Report from Dagstuhl Seminar 17132

Opportunities and Risks of Blockchain Technologies

Edited by

Roman Beck[1], Christian Becker[2], Juho Lindman[3], and Matti Rossi[4]

1 **IT University of Copenhagen, DK,** beck@itu.dk
2 **Universität Mannheim, DE,** christian.becker@uni-mannheim.de
3 **University of Gothenburg and Chalmers UT, SE,** juho.lindman@ait.gu.se
4 **Aalto University, FI,** matti.rossi@aalto.fi

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 17132 "Opportunities and Risks of Blockchain Technologies". Blockchain-based applications such as Bitcoin or Ethereum are emerging technologies, but a dramatic increase in industrial and academic interest in the technology is evident. Start-ups and large financial players are working intensely on blockchain-based applications, making this one of the most promising drivers of financial innovation. However, the design and implementation of blockchain-based systems requires deep technical know-how in various areas, as well as consideration of economic and societal issues. These opportunities and challenges provided the starting point for the Dagstuhl Seminar where we analyzed and synthesized the current body of knowledge on the emerging landscape of blockchain technologies. We linked cryptographic economic systems to already established research streams around trust-related issues in payment systems and digital currencies, and digital asset management.

Seminar March 26–29, 2017 – http://www.dagstuhl.de/17132
1998 ACM Subject Classification D.2.0 Software Engineering, K.6.5 Security and Protection
Keywords and phrases bitcoin, blockchain, cryptocurrencies, trust networks, trust platforms
Digital Object Identifier 10.4230/DagRep.7.3.99

1 Executive Summary

Juho Lindman
Roman Beck
Christian Becker
Matti Rossi

Introduction

The Dagstuhl seminar "Opportunities and Risks of Blockchain Technologies" had 21 participants from universities, public institutions, and enterprises. Blockchain is both an information technology as well as an economic innovation. As a technical innovation it is a new version of a distributed transactional database technology, especially suited for decentralized environments of limited or imperfect trust. As an economic innovation it offers novel tools to any problem domain where there exists a need for a reliable record of transactions in a decentralized environment where not all parties, whether humans or machines, can be fully trusted.

Opportunities and Risks of Blockchain Technologies, *Dagstuhl Reports*, Vol. 7, Issue 3, pp. 99–142
Editors: Roman Beck, Christian Becker, Juho Lindman, and Matti Rossi
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Computer scientists have researched key issues of blockchain technologies such as technical availability, tools, standards, and applications that enable these networks. Our seminar aimed to bridge the gap between this research stream and research perspectives from Service Science, Wirtschaftsinformatik, and Information Systems. We brought together a multi-disciplinary group of academic and industry researchers; specifically those working in fields such as open platforms, open source, distributed trust platforms, cryptocurrency tools, as well as the related social and legal challenges.

We set to analyze and synthesize the current body of knowledge on the emerging landscape of blockchain technologies. We linked the emerging phenomenon of cryptographic economic systems to already established research streams around trust-related issues in payment systems, online currencies, and supply chain management through group work and keynotes. We worked on four theme groups:

1. Research centers
2. Blockchain and Fintech
3. Essence and future of blockchain technologies
4. Impact/changing institutions

In the following we look at each of these shortly. The full report contains a number of position papers that explore these issues in further detail.

Research centers

The research center work group sought ways of strengthening the European and global research on blockchain. A starting point was a proposal to form a network of similar minded Blockchain experts and research groups across Europe. Several groups from countries such as in Denmark, Ireland, UK, and Switzerland could start as a loosely coupled interest group to work on potential research agendas and teaching curricula. The Blockchain seminar at Dagstuhl can be regarded as the starting point for the formation of the research network. Based on this network, the next step would be to convince funding agencies and industry to write research proposals for the DRAO (Distributed Research Autonomous Organization). The idea of DRAO is that the Blockchain research center should not be just another research center, doing research on Blockchain, but actually should be based on Blockchain, as a distributed autonomous research organization.

Furthermore, the group discussed a proposal for Blockchain teaching and education. This would result in a suite of courses on various areas, possibly as follows:

Computer Science Foundations

- Cryptography, authentication and signature methods.
- Distributed computing, distributed algorithms, understanding of the tradeoffs, consensus protocols
- Distributed systems
- Domain specific languages for contracts and for protocols.
- Large scale software engineering for distributed ledger development, software engineering
- Program analysis and software quality, objective way of verifying properties

Information Systems Economics

- Economic theories on incentive models, auctions and mechanism design (basically game theory insights)
- Inter-organizational, distributed governance and management theories

- Collective economies, reputation and trust management
- Digital Mindset and management of digital personas
- Ethics and critical reflections of Blockchain and societal implications

Information Systems Management and Organization

- Innovation Design: from Blockchain idea to prototype
- Digital Entrepreneurship: from Blockchain prototypes to markets
- Taxation, auditing and integration of Blockchain in organizations

IT Law

- Legal implications of Blockchain, property rights, ownership, responsibilities

Blockchain and Fintech

Our second worgroup dealt with the relationship between Blockchain and the Fintech industry. The group produced a matrix of different financial and legal functions, tools required to handle those and the potential of Blockchain to replace solutions to these functions.

Essence and Future of Blockchain Technologies

The workgroup on the essence of blockchain technologies set out to understand what forms the core of the technology. Its preliminary definition is that a blockchain implementation should contain First, the data storage that implements a distributed ledger system (DLS), the actual Blockchain, which is the data structure used in DLS is a hash-linked chain of blocks. A block is a collection of transactions that form the ledger. Furthermore, a Consensus Mechanism allowing for (de-)Centralization of power to decide which transactions are valid in the network. The innovative combination of the above mentioned three components give DLS interesting characteristics that we describe in the next section.

Impacts/changing institutions

This workgroup set out to understand the relationship between technical change and social change. It tried chart the relationship of blockchain and institutions. The discussion centered around the resilience of institutions and the need for stop gap measures, which are often provided by quite traditional public infrastructures and legal frameworks. In some cases, institutions will have to put conditions in place to allow blockchain to work (in particular to avoid harm). The idea of Blockchain being able to replace or eliminate trust was a central topic and it was noted that this can be an issue in cases of fraud (e.g. Ethereum fork as an example). The group also discussed who provides stable identifiers and who decides what can be stored in a given ledger. Similarly, the assignment of value and ownership and their control remain important issues that are now seen as tertiary to the technology. Key questions arising from this were:

- How will blockchain solutions that work well in theory or as prototypes function when used as large-scale solutions?
- Are certain groups or communities better suited to adopt blockchain?

Final comments

We believe that despite some hiccups (e.g., DAO fork) blockchain will emerge as an important technological and economical phenomenon. Its key properties and impacts should be studied intensively to allow for new innovations in the financial sector and other areas, where the technology's affordances promise to create value. The work continues through a manifesto in Business & Information Systems Engineering, a viewpoint in Communications of the ACM, and a special issue in the Journal of the Association for Information Systems.

2 Table of Contents

3 Overview of Talks

3.1 Smart Money: Blockchain-Based Customizable Payments System

Michel Avital (Copenhagen Business School, DK)

Joint work of Jonas Hedman; Lars Albinsson

Abstract. Legal tender in the form of coins and banknotes is expected to be replaced at one point in the future by digital legal tender. This transformation is an opportunity for central banks to rethink the idea of money and overhaul the prevailing payment systems. Digital legal tender is expected to reduce transaction costs by providing seamless real-time payments. In addition, digital legal tender that is based on blockchain technology can provide a foundation for customizable "smart money" which can be used to manage the appropriation of money and its use. In essence, the smart money is a customizable value exchange instrument that relies on computer protocols to facilitate, verify, and enforce certain conditions for its appropriation as payment, e.g. who may use the money, where, and for what. If we believe that digital legal tender will become ubiquitous, then the emergence and diffusion of smart money is inevitable and deserves further investigation.

Keywords: money, legal tender, digital money, customizable money, payment system, blockchain, distributed ledger technology.

The infrastructure of payment transactions is interrelated to the nature of money. Not long ago, ships were used to carry coffers of gold and silver coins which had intrinsic value. The growth and dynamics of worldwide commercial markets set the stage for the development of government-issued fiat money in the form of compact paper notes. The digitalization of bank accounts and the establishment of global communication networks, such as SWIFT, was instrumental in the development of today's electronic fund transfer (EFT) system and the virtualization of money. On the horizon, legal tender in the form of coins and banknotes is expected to vanish and be replaced by a digital legal tender that will be exchanged on distributed ledger technology (DTL) based platforms (Avital et al., 2016). Subsequently, the ubiquity of DLT platforms is expected to speed up money transactions as well as to provide the foundation for customizable "smart money" that can be used to manage the appropriation of money and its use as a medium of exchange.

In the last decade, we witness fundamental changes in the inter-bank exchange and payment infrastructure that are designed to tighten control and transparency. Many of these changes are fueled by regulatory pressure to mitigate particular security and compliance issues, such as money laundering, terrorism, corruption, and increase competition. For instance, the European Union (EU) are in the process of creating a single payment market in through the enforcement of the Single Euro Payments Area (SEPA) and the Payment Service Directive 2 (PSD2). The PSD2 forces banks and financial institutions to open up their payment infrastructure to provide third party payment providers with access to bank accounts and initiate payments [4].

Besides the regulatory changes, members in the banking sector experience increasing competition from non-bank players that offer similar and substitute services. Internet giants, such as Facebook, Alibaba, and Google, as well as device manufacturers, such as Apple and Samsung, have entered the financial market, together with at least 12000 Fintech startups [6]. These firms are dependent on the innovative utilization of existing and emerging technologies to challenge the incumbents of the financial sector [2, 7].

The regulatory changes, the technology development, and the competitive challenges are the new normal for any player in the financial sector. Therefore, it is not surprising that legacy organizations and especially banks make massive investments in the current payment infrastructure in an attempt to defend and bolster their respective market position [5]. The new emerging payment infrastructure is designed not only to address the regulatory and competitive issues; it also provides an opportunity to further develop money as a multifaceted medium of exchange that portrays more than merely monetary value. Subsequently, global transaction banking in the future would need to treat payment as a rich construct that goes beyond amount and effective transaction date.

Today, money is a general-purpose medium of exchange with unrestricted usage, i.e. money can be used by anyone to pay for virtually any product or service anywhere. In contrast, besides seamless real-time payments, the future DLT-based infrastructure offers opportunities to customize payments with sophisticated money that portrays a set of customizable conditions in addition to monetary value– i.e. smart money. In essence, the smart money is value exchange instrument that is based on computer protocols which facilitate, verify, or enforce preset conditions for its appropriation as payment, e.g. who may use the money, what products and services can be bought, and where.

Smart money can be used by society, organizations or individuals to manage the appropriation of money and its use as a customizable medium of exchange. Consider the following example:

Gill and Mark, two loving vegetarian parents, have decided to restrict Peter's (their 15-year-old son) use of his weekly allowance. Peter often used his lunch money to buy hamburgers and sodas, so his parents decided to control his use of his lunch money. The transfer of the weekly lunch allowance goes from Gