextra.com/finextra-downloads/newsdocs/The%20Fintech%202%200%20Paper.PDF. In this instance, the blockchain version of clearing is a complete decentralisation where the roles of the exchange, the clearing house and the settlement system are no longer separated since they are combined into a single distributed blockchain architecture. However, once could argue that for reasons governance it may be more appropriate to consider intermediate architectures for blockchain decentralisation that still incorporates these separations of roles, such as the ones discussed in this section

## 6 Blockchain Technology and Multi-signature Escrow Services

To complete discussions on blockchain technologies and their applications in banking settings we mention some brief details on their influence in multi-signature Escrow services. This could be particularly beneficial for the banking ledger and settlement process applications described above as a means of resolving disputed financial transactions. As has been discussed above, some versions of blockchain technologies such as the version created for the bitcoin protocol require that the transactions are irreversible. This can be both beneficial and also a hinderance to the application of such technologies. Due to this feature, there is no aspect of dispute mediation present, as there would be with other electronic based payment systems. It has been reported, see Chap. 4 of Franco (2014), that as a result of this feature, the transaction processing costs of bitcoin based payment services are significantly lower than those of other remittance market services. Whilst the average fee for typical remittance market services is around 8–9 %, those currently available for Bitcoin payment services are only of the order of 0.01–0.05 %, largely due to the lower cost of not needing to process or perform disputes in transactions. However, for more general applications, this lack of reversibility can be problematic, see discussions in Buterin (2014a). Certainly, in many blockchain technology applications it may be beneficial to have an ability to make modifications or amendments to disputed transactions.

Ideas to achieve this have begun to be explored in settings of blockchain technology such as for payment or contract transfers involving multiple signatories via an Escrow service. An Escrow service will provide an opportunity to perform a dispute resolution between two transactions in the following manner. The two transacting parties identify a trusted intermediary party (Escrow service) who then provides them each with an electronic "address'' and maintains a private cryptographic key to control this address. Then to perform the transactions, agent A sends the information/e-property/e-money to a 2-of-3 multi-signature address. The addresses involved are those of the other party (agent B), the agent (A) and the Escrow service provider, then one has three possible outcomes to consider:

- The agent A may receive the information/e-property/e-money as agreed and in return they verify a transaction that releases the renumeration or alert of receipt to agent B through the 2-of-3 multisignature address to the Escrow agents address. The Escrow agent then signs the 2-of-3 multisignature address with their own key and publishes it on the blockchain.;
- If there is a problem with the contractual obligations agreed from agent A's perspective and agent B agrees with this, then agent B would sign the 2-of-3 multisignature address and send appropriate renumeration to agent A's address. Then Agent A upon receipt of this signs the 2-of-3 multisignature address and publishes it on the blockchain.
- If there is a dispute between agent A and agent B as to the contractual agreements and who should be remunerated, then the Escrow service provides an intervention. Here the Escrow service decides the outcome of the funds by signing the 2-of-3 multisignature address remunerating the appropriate party and then the party receiving renumeration signs the 2-of-3 multisignature address and publishes this on the blockchain. Note, in this third case the Escrow service would typically charge a fee.

We believe such approaches can be more widely adopted in blockchain technologies via automated smart contract structures.

## 7 Conclusions

This chapter has served to first highlight some of the recent innovations in the space of blockchain technologies. It has outlined some important aspects of blockchain architectures and their commonality and distinguishing features from different types of database structures. It has then described a number of features that are vital from a financial application perspective, including permissioning, data integrity, data security and data authenticity as well as important regulatory requirements relating to account provisioning for financial asset reporting, and the blockchain aspects that can help adhere to these. Then several innovative new areas of development for second generation blockchain technologies are detailed, including central bank treasury ledgers, retail and investment bank ledgers, trading, settlement and clearing processes, finishing with a discussion on multi-signature Escrow services. Like all prior disruptive technologies there will be beneficial and detrimental aspects of blockchain technologies that will need to be carefully considered prior to development and commercialisation of the ideas presented in this chapter. However, we believe that with the onset of the internet of money, the blockchain revolution will play an integral part in this brave new world.

## References

Barber, S., Boyen, X., Shi, E., Uzun, E.: Bitter to betterhow to make bitcoin a better currency. Financial Cryptography and Data Security, pp. 399–414. Springer (2012)

Bell, D.E., LaPadula, L.J.: Secure computer systems: mathematical foundations. Technical report. DTIC Document (1973)

Benkler, Y.: The Wealth of Networks: how Social Production Transforms Markets and Freedom. Yale University Press (2006)

Biba, K.J.: Integrity considerations for secure computer systems. Technical report. DTIC Document (1977)

Bliss, R.R., Steigerwald, R.S.: Derivatives clearing and settlement: A comparison of central counterparties and alternative structures. Econ. Perspect. **30**(4) (2006)

Buterin, V.: Multisig: The Future of Bitcoin (2014a)

Buterin, V.: A next-generation smart contract and decentralized application platform. White Paper (2014b)

Carter, J.L., Wegman, M.N.: Universal classes of hash functions. In: Proceedings of the ninth annual ACM symposium on Theory of computing, pp. 106–112. ACM (1977)

Clark, D.D., Wilson, D.R.: A comparison of commercial and military computer security policies. In: 1987 IEEE Symposium on. IEEE Security and Privacy, pp. 184–184 (1987)

Czepluch, J.S., Lollike, N.Z., Malone, S.O.: The Use of Block Chain Technology in Di_erent Application Domains (2015)

Denning, Dorothy E.: A lattice model of secure information ow. Commun. ACM **19**(5), 236–243 (1976)

Devanbu, P., Gertz, M., Martel, C., Stubblebine, S.G.: Authentic third-party data publication. In: Data and Application Security, pp. 101–112. Springer (2001)

Douceur, J.R.: The sybil attack. In: Peer-to-peer Systems, pp. 251–260. Springer (2002)

Duffe, D., Zhu, H.: Does a central clearing counterparty reduce counterparty risk? Review of Asset Pricing Studies, **1**(1), 74–95 (2011)

Elmasri, R., Navathe, S.B.: Fundamentals of Database Systems. Pearson (2014)

Franco, P.: Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley (2014)

Ge, X., Polack, F., Laleau, R.: Secure databases: an analysis of Clark-Wilson model in a database environment. In: Advanced Information Systems Engineering, pp. 234–247. Springer (2004)

Halevi, S., Harnik, D., Pinkas, B, Shulman-Peleg, A.: Proofs of owner- ship in remote storage systems. In: Proceedings of the 18th ACM conference on Computer and communications security, pp. 491–500. ACM (2011)

Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. Technical report. Cryptology ePrint Archive, Report 2015/675, 2015 (2015). http://eprint.iacr.org

Lamport, Leslie, Shostak, Robert, Pease, Marshall: The Byzantine generals problem. ACM Trans. Program. Lang. Syst. (TOPLAS) **4**(3), 382–401 (1982)

Merkle, R.C.: Protocols for public key cryptosystems. In: Null, pp. 122. IEEE (1980)

Merkle, R.C.: Secrecy, Authentication, and Public Key Systems (1979)

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

Pessoa, M., Williams, M.J.: Government cash management: relationship between the treasury and the Central Bank. Int. Monetary Fund (2013)

Peters, G.W., Panayi, E., Chapelle, A.: Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective (2015). arXiv preprint arXiv:1508.04364

Peters, G.W., Chapelle, A., Panayi, E.: Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: an operational risk perspective. Available at SSRN 2491991

Redmond, E., Wilson, J.R.: Seven databases in seven weeks: a guide to modern databases and the NoSQL movement. Pragmatic Bookshelf (2012)

Reid, F., Harrigan, M.: An Analysis of Anonymity in the Bitcoin System. Springer (2013)

Rosenfeld, M.: Overview of colored coins. White paper, bitcoil.co.il (2013)

Sandhu, Ravi S.: Lattice-based access control models. Computer **26**(11), 9–19 (1993)

Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. (2015)

Swanson, T.: (2015) Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems

Szabo, Nick: Formalizing and securing relationships on public networks. First Monday **2**(9), 31 (1997)

Tripunitara, Mahesh V., Li, Ninghui: The foundational work of Harrison-Ruzzo-Ullman revisited. IEEE Trans. Dependable Secure Comput. **10**(1), 28–39 (2013)

Wood, G.: Ethereum: a secure decentralised generalised transaction ledger (2014)

Yaker, I.F., Pattanayak, S.: . Treasury Single Account: an essential tool for government cash management. Int. Monetary Fund (2012)

Zyskind, G., Nathan, O.z., Pentland, A.: Enigma: Decentralized Computation Platform with Guaranteed Privacy (2015). arXiv preprint arXiv:1506.03471

## Author Biographies

**Dr. Gareth W. Peters** is an Assistant Professor in the Department of Statistical Science in University College London and a Principle Investigator in CSML , University College London (UCL) and an Academic Member of the UK PhD Center in Financial Computing (UCL). He has published in excess of 100 peer reviewed articles, 2 research text books on Operational Risk and Insurance as well as being the editor and contributor to 3 edited text books on spatial statistics and Monte Carlo methods. He holds positions as an Adjunct Scientist in the Mathematics, Informatics and Statistics, Commonwealth Scientific and Industrial Research Organisation (CSIRO) since 2009 as well being an Associate Member Oxford-Man Institute in Oxford University since 2012, an Associate Member Systemic Risk Center in London School of Economics since 2014; an Affiliated Prof. School of Earth and Space Sciences, Peking University PKU, Beijing, China since 2015 and a Visiting Prof. in the Institute of Statistical Mathematics, Tokyo, Japan each year since 2010.

**Efstathios Panayi** is currently working as a Data Scientist at Cumulus/City Financial while keeping his association with academia through an honorary research associate position at UCL. His academic research relates to liquidity modelling in equities markets, but he has also published work on the operational risk considerations of crypto-currencies for financial institutions.

# Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking

**Trent J. MacDonald, Darcy W.E. Allen and Jason Potts**

**Abstract** This chapter uses economic theory to explore the implications of blockchain technology on the future of banking. We apply an economic analysis of blockchains based on both new institutional economics and public choice economics. Our main focus is on the economics of why banks exist as organizations (rather than a world in which all financial transactions occurring in markets), and how banks are then impacted by technological change that affects transaction costs. Our core argument is that blockchains are more than just a new technology to be applied by banks, but rather compete with banks as organizations, enabling banking transactions to shift out of centralized hierarchical organizations and back into decentralized markets. Blockchains are a new institutional technology—because of how they affect transaction costs in financial markets—that will fundamentally re-order the governance of the production of banking services. We then explore this implication through broader political economy lens in which banking moves out of organizations and deeper into markets. We examine this as a form of institutional economic evolution in which the boundary of catallaxy—i.e., a self-organized economy—is enlarged, at the margin of the banking sector. Such institutional competition enables evolutionary discovery in the institutions of banking.

**Keywords** Blockchain · Bitcoin · Cryptocurrency · New Institutional Economics · Austrian Economics · Catallaxy

T.J. MacDonald · D.W.E. Allen · J. Potts (✉)
School of Economics, Finance & Marketing, RMIT University, Melbourne, Australia
e-mail: jason.potts@rmit.edu.au

T.J. MacDonald
e-mail: trent.macdonald@rmit.edu.au

D.W.E. Allen
e-mail: darcy.allen@rmit.edu.au

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_14

# 1 Introduction

This chapter uses economic theory to explore the implications of the blockchain technology on the future of banking. We apply an economic analysis of blockchain based on both new institutional economics and public choice economics (Davidson et al. 2016). Our main focus is on the economics of why banks exist as organizations (rather than a world in which all financial transactions occurring in markets), and how banks are then impacted by technological change that affects transaction costs. Our core argument is that blockchains are more than just a new technology to be applied by banks in the same way that computers and the internet have driven significant improvements in banking technology. If we were to think about blockchains in this way—from the perspective as a new technology to be adopted and diffused—banks would more or less remain the same. Instead, we argue that blockchains compete with banks as organizations, enabling banking transactions to shift out of centralized hierarchical organizations and back into decentralized markets. Blockchains are a new institutional technology—because of how they affect transaction costs in financial markets—that will fundamentally re-order the governance of the production of banking services. The upshot is that while banking itself may not fundamentally change, banks might. Blockchains, we argue, will alter the boundaries of self-organization; the question is why, and how?

The second half of this chapter explores this implication through broader political economy lens in which banking moves out of organizations and deeper into markets. We examine this as a form of institutional economic evolution in which the boundary of catallaxy—i.e., a self-organized economy (Hayek 1960)—is enlarged, at the margin of the banking sector. As blockchain technologies work through banking—at the margins of measurement, monitoring, and new forms of automated governance (e.g. smart contracts and Distributed Autonomous Organizations)—they will enable a deeper process of institutional evolution to begin to unfold (MacDonald 2015b). The permisionless and non-territorial character of this unfolding 'secession' of banking transactions—from hierarchically organized banks to spontaneously organized blockchains—reduces institutional exit costs. Such institutional competition enables evolutionary discovery in the institutions of banking.

We proceed as follows. Section 1 outlines the basic economics of banks as organizations in the provision of banking services. We argue banks exist because of the transaction costs of using markets in coordinating the supply and demand for financial services. Section 2 introduces the new economics of blockchain, based on new institutional and public choice economics. This discussion is centered on transaction cost economics and the economics of governance more broadly. Section 3 ties these arguments together to derive a first principles economic analysis of the effect of blockchain technology on banking. Section 4 then explores broader political economy implications of the institutional orders of a market economy.

## 2 A Bank Is a Firm that Intermediates a Market

Banking, finance, and payments services are among the oldest of industries. These commercial services predate modern capitalism, even emerging before modern governments (Ferguson 2008; Hodgson 2015). Many of the functions that banks serve are necessarily familiar to us: the movement and production of capital (savings, finance), and the operation of the payments system (money). That banks, and the economic functions they perform, have existed for thousands of years, and in all parts of the world, at all stages of economic development, suggests a robust economic function. But what precisely is the robust economic function that banks provide; why do banks persistently exist?

Put simply, banks provide the specialized function of securely storing liquid capital. For effectively any storable fungible assets banks are able to utilize scale economies associated with providing this service. These scale economies would also suggest oligopoly or even monopoly provision in a particular geographical region; that is, centralization. Centralizing the excess supply of capital opens the possibility of creating a new market by lending this capital out to those with excess demand, such that banks becomes an internal capital markets.

The economic role of banks in a market economy, like firms more generally, is to internalize externalities; and in doing so they form subeconomies (Holmstrom 1999). Metaphorically, banks can be viewed as miniature economies: "islands" of command organization in a "sea" of spontaneous market exchanges (Coase 1937). Moreover, the island economies are complete with their own "rules of the game" (Buchanan 1990), over which individuals (as borrowers and savers) can choose to opt in or out. To complete the metaphor, the banking industry is not a centralized supercontinent but an archipelago, due to the value of exit rights as an incentive mechanism and tool to discipline the abuse of power.

It is clear, then, that beyond the physical storage of precious metals and other financial assets, a bank in this sense is a *centralized ledger* of transactions, whether of capital or payments, which records balances between many different parties. A bank, in the modern sense, is an internalized market: it is an organization that functions as a platform (a two-sided market, Rochet and Tirole 2003) to match those with excess supply of capital (savers) with those with excess demand for capital (borrowers). Banks intermediate two sides of a market. This intermediation is precisely what the recent wave of P2P finance endeavors to disrupt. By matching sellers of capital (those who would otherwise make deposits in a bank) with buyers of capital (those who would otherwise seek loans from banks) directly, the P2P finance directly threatens banks.

Let us return to the simple economic question with which we began: why do banks exist? That is, why are reallocations of financial capital, including payments, not entirely undertaken as decentralized market transactions in the form of a two-party system, rather than in the three-party system with banks as the third party intermediating agent? This is what P2P finance is trying to create, but it hasn't quite got there yet. From what we have established above, these questions are equivalent to enquiring into the value of a centralized ledger itself.

The basic scheme of answer to this, we propose, uses New Institutional Economics (NIE), also known as Transaction Cost Economics (TCE) . This area of economics follows Nobel Laureate Ronald Coase (1937) who first explained the existence of firms in consequence of the transaction costs of using a market. For someone with a surplus of capital, the transaction costs of participating in a financial market would usually be prohibitively expensive. To find a borrower, write a contract, monitor the exchange, and enforce that contract would quite simply require huge amounts of capital, time and expertise. The owner of the surplus capital would also be sacrificing liquidity. A symmetric problem similarly exists for the demander; how does a borrower find a potential supplier that meets their idiosyncratic terms? Without banks many of these mutually welfare-enhancing exchanges would simply never take place.

This is a two-sided matching problem (Roth and Sotomayor 1992) that is greatly facilitated by the existence of a specialized third-party acting as both a focal point and aggregator to transform otherwise highly heterogeneous agents into liquid capital markets. Banks achieve this through capital pooling, through aggregation and disaggregation, information pooling, economies in monitoring, creating submarkets with different risk-reward profiles, through various specializations in writing and enforcing contracts, and bundling financial services. Banks create and harness reputational incentive mechanisms that enable them to enforce contracts at lower cost than could distributed agents because of their ability to exclude defaulting borrowers from subsequent access to finance. A third party also enables coordination across geographic regions through networks through economies of scale, as well as bundling together different types of financial services through economies of scope.

In sum, banks exist as third-party intermediating organizations because there are substantial costs—physical costs, information costs, coordination costs—with using the market to match the supply of and demand for financial assets (Earl and Dow 1982). Financial intermediaries such as banks have been the method for solving this problem for many centuries. Banks have been comparatively economic efficient, so to speak. The entrance of blockchains as crypto-secured distributed ledgers, however, disrupts these basic transaction costs of the market for financial assets. This then affects the economic logic and efficiency margins of banks, whose entire logic of existence derives from their comparative economic efficiency compared to markets. What, then, are the specific transaction costs margins at which blockchains will impact upon banks? This will be the subject of Sects. 2 and 3.

## 3 New Economics of Blockchain

### *3.1 Blockchain as a New General Purpose Technology*

A blockchain is a public decentralized ledger platform (Evans 2014; Swan 2015; Walport 2016). As a specific technology for digital currencies, the blockchain is a technical solution to the double-spending problem (what in computer science is called the ‘Byzantine General’s problem’) that hither-to had defeated all endeavors to create a non-centralized peer-to-peer electronic cash system (Dourado and Brito 2014). The blockchain solves this problem using a decentralized database (or ledger) with network-enforced processes that are based on a proof-of-work consensus mechanism for updating the database (Nakamoto 2008; Franco 2014).

The blockchain is best decoupled from its connection to Bitcoin because the economic value and disruptive potential of blockchain does not depend upon the value and prospect of Bitcoin (Buterin 2015). Blockchains are better understood as a new ‘general purpose technology’ (Bresnahan and Trajtenberg 1995; Lipsey et al. 2005) in the form of a highly transparent, resilient and efficient distributed public ledger (i.e., decentralized database). The general purpose technology is the blockchain and the many applications stemming from this invention are specific innovations (Pilkington 2016). The entrepreneurial problem of the blockchain is to discover such market applications (Allen 2016), which is a considerable challenge involving concurrent *institutional* innovations (i.e., in governance). This is because in principle such a distributed ledger can be applied to disrupt *any* centralized system that coordinates valuable information (Wright and De Filippi 2015; He et al. 2016; Walport 2016).

Ledgers are a very old technology. By the late twentieth century they have been digitized, but until invention of blockchain in 2008, they always remained centralized. The ledger is a technology of accounting, of keeping track of who owns what, and is instrumental to modern capitalism (Nussbaum 1933; Allen 2011; Hodgson 2015). But so too is trust in the ledger, which is most effective when it is centralized and strong, and so centralized ledgers for property titling, contracts, money, and so on, are also critical in connecting government to modern capitalism.

Centralized solutions are expensive and have many problems, particularly in relation to problems of trust and its abuse. Yet until very recently no effective decentralized solution has existed. In contrast, the blockchain technology is *trustless*, meaning that it does not require third party verification (i.e., trust), but instead uses a powerful consensus mechanism with cryptoeconomic incentives to verify authenticity of a transaction in the database. These properties also make blockchains safe. Security is maintained even in the presence of powerful or hostile third parties. In a recent lead article on blockchain—which they dubbed ‘The trust machine’—*The Economist* (2015) explained that:

> “Ledgers that no longer need to be maintained by a company—or a government—may in time spur new changes in how companies and governments work, in what is expected of them and in what can be done without them.”

There are many ways to think about the basic economics of blockchains. One method centers on why decentralized solutions to ledgers, now technically possible, are likely to become increasingly cost effective compared to centralized solutions. Along this line we could model the economics of blockchain as a new technology that is rapidly running down a learning curve, or equivalently as a technology cost curve rapidly falling, such that it becomes increasingly competitive against the mature technology of a centralized ledger, driving technological substitution. The innovation-adoption approach, for instance, underpins the study of cryptocurrencies from the perspective of modern monetary theory that recognizes the competitive efficiencies of private currencies (Böhme et al. 2015; Dwyer 2015; White 2015a; Luther 2015).

Another method views the economics of blockchain as an entrepreneur-driven technological competition, which is often met with political response (Olson 1965, 1982). Here we would expect that although centralized ledgers may not always be able to compete on cost, they can still compete through co-option of force, through enacting legislation or regulation to artificially drive up the cost of decentralized technologies (Hendrickson et al. 2015). As a new technology, the blockchain is in the early disruptive phase of the Schumpeterian process of 'creative destruction' (1942). Buterin (2015) argues that there is no 'killer app' for blockchain, just as there was not for open source, but rather a long tail of marginal use cases among particular groups, adding up to a lot. This diffusion trajectory will unfold as sequential applications are discovered and adopted along an entrepreneur-led market process of industrial dynamics in the adoption and diffusion of the new blockchain technology. But we propose a new view to the economics of blockchain: blockchain is an institutional governance technology of decentralization.

## 3.2 *Blockchain as a Technology of Decentralization, like a Market*

Blockchains are fundamentally a technology of decentralization. This suggests a different approach to the economics of blockchain, focusing on the economics of decentralized systems.

Open decentralized systems are centered on an evolutionary argument about *dynamic efficiency*. Evolving complex systems tend to develop from centralization to decentralization. Systems begin with centralization because this is the most efficient structure to create, establish and enforce rules, i.e., to create knowledge structures. This minimizes duplication and establishes clear hierarchy, and can adjudicate disputes. But those very features mean that centralization has costs that begin to accumulate as these powers become vulnerable to exploitation. In economic systems, this manifests as inflation, corruption, and rent seeking. Eventually, adaptation and differential selection drives such systems toward decentralization because the costs of centralization rise along the path of exploitation, while at the same time the costs of decentralization fall, often due to technological progress. Centralization brings order, but this order can be brittle, and adaptation toward decentralization begins to make the system more robust, flexible, secure and efficient.

The most general technological service blockchains perform is that they decentralize. They are a technology that pushes the governance of economic activity away from centralized organizations and toward decentralized markets. That is, blockchains can be conceptually be placed alongside markets, as an open platform technology (i.e., rule system) that performs this general service of decentralization (Potts 2001).

### 3.3 The Transaction Cost Approach to Blockchain

Blockchains are best understood as a new institutional technology that makes possible new types of contracts and organizations. Viewed through the lens of transaction cost economics, organizations and markets are alternative economic institutions for economic coordination—i.e., for organizing and governing transactions—and therefore the efficient mix of institutions in an economy will emerge as agents economize on transaction costs. Economizing on transaction costs leads to an efficient institutional structure of economic organization and governance.

In the economic theory of efficient governance (Williamson 1979, 1985), bounded rationality implies that contracts will be incomplete, while asset specific (idiosyncratic) investments bring the threat of opportunism. Quasi-rents due to investments in specific assets, where the value of those investments depends upon equally specific investments by others, creates *ex post* hazards of opportunism. That is, one party can exploit another through hold-up or bargaining after investments have already been made. These transactions costs can be economized through the use of efficient governance structures.

So why do some transactions occur in firms (hierarchies) rather than in markets? Put simply, different governance structures deal with different economic problems in different ways. Because of uncertainty, asset specificity and associated opportunism, and frequency of dealings, some transactions are more efficiently conducted in hierarchies rather than markets. For instance, markets are often efficient governance institutions for spot contracts (a pure exchange economy). In other scenarios, where economic activity requires coordinated investment through time (due to asset specificity), or an ongoing relation between parties (due to frequency), or involves uncontractable dealings (due to uncertainty), alternative governance institutions such as firms or relational contracting can be efficient ways to economize on transaction costs.

The boundary between the firm and the markets—i.e., which transaction occurs under what governance structures—is some function of the transaction costs and characteristics of different governance institutions. What, then, is this transaction cost economics logic applied to blockchains? The relevant question then is why do (or might) some transactions occur in blockchains, rather than in firms or markets?

### 3.4 A Blockchain Is a Catallaxy

Once we see blockchains as alternative governance institutions—alongside firms, markets and relational contracting—it is a short step from there to see that by adding a few more operational features—constitutions or foundational governing rules (Hayek 1960; Buchanan 1990), collective decision-making rules and procedures (Buchanan and Tullock 1962; Ostrom 1990), and private money (Hayek 1978)—blockchains appear as a technology for making economies. That is, a blockchain creates a self-organizing and constitutionally ordered catallaxy, or what MacDonald (2015c) has labeled a 'constellaxy'.

In this new view blockchains are not organizations; blockchains are spontaneous organizations which compete with organizations. But blockchains aren't markets, either. Blockchains have market-like properties, but their role is to facilitate transactions, not (just) exchange. Fundamentally blockchains coordinate a distributed group of people, making them actually closer to being an economy.

F. A. Hayek was a pioneer of the study of decentralized economies and distributed information processing. He defined an *economy* as an organization or an arrangement in which someone conspicuously uses means in the service of a uniform hierarchy of ends. Hayek's point was to distinguish the concept of an economy from the spontaneous order brought by the market—for which he preferred the term catallaxy. For Hayek,

> "a catallaxy is a special kind of spontaneous order produced by the market by people acting within the rules of the law of property, tort and contract" (1982: 269).

From the Hayekian perspective then, blockchains are actually catallaxies, not economies, for they serve not one particular end "but contribute to the realization of a number of individual objectives which no one knows in their totality". A catallaxy is characterized by a multitude of agents living within an 'extended order' (Hayek 1988). Blockchains are 'orders of economies' in the same way a market order is a catallaxy of mutually adjusting individual plans (economies). The first remarkable property of emergent economies built on blockchains is that they are non-territorially unbundled (MacDonald 2015d). Second, the price system in Hayek's conception operates at the level of a system of markets, as in a region or nation, but a further surprising property of blockchains is that they provide a mechanism to radically *reduce* the size and scale of effective catallaxies.

## 4 What the Economics of Blockchains Implies for Banking

We can now furnish some broad outlines based upon economic theory—or what are sometimes called 'pattern predictions' (Hayek 1964, 1989)—about the future of how blockchains might develop in banking. Above, we identified the relevant theory as the economics of technological dynamics, new institutional economics, and public choice economics. Our aim here should not in any way be taken to be equivalent or even comparable to specific identification of entrepreneurial opportunities from blockchains, nor do we seek to outline specific risks arising from their adoption (Tasca 2015). We do not wish to be seen to underestimate the immense entrepreneurial problem underpinning the discovery of applicable opportunities for blockchains (Allen 2016) or the potentially immense societal impacts from systemic diffusion of the technology (Atzori 2015; MacDonald 2015a). Rather, our framing is limited to: how could blockchain technology impact the economic organization of banking, and what are the relevant economic models to use in order to think about this problem?

The first clear point we sought to highlight was to challenge the otherwise seemingly compelling notion that blockchain is simply a new ICT-like technology that will be adopted into banks, thus improving the competitive efficiency of banks that adopt this technology, and harming the competitive position of banks that are slower to adopt (Chuen 2015). The model for understanding this would be, say, adoption of other general purpose banking technologies such as debit cards, ATMs or internet banking. This is a dominant thesis at the time of writing among banks who view this as a way to improve back-office efficiency in clearing transactions (for example consortiums such as Ripple). This, however, may be a mischaracterization of the nature of the blockchain technology.

What type of technology is a blockchain? As a new technology of decentralization, blockchains can then be understood to be a new competitor to the central objects that economics studies: markets. When coupled with token systems, blockchains seem to describe institutional orders that we might reasonably call an economy, or following Hayek (1960), a catallaxy. A blockchain is in this sense an unusual technology in that while manifestly an information and computation technology (an ICT)—viz. a blockchain is a new technology for public databases of digital information—blockchains are actually better understood as an institutional or social technology for coordinating people.

What, then, is the margin of competition for blockchains? As a new general purpose technology, there is a great deal of interest in the way in which existing firms and industries will adopt and use blockchains. This includes consortium and private blockchains, where restricted access protocols are used instead of trustless cryptoeconomic incentives. But the question we have sought to focus on here, through the lens of transaction cost economics, is not how firms and markets will adopt and use blockchains, but rather how blockchains will compete with firms and markets.

By adopting the Coase and Williamson perspective in which firms, markets, relational contracts, and now also blockchains, are alternative governance institutions—whose relative efficiency is determined by micro-institutional transaction cost considerations—we can understand how blockchains compete with banks, rather than being viewed as a technology adopted by banks. This is only visible when we view the basic analytic unit of blockchain economics as the transaction (i.e., the executable contract). This is the fullest expression of blockchains not as a new informational and communications technology, but as a new institutional technology.

Blockchains, as a new institutional technology, are a cryptoeconomic mechanism through which individuals can govern the difficulties inherent in transacting. There is one particular transaction difficulty that has long been dealt with through a hierarchical organization: opportunism. The presence of opportunism in many transactions makes hierarchies and relational contracting more transaction cost efficient mechanisms of governance. But blockchains look to have changed these comparative governance efficiencies—particularly through smart contracts and DAOs (Buterin 2014a, b)—by eliminating opportunism. Therefore blockchains, as institutional technologies, undermine the strong case for the economic efficiency of hierarchies (which exploits incomplete contracts) and relational contracting (which requires trust between parties) over markets. Where blockchains can eliminate opportunism they will, at least theoretically, outcompete traditional organizational hierarchies and relational contracts.

# 5 The New Political Economy of Blockchain

## *5.1 Cryptosecession to Blockchain Economies*

Because blockchain is a new institutional governance technology, agents must decide whether to remain within the structures of markets and hierarchies, or secede to the new institutions of decentralization. As such, MacDonald (2015a), building on the foundational work of Buchanan and Faith (1987), explains how the interplay between blockchain technology and hierarchical institutions may lead to a political-economic rupture called 'cryptosecession'. The mechanism of cryptosecession—partial, non-territorial, and permissionless exit from incumbent institutions—enables us to build a new political economy of blockchains, which is the task of this section (cf. Kostakis and Giotitsas 2014).

Blockchains are fundamentally a mechanism of cryptosecession, where agents can escape the now less than optimal mechanisms of banking and money. Cryptosecession has so far been applied to the fiscal process, with similar domain claims possible about cryptolaw (De Filippi 2014; Wright and De Filippi 2015), cryptomoney (Hayek 1978; White 2015), and cryptofinance (Harvey 2015; Scott 2016).

The immediate implication of cryptosecession is that the *overtaxing proclivities* of governments must be severely curtailed, such that fiscal exploitation is reduced and eventually eliminated as the capability of citizens to cryptosecede increases and becomes absolute. That is, the balance of citizen opacity and government legibility —which is a function of the development of cryptographic and blockchain technologies—determines the balance of fiscal exploitation versus equivalence.

For cryptolaw the implication becomes that the *overregulating proclivities* of government must be curtailed (De Filippi 2014), such that the level of 'optimally exploitative' regulation (Stigler 1971; Peltzman 1976) must be reduced in respect of the capabilities of entrepreneurs and businesses operating on the cryptosecession frontier. This all depends on the viability of secession from the 'physical' jurisdiction of governments. Seceding from this physical jurisdiction, however, may be limited in certain entrepreneurial contexts. An example of successful cryptosecession from incumbent regulatory institutions, ironically, is the very development of cryptographic and blockchain technologies and applications. Notwithstanding, crypto and blockchain innovation is beginning to attract the attention of regulatory authorities (De Filippi 2014; Brito 2015; Peters et al. 2015). But the basic mechanism remains: to the extent that entrepreneurial activity can be excised from the regulatory reach of the state, via cryptographic blockchain technologies, regulatory capture will be diminished.

For cryptomoney the hierarchical institution is the central bank (and fiat money) and their interest rate manipulation, inflation, and currency debasement (White 1999; Hayek and White 2007; White 2015). Seen in this light, cryptocurrencies are actually a vehicle of monetary cryptosecession. Their primary purpose is not to emulate some definitive and optimally efficient monetary setting, but rather to permit citizens to escape the circumstances of 'optimal monetary exploitation' (in which certain individuals and businesses are advantaged by monetary policy settings at the expense of others) if even for only marginally improved institutions. Accordingly, as monetary cryptosecession becomes more potent an intensifying competitive dynamic between the incumbent institution (central banks) and potential competitors (bitcoin and other cryptocurrencies) should see the parameters of monetary policy shifted in the direction of 'sound money'. Again, much like fiscal cryptosecession, this is limited by the development of cryptocurrencies; i.e., their position on the spectrum of opacity-legibility (which is relatively high) but also by the extent of the market for cryptocurrencies (which is still trivially small) (White 2015; MacDonald 2015a).

The political economy of blockchains also applies in the banking and finance industries. That is to say the cryposecession dynamic threatens not only incumbent hierarchical institutions of government, but also legacy banking and financial organizations and markets. Blockchains seem apt to outcompete banks (as hierarchical organizations) and relational market contracting (as trust requiring transactions), which are both prone to opportunism. When banks and peer-to-peer finance (*sans* blockchains) succumb to this shortcoming there is essentially a redistribution of value from one party to another, which is analogous to the cases of fiscal, regulatory, and monetary predation outlined above. Thus in the political economy perspective the blockchain imperative derives not *only* from a drive to economy-wide efficiency as a recalibration of the institutions in which banking and finance take place. There is also a game-theoretic logic at play here, in which it is individually rational for those currently or potentially harmed by opportunism to secede to blockchains (if only to unwind predation and even in a zero-sum context). Again, this is limited by the extent of the market for cryptofinanceand the development of its technology.

## 5.2 Blockchains and Institutional Exit Costs

We can also examine the ability of individuals to exit their current institutional environment using blockchains. In this view, what blockchains really do, and what we argue in this section, is radically reduce institutional exit costs. There are two main ways blockchains reduce exit costs. The first is through reducing the *transition costs* because of their *permissionless nature* (Thierer 2014). That is, blockchains drastically reduce the cost of moving from one institution to another, especially in relation to state-imposed barriers. The second is through reducing the *opportunity costs* because of their *non-territorial nature*. That is, because blockchains operate through the non-territorial internet, they enable agents to *partially exit* their current institutions. Combining these two cost reductions we conclude that blockchains significantly ease individuals' institutional exit to the cryptoeconomy.

The transition from one institutional setup to another—say from banking organizations within financial markets to a blockchain-based financial system—does not occur in costless meta-institutions (Pagano and Vatiero 2015). Quite apart from the distribution of transaction costs within competing setups, we cannot theorise a frictionless transitional process between institutions. The process is better thought of as subject to a kind of meta-institutional *transition cost*. These are equivalent to mobility costs in the jurisdictional arbitrage setting.

States (governments) are the main arbiters of such institutional transition costs. If states intervene in decisions to switch between institutions—say by either inhibiting with regulation or outright prohibiting the use of blockchain and cryptographic technology—then exit costs will be higher. This might happen because states themselves wish to regulate or deter the exit to new institutions, for whatever reason, or at the behest of vested interests (e.g. banking industry).

By 'permissionless exit' we mean that there is no additional cost on top of the meta-institutional transition cost such (e.g. a manipulated component; Twight 2004) as would affect the transition to blockchains at the margin. The strong-form claim often made is that due to the cryptographic nature of blockchain technology it is resistant to state intervention and regulation, and is thus 'permissionless' per definition.

Aside from transition costs, we must also consider how complementary institutions affect their costs (Pagano and Vatiero 2015). When choosing between institutional setups one must consider *opportunity costs*. Only when we think about opportunity costs does the non-territorial nature of blockchain economies become important. In territorial systems the opportunity costs relate to the sacrifice of benefits of seceding from one geographical location to another.

Blockchain economies are coordinated via the internet, which is fundamentally a non-territorial space. Individuals need not sacrifice the benefits of conducting economic activities in particular locations. They can *partially* exit from, say, the banking system of their current locale without having to physically move to the location or jurisdiction of the banking system they prefer. The opportunity costs of institutional arbitrage are small, converging on zero. Institutions follow the individual, not the other way around. And they do so in a piecemeal or unbundled fashion. Essentially this is the hyper-realization of globalization achieved through ICT technology, and further accentuated by blockchain technology.

Cryptographic blockchain technology reduces institutional exit costs through the permissionless and non-territorial character of the institutional change it engenders.

This depends on two things: (1) blockchain technology is needed to create viable exit options; while (2) cryptographic technology is needed to keep those exit options open. First, the viability of exit is defined as the scope of and extent to which economic activity can be dissociated from legacy institutions and migrated to blockchain institutions. Clearly exit cannot proceed (permissionless or otherwise) for those activities for which there are no competing blockchain institutional options available. Similarly, because blockchain economies are coordinated via the internet (which is a non-territorial space) exit can be deterritorialized only to the extent that activity can be migrated to blockchain institutions. Second, the viability of exit depends on the extent to which cryptographic exit can create a genuine veil of opacity between transactions and states (e.g. a veil between polity and economy). If this is the case then exit will be permissionless in the sense that governments cannot intervene (e.g. neither in the creation of parallel institutions or choice to exit to them), and non-territorial because state borders will no longer demarcate transactions.

## *5.3 Blockchains and Institutional Evolution*

The upshot of radically reduced institutional exit costs is greater competition; not between organizations, markets, and institutions *within* the banking industry, but between these incumbents and new blockchain based ones. Competition as an evolutionary, knowledge-generating process is a central idea in both Austrian and evolutionary economics (Hayek 1948; Vihanto 1992; Wohlgemuth 2008). Thus the emergence of blockchains has stimulated a kind of meta-intuitional evolution, and this elicits a knowledge-generating discovery process at the level of orders of economies. With the advent of blockchains we stand to discover which institution best governs financial transactions: markets, firms, or blockchains?

Evolutionary theory tells us that the strength of the variation and selection mechanisms—that is, the number of parallel experiments and the ease of citizen exit respectively—determine the rate of institutional evolution. Through this lens we can hypothesise that the mechanism of cryptosecession will intensify discovery processes by accelerating the rate of intuitional evolution. This is because both the selection mechanism (exit of people) and the source of variation (entrepreneurial conjectures) are permissionless and thus heightened. Low switching costs (permissionless exit) strengthen the selection mechanism, while low barriers to entry (permissionless innovation) means a more vibrant source of variation.

Parallel experimentation is a fundamental dynamic efficiency scheme to enhance and accelerate variation, innovation, and evolution (Ellerman 2014). Due to the non-territorial character of blockchains there can be multiple orders of economies tested at a time—i.e., both legacy banking and new cryptobanking at once—a laboratory of parallel experimentation *par excellence*. In much the same way that territorially decentralized intuitional experimentation is conceptualized as 'laboratory federalism', MacDonald (2015d) describes the theory of the discovery process through non-territorial institutional competition—as per emergent economies built on blockchains—as 'laboratory panarchism.' The final analysis of the political economy of blockchains can therefore by labeled 'evotopian' (Hodgson 1999): blockchains cultivate an evolutionary learning process that will coordinate the discovery of improved institutions for governing banking transactions.

## 6 Conclusion

There are two basic economic lenses through which to view the economics of blockchain. The first is to view the economics of the adoption and diffusion of the blockchain as powerful new *ICT technology*. Such a technology-based approach is currently the default perspective in the finance and banking sector, viewing blockchain as a new technology that will be adopted differentially by some banks, leading to a further round of technological competition in the banking sector. The conclusion to this view is to expect the same market process as we have seen with other technologies: some banks will adapt and prosper, others will lag and collapse. Their success will depend on their strategic choices and uses of this new technology to drive productivity and competitive efficiency.

But there is also a second economic perspective, focusing not on technology, but on governance. This view based on economic reasoning, begins by asking what type of technology is blockchain. The answer to that question, we have argued in this chapter, is that blockchain is fundamentally a technology of decentralization and is therefore better understood as a new *institutional technology* for coordinating people—i.e., for making economic transactions—which then competes with firms and markets. This path seeks to understand what economic transactions currently occurring in firms or markets will shift to blockchains.

The new institutional economics and public choice economics of blockchains emphasize disintermediation and decentralization. In a world of blockchains the functions and operations of banking may not change, but the economic organization of banking may shift significantly. In this view, it is banks that will experience fundamental shifts in their organizational boundaries, with many transactions currently governed through hierarchy, relational contracting or market transactions shifting to the blockchain as an outworking of economic efficiency over transaction costs.

Blockchain is a technology for internal exit from incumbent institutions. Simultaneously it is a technology for the creation of new institutions. The upshot of this is emergent economies built on blockchains. This is a political-economic rupture and bifurcation in which an incumbent institutional order precipitates a constellaxy—a constitutionally ordered catallaxy. The relevance of the development of blockchains for banking is that it has shifted the boundary between hierarchical banking organizations and non-territorial, spontaneously ordered, self-organizing economies. This transition suggests the future of banking will be conducted in more evolvable and dynamically efficient institutions of governance.

**Acknowledgments** This chapter draws heavily on, and in part reproduces, material previously published in Davidson et al. (2016), and also MacDonald (2015a).

## References

Allen, D.W.: The institutional revolution: measurement and the economic emergence of the modern world, University of Chicago Press (2011)

Allen, D.W.E.: Discovering and developing the blockchain cryptoeconomy (2016). http://ssrn.com/abstract=2815255

Atzori, M.: Blockchain technology and decentralized governance: is the state still necessary? (2015). http://ssrn.com/abstract=2709713

Böhme, R., Christin, N., Edelman, B., Moore, T.: Bitcoin: Economics, technology, governance. J. Econ. Perspect. **29**(2), 213–238 (2015)

Bresnahan, T.F., Trajtenberg, M.: General purpose technologies 'Engines of growth'? J. Econom. **65**(1), 83–108 (1995)

Brito, J.: The Law of Bitcoin, iUniverse (2015)

Buchanan, J.M.: The domain of constitutional economics. Const. Polit. Econ. **1**(1), 1–18 (1990)

Buchanan, J.M., Faith, R.: Secession and the limits of taxation: Toward a theory of internal exit. Am. Econ. Rev. **77**(5), 1023–1031 (1987)

Buchanan, J.M., Tullock, G.: The Calculus of Consent, University of Michigan Press (1962)

Buterin, V.: DAOs, DACs, DAS and more: an incomplete terminology guide, Ethereum Blog (2014a). https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

Buterin, V.: Ethereum whitepaper: A next generation smart contract and decentralized application platform (2014b). https://www.ethereum.org/pdfs/EthereumWhitePaper.pdf

Buterin, V.: Visions part I: The value of blockchain technology (2015). https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology/

Chuen, D.L.K.: Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data, Academic Press (2015)

Coase, R.H.: The nature of the firm. Economica **4**(16), 386–405 (1937)

Davidson, S., De Filippi, P., Potts, J.: Economics of blockchain (2016). http://ssrn.com/abstract=2744751

De Filippi, P.: Bitcoin: a regulatory nightmare to a libertarian dream. Internet Policy Rev. **2**(2), 1–11 (2014)

Dourado, E., Brito, J.: Cryptocurrency. In: Durlauf, S.N., Blume, L.E. (eds.) The New Palgrave Dictionary of Economics (2014) http://www.dictionaryofeconomics.com/article?id=pde2014_C000625

Dwyer, G.P.: The economics of Bitcoin and similar private currencies. J. Financ. Stab. **17**, 81–91 (2015)

Earl, P., Dow, S.: Money Matters, Harvester Wheatsheaf (1982)

Economist: The promise of the blockchain: The trust machine (2015). http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine

Ellerman, D.: Parallel experimentation: a basic scheme for dynamic efficiency. J. Bioecon. **16**(3), 259–287 (2014)

Evans, D.: Economic aspects of Bitcoin and other decentralised public-ledger currency platforms', Coase-Sandor Institute for Law and Economics, working paper#685 (2014)

Ferguson, N.: The Ascent of Money: A Financial History of the World, Penguin Books (2008)

Franco, P.: Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley (2014)

Harvey, C.: 'Cryptofinance'(2015). http://ssrn.com/abstract=2438299

Hayek, F.A.: Individualism and Economic Order, University of Chicago Press (1948)

Hayek, F.A.: The Constitution of Liberty, University of Chicago Press (1960)

Hayek, F.A.: The theory of complex phenomena. In: Bunge, M. (ed.) The Critical Approach to Science and Philosophy: Essays in Honour of Karl Popper. Transaction Publishers (1964)

Hayek, F.A.: The Denationalization of Money: The Argument Refined. Institute for Economic Affairs (1978)

Hayek, F.A.: Law, Legislation and Liberty: A New Statement of the Liberal Principles of Justice and Political Economy. Routledge (1982)

Hayek, F.A.: The Fatal Conceit: The Errors of Socialism. Routledge (1988)

Hayek, F.A.: The pretence of knowledge. Am. Econ. Rev. **79**(6), 3–7 (1989)

Hayek, F.A., White, L.H.: The Pure Theory of Capital. University of Chicago Press (2007)

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Sedik, T.S., Stetsenko, N., Verdugo-Yepes, C.: Virtual Currencies and Beyond: Initial Considerations. International Monetary Fund (2016)

Hendrickson, J.R., Hogan, T.L., Luther, W.J.: The political economy of bitcoin. Econ. Inq. **54**(2), 925–939 (2015)

Hodgson, G.M.: Economics and Utopia: Why the Learning Economy is not the End of History. Psychology Press (1999)

Hodgson, G.M.: Conceptualizing Capitalism. University of Chicago Press (2015)

Holmstrom, B.: The firm as a subeconomy. J. Law. Econ. Organ. **15**(1), 74–102 (1999)

Kostakis, V., Giotitsas, C.: The (a)political economy of Bitcoin'. Commun. Capital. Crit. Open Access J. Glob. Sustain. Inf. Soc. **12**(2), 431–440 (2014)

Lipsey, R., Carlaw, K., Bekhar, C.: Economic Transformations: General Purpose Technologies and Long Term Economic Growth. Oxford University Press (2005)

Luther, W.J.: Cryptocurrencies, network effects, and switching costs. In: Contemporary Economic Policy (2015). http://onlinelibrary.wiley.com/doi/10.1111/coep.12151/abstract

MacDonald, T.J.: Cryptosecession and the limits of taxation: Toward a theory of non-territorial internal exit (2015a).http://ssrn.com/abstract=2661226

MacDonald, T.J.: Spontaneous order in the formation of non-territorial political jurisdictions (2015b). http://ssrn.com/abstract=2661250

MacDonald, T.J.: The social media spontaneous order is a constellaxy. J. Brief Ideas (2015c). http://beta.briefideas.org/ideas/2e9e15b6adb3e76e44f4cf2a9f8f9a01

MacDonald, T.J.: The unbundled state: Economic theory of non-territorial unbundling. In: Tucker, A., de Bellis, G.P. (eds), Panarchy: Political Theories of Non-Territorial States. Routledge (2015d)

Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf

Nussbaum, F.: A History of the Economic Institutions of Modern Europe: An Introduction of 'Der Moderne Kapitalismus' of Werner Sombart. Crofts (1933)

Olson, M.: The Logic of Collective Action. Harvard University Press (1965)

Olson, M.: The Rise and Decline of Nations. Yale University Press (1982)

Ostrom, E.: Governing the Commons: The Evolution of Institutions for Collective Action. Cambridge University Press (1990)

Pagano, U., Vatiero, M.: Costly institutions as substitutes: Novelty and limits of the Coasian approach. J. Inst. Econ. **11**(2), 265–281 (2015)

Peltzman, S.: Toward a more general theory of regulation. J. Law. Econ. **2**, 211–240 (1976)

Peters, G.W., Panayi, E., Chapelle, A.: Trends in crypto-currencies and blockchain technologies: a monetary theory and regulation perspective (2015). http://ssrn.com/abstract=2646618

Pilkington, M.: Blockchain technology: Principles and applications. In: Olleros, F.X., Zhegu. M. (eds.) Research Handbook on Digital Transformations. Edward Elgar (2016)

Potts, J.: Knowledge and markets. J. Evol. Econ. **11**(4), 413–431 (2001)

Rochet, J.C., Tirole, J.: Platform competition in two-sided markets. J. Eur. Econ. Assoc. **1**(4), 990–1029 (2003)

Roth, A.E., Sotomayor, M.A.O.: Two-Sided Matching: A Study in Game-Theoretic Modeling and Analysis. Cambridge University Press (1992)

Schumpeter, J.A.: Capitalism, Socialism and Democracy. Harper & Brothers (1942)

Scott, B.: How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?. United Nations Research Institute for Social Development (2016)

Stigler, G.J.: The theory of economic regulation. Bell J. Econ. Manag. Sci. **2**, 3–21 (1971)

Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media (2015)

Tasca, P.: Digital Currencies: Principles, trends, opportunities, and risks (2015). http://ssrn.com/abstract=2657598

Thierer, A.: Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom. Mercatus Center at George Mason University (2014)

Twight, C.A.: Political transaction-cost manipulation. In: Rowley, C., Schneider, F. (eds.) The Encyclopedia of Public Choice. Springer (2004)

Vihanto, M.: Competition between local governments as a discovery procedure. J. Inst. Theor. Econ. **148**(3), 411–436 (1992)

Walport, M.: Distributed Ledger Technology: Beyond Blockchain. UK Government Office for Science (2016)

White, L.H.: The Theory of Monetary Institutions. Blackwell (1999)

White, L.H.: Inflation and the Federal Reserve: The Consequences of Political Money Supply, Cato Policy Analysis (2015). http://www.cato.org/publications/policy-analysis/inflation-federal-reserve-consequences-political-money-supply

White, L.H.: The market for cryptocurrencies. Cato J. **35**(2): 383–402 (2015a)

Williamson, O.E.: Transaction cost economics: the governance of contractual relations. J. Law. Econ. **22**(2), 233–261 (1979)

Williamson, O.E.: The Economic Institutions of Capitalism. Free Press (1985)

Wohlgemuth, M.: Learning through institutional competition. In: Bergh, A., Höijer, R. (eds.) Institutional Competition. Cheltenham (2008)

Wright, A., De Filippi, P.: Decentralized blockchain technology and the rise of Lex Cryptographia (2015). http://ssrn.com/abstract=2580664

## Author Biographies

**Trent MacDonald** is a postdoctoral economist with the School of Economics, Finance and Marketing at RMIT University and the Swinburne Institute for Social Research at Swinburne University, both in Melbourne. He coordinates Melbourne Crypto, which is a multidisciplinary, multi-institute research network for legal, social, and economic approaches to blockchain studies. His research employs institutional economics, public choice theory, and Hayekian political economy to study non-territorial political systems.

**Darcy Allen** is an economics doctoral candidate in the School of Economics, Finance and Marketing at RMIT University. His work focuses on applying new institutional economics to entrepreneurial discovery. Darcy is also Research Fellow at the Institute of Public Affairs in Melbourne, where his work focuses on the relationship between regulation and emerging industries.

**Jason Potts** is Professor of Economics at RMIT University and Adjunct Fellow at the Institute of Public Affairs. He works in areas of economic evolution, technological change, institutional economics, economics of innovation, economics of cities, and the economics of cultural and creative industries. His current research builds on the work of Elinor Ostrom to develop the concept of innovation commons.

# Blockchain 2.0 and Beyond: Adhocracies

**Mihaela Ulieru**

**Abstract** This concluding chapter offers a book synopsis. Parsing the chapters which follow the evolution of decentralized platforms from initial attempts at peer to peer lending and crowdfunding to new market dynamics enabled by blockchain rooted, smart contract fueled P2P platforms—we reveal the ultimate quest in deploying this social technology for building new economies.

**Keywords** Synopsis • P2P platforms evolution • Social technology • New economy • Self-organizing communities • Adhocracies • Catallaxies

Current institutional structures are drastically challenged by the rate of change of society, technology and the environment which far outstrips their capacity to adapt. Governments and international organizations are losing their legitimacy to competition from entirely new structures of collective action emerging from adhocracies, aka self-organising Information Communication Technologies (ICT)-enabled groups and communities (Ulieru 2014). We consider four key factors fuelling institutional change under the above mentioned disruptions. Firstly, that individuals, ICT-enabled devices and conventional institutions are now deeply entangled. Secondly, that is it possible to equip those devices with social intelligence to be equal participants in society (Brynjolfsson and McAfee 2014). Thirdly, that out of the entanglement and the intelligence, new dynamical structures emerge which are more responsive, have greater agility and are less prone to path dependency and this socio-technical entanglement can lead to the emergence of high quality constructive social processes (Ulieru and Doursat 2011). And finally, that people still retain the power to self-organise these structures and self-regulate their behaviour in the context of these structures according to agreed rules (Chase 2015).

The book features pioneering attempts at deploying new economic models which move the field from describing monetary flows to understanding complex social processes that underlie the dynamics of the economy. It begins by describing

M. Ulieru (✉)
Impact Institute for the Digital Economy, Ottawa, Canada, USA
e-mail: mihaela@theimpactinstitute.org

P. Tasca et al. (eds.), *Banking Beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4_15

the socio-economic nature and legal challenges brought about by the emergence and proliferation of P2P platforms. On this basis various alternatives to the centralized approaches that rule the current financial sector—which lost its legitimacy in 2008 by not keeping its promises to its customers—are exposed.

Pelizzon, Rieder and Tasca in the Chapter "Classification of Crowdfunding and P2P Lending in the Financial System" give an overview of the first P2P platforms that enabled new market structures to emerge, such as Crowdfunding. If the emergence of P2P platforms may somehow be related to banks being under stress as claimed by Blaseng and Koetter in the Chapter "Crowdfunding and Bank Stress", FinTech has continued to provide cost effective platforms as an alternative to traditional banking. In "How Peer to Peer Lending and Crowdfunding drive the FinTech Revolution in the UK" Chisti explains the role of P2P lending and P2P equity markets as the drivers of the alternative finance revolution which in the UK is experiencing some of the highest growth rates in the world. Apart from the UK, P2P technology-enabled platforms are speedily replacing the traditional banking services also in Asia. In particular, Barberis and Arner in the Chapter "From Shadow Banking to P2P Lending" emphasize the regulatory challenges of P2P lending in China: the country with the largest proliferation of P2P lending platforms in the world. The authors argue that, due to the recently increased attention received by the shadow banking sector and the better transparency allowed by its technological readiness, the Chinese government now has a prime window of opportunity to regulate non-bank finance in China without impeding economic growth, nor risking a financial security meltdown. China would effectively transform its last-mover advantage in the field of financial reform into a first-mover advantage. Finally, the authors present their view of data-supported regulation, or "RegTech".

The book continues by offering a very exciting and inquisitive incursion into the new market dynamics brought about by the principles of decentralization and sharing enabled by (blockchain based) P2P platforms. Although, Courtois in the Chapter "Features or Bugs: The Seven Sins of Current Bitcoin" warns against a number of pitfalls in the current implementation of the first and largest blockchain application so far (i.e., Bitcoin), in the Chapter "Decentralized Banking: A Return to Technocracy In the Digital Age", Hayes makes the point that digital currencies could more securely and cheaply connect the world. The invention of the Blockchain is opening up the possibility of a different kind of monetary order run by inviolate mathematics, not a person or committee. Further, Gavin in the Chapter "Trustless computing—the what not the how" details how these FinTech innovations provide more functionality than nation state monies, at a lower cost, with safety and security achieved without armed guards and vaults and guaranteeing stability through attractive finite issue limits, again dictated by math rather than being subject to pressures to inflate to escape difficult political choices.

The Chapters authored by Porter and Rousse ("Reinventing Money and Lending for the Digital Age") on crypto currencies and Biggs ("The Opportunity for Non-Banks in Financial Inclusion and Remittance") on mobile money present a number of narratives about why those FinTech innovations may be empowering for people, especially in historically poor and financially underserved communities, as well as in less developed countries:

- as a means to facilitate low-cost remittances for those seeking to transfer small amounts of money internationally
- as a means for an otherwise excluded individual to have a decentralized global bank account, accessible simply by downloading an open source wallet from the internet, rather than having to set up with a formal financial institution
- subsequently providing the basis for a richer set of financial services, cooperative structures and even micro-insurance systems (Scott 2016).

The Blockchain ledger is not simply for accounting monetary transactions. At its core, it is a platform that allows people to come to agreement on virtually anything without intermediaries. It provides a foundation to make social contracts based on the principle of consensus. Its universality enables it to be an asset registry, inventory, tracking, and exchange infrastructure, a universal registry, listing, and management system for any of the world's assets, smart property, and itemizable quanta. It is an infrastructure which provides society's public records repository, a representative and participatory legal and governance system. Thus the Blockchain is poised to become a social technology for whole new institutional forms of economies sporting new market dynamics. Brought about by the principles of decentralization and sharing enabled by (blockchain based) P2P platforms, a deeper societal transformation is catalyzed, resulting in the basis of economic life being mutual cooperation and solidarity, rather than individual competition for narrow economic success. The idea is that in removing the need to trust central authorities (as Gavin clarifies in the Chapter on Trustless Computing), blockchains could be platforms upon which one can build new forms of non-hierarchal cooperation between strangers.

While formal market systems may be a source of economic growth and individual enhancement, they are simultaneously the source of social inequality, individual alienation and community disintegration. In essence, the cryptographic apolitical purity of a blockchain system appears not just as a way to stop abusive people who control central institutions, but as a way to once-and-for-all resolve the problem of how to establish contractual relationships between untrustworthy human beings who seek out their self-interest (Scott 2016). Aste, Caccioli and Livan ("Scalability and Egalitarianism in peer-to-peer networks") further prove using network theory that there is a trade-off egalitarianism vs efficiency for Blockchain based communities. Further, Barberis and Arner (From Shadow Banking to P2P Lending) and Chishti (How Peer to Peer Lending and Crowdfunding drive the FinTech Revolution in the UK) show how in deploying such decentralized platforms cryptocurrency is interesting because it has features that potentially allow for non-hierarchal self-organization and peer-to-peer collaboration within a communitarian network structure.

With advances in Blockchain technology now removed from the constraints of Bitcoin, it is possible to encode smart contracts as algorithms that will act as a trusted enforcer of agreements. Sclavonius et al. ("Are Transaction Costs Drivers of Financial Institutions? Contracts Made in Heaven, Hell, and The Cloud in Between") offer a review of how technological innovation is changing transaction costs and therefore the economic and financial system. They explain the socio-economic impacts of "smart contracts": modules of computer code that run on blockchains and can be programmed to transfer tokens of value, enable access to resources or otherwise automate functions based on conditions. This opens the perspective of increased access to critical financial services for all, creating more transparent democracies, and developing services that dramatically reduce barriers for global commerce. Panay ("Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money") deepens this understanding by illustrating how smart contracts can ensure financial stability. E.g. if the economy is growing too rapidly, the rate of money formation should be reduced over the next time period. In such instance, smart contracts working on behalf of a virtual organization could engage in purchases of foreign currencies in FOREX markets, as well as stabilize prices by purchasing bonds and equity in exchange for its stock of digital currency. Further, in order to quickly reduce the money supply outstanding, smart contracts could feasibly buy up existing digital currency and even destroy some of that currency by sending it to an unusable wallet address. This would have a similar effect to raising interest rates in that it would make money more scarce on the margin, that is, more expensive. Such intelligent virtual organizations running via smart contracts and acting as monetary authority can truly be removed from government, central authorities, or the influence from policymakers and corporate lobbying, thus opening the perspective of a more fair society with fair exchanges (Ulieru 2014).

Beyond the financial applications though, the Blockchain 2.0 movement is characterized by emergent attempts to build digital currencies with a focus on understanding the value created by online peer-production communities, and how such value can be used as a means to support and encourage the process of commons-based peer-production envisioned as a means of exchange for explicitly cooperative and collaborative enterprises that exist outside the logic of normal market processes.

Open question for those inspired by such Blockchain 2.0 platforms is whether blockchain systems can be a basis upon which people can easily interact with distant strangers for collaboration at scale. In this vision, the objective is to replace hierarchal centralized institutions with decentralized ones, but the point of doing this is (as we mentioned above) not to once-and-for-all perfect a means for naturally self-interested individual humans to contract with each other. Rather it is to allow naturally social beings to flourish and collaborate with each other in a spirit of cooperation, not individualistic competition. (Ulieru 2014). There are already creative initiatives to strengthen political accountability through the use of this technology. For example London mayoral candidate George Galloway is calling for the city to adopt Blockchain-based accounting in order to provide full transparency for the public of the city's financial activities. The Mayor's Chain Project aims to put the city's annual budget on a Blockchain to foster collective auditing by citizens.

The Blockchain thus, creates incentive for participants to work honestly where rules are applied to all equally. The Blockchain fosters a true consent of the governed through voluntary participation and enables self-regulation taken up by each choosing to abide by the rule of consensus. Foremost, the Blockchain enables a larger function of accounting; performing checks and balance on the self interests and the corruptible tendencies that exist in society. Unlike traditional representative models of governance, where systems of checks and balance are exercised through third parties, under bitcoin's consensus model, accountability is distributed directly and exercised by all in the network. With the blockchain's transparency, those who prefer profit without work will have no place to run and no place to hide. What emerges in this innovation is a new form of social accountability (Scott 2016). On this foundation we can envision a city network of informal street vendors running a collective mutual insurance pool between themselves using only their smartphones to interact with a distributed ledger system, with no central financial institution involved. Or a regional mutual credit system—effectively a ledger of credits and debits—implemented in a decentralized blockchain form (Scott 2016).

To this extent the blockchain becomes a technology for building new economies, as MacDonald, Allen, and Potts expose in the Chapter "Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking". As "the secure, verifiable, trustless (i.e. cryptographically secure) mechanism to record the actions upon the rules" the Blockchain becomes a social technology for whole new institutional forms of economies. More precisely the Blockchain enables the deployment of emergent temporary catallaxies, aka economies rooted in the very "adhocracies" featured in the title, and which we introduced in the beginning of this concluding Chapter. As "a foundation for social order, built on mathematical truth as verified, rather than political force as threatened", the Blockchain becomes "a source of welfare" acquired from releasing "the vast captured resources we have hitherto devoted to artificially manufacturing trust" into adhocracies that embody a "pure task economy where you find your people, you make your rules, and you do your thing".

Pioneering examples of such decentralized collaborative platforms enabling the deployment of adhocracies include: Backfeed (http://backfeed.cc/)—a Blockchain-enabled reputation based platform aiming to eliminate intermediaries from peer-to-peer exchanges; Sensorica (http://www.sensorica.co/)—a maker platform for collaborative design of specialized high end technical products, which runs an original "Value Accounting System" on a "Network Resource Planning" background to guarantee that participants are rewarded fairly according to their respective contributions (Turgeon et al. 2014); and Hylo (https://www.hylo.com/)—a co-creation platform catalysing communities around common intentions to bring the right skill set and resources to the right project timely.

Future studies are needed to reveal the respective legal frameworks in which these and other platforms operate (Dawson and Bynghall 2011), as well as the viability of alternative governance models—combining regulation by code, smart contracts and social norms—implemented by these platforms on top of the legal framework, either as a complement or a supplement to the former. Hypotheses such as those posed by Bollier et al. (Bollier et al. 2015) regarding the deployment of collaborative entities that issue blockchain-based shares—or crypto-equity tokens—that give the holders ownership or membership rights in a type of decentralized cooperative, need to be tested. How such organizations might end up looking in the real world remains to be seen, but they may be an interesting new form to explore in the quest to build social and solidarity-based finance (Scott 2016).

The ultimate quest concerns the emergence of adhocracies in a catallaxy and their societal transformative potential, with focus on how the Blockchain technologies enable implicit trusted exchanges in an open environment. In other words: How to enable large scale, free and systematic cooperation in a self-organizing manner that will produce constructive social and economic dynamics? (Ulieru 2014). How can social interactions be aligned with macro-level goals and how policies steering action towards goal achievement can emerge from such interactions? (Pitt et al. 2012). The answer we hope will contribute to the creation of more tools that facilitate the governance of online communities, and increase the innovative potential and productivity of commons-based peer-production platforms.

As an infrastructure which provides society's public records repository, a representative and participatory legal and governance system, Blockchain technology has the potential to benefit people with privacy, security and freedom of conveyance of data—which clearly ranks up there with life, liberty and the pursuit of happiness (Roszak 2016).

## References

Bollier, D., de Filippi, P., Dietz, J., Shadab, H., van Valkenberg, P., Xethalis, G.: Distributed collaborative organisations: distributed networks & regulatory frameworks. Coin Center Working Paper. http://bollier.org/sites/default/files/misc-fileupload/files/DistributedNetworksandtheLaw%20report,%20SwarmCoin%20Center-Berkman.pdf (2015). Accessed 17 Aug 2015

Brynjolfsson, E., McAfee, A.: The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton, New York (2014)

Chase, R.: Peers Inc: How People and Platforms are Inventing the Collaborative Economy and Reinventing Capitalism. Public Affairs, NY (2015)

Dawson, R., Bynghall, S.: Getting Results from Crowds: the Definitive Guide to Using Crowdsourcing to Grow Your Business. Advanced Human Technologies, San Francisco (2011)

Pitt, J., Schaumeier, J., Artikis, A.: Axiomatization of socio-economic principles for self-organizing institutions: concepts, experiments and challenges. Trans. Auton. Adapt. Sys. **7**(4), 1–39 (2012)

Roszak, M.: Blockchain testimony to the US Congress. http://docs.house.gov/meetings/IF/IF17/20160316/104677/HHRG-114-IF17-Wstate-RoszakM-20160316.pdf (2016). Accessed 16 Mar 2016

Scott, B.: How can Cryptocurrency and Blockchain technology play a role in building social and solidarity finance? UNRISD Report, Feb 2016. (http://www.unrisd.org/80256B3C005BCCF9/(httpAuxPages)/196AEF663B617144C1257F550057887C/$file/Brett%20Scott.pdf)

Turgeon, N., Thai, M., Epuran, G.: ODH start-ups' business development challenges: the case of sensorica from a total integrated marketing perspective. Int. J. Econ. Pract. Theor. **4**(2) (2014). Special issue on Marketing and Business Development, e-ISSN: 2247–7225

Ulieru, M., Doursat, R.: Emergent engineering: a radical paradigm shift. Int. J. Auton. Adapt. Commun. Syst. (IJAACS) **4**(1) (2011)

Ulieru, M.: Organic governance through the logic of holonic systems. In: Clippinger, J., Bollier, D. (eds.) From Bitcoin to Burning Man and Beyond, ID3 2014, pp. 113–129 (2014)

## Author Biography

**Mihaela Ulieru** works with many governments and organizations seeking to make ICT an integral component policy making for a healthier, safer, more sustainable and innovation-driven world. She founded two research labs leading several international large-scale projects, among which: Organic Governance, Adaptive Risk Management, Self-organizing Security, Living Technologies and Emulating the Mind. Coaching young people to value relationships and making powerful introductions to assist them, has contributed to their ongoing success. One example is Garrett Camp, founder of StumbleUpon and Uber, whom she guided for his MSc degree one decade ago. For her results which have positively impacted citizens in emerging and advanced economies including Asia Pac, North America and Europe she was awarded, among many others, the "Industrial Research Chair in Intelligent Systems" and the "Canada Research Chair in e-Society" and was appointed to numerous boards among which the Science Councils of Singapore, Canada and European Commission and to the Global Agenda Council of the World Economic Forum. She is a Research Professor at Carleton University, Global Leader with the Aspen Institute and Chief Innovation Officer of Affectio, the first Blockchain-enabled human data analytics platform fueling personal empowerment.

# List of Concepts

P. Tasca et al. (eds.), *Banking beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4

# List of Names/Authors Cited in the Book

P. Tasca et al. (eds.), *Banking beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4

# List of Names

P. Tasca et al. (eds.), *Banking beyond Banks and Money*,
New Economic Windows, DOI 10.1007/978-3-319-42448-4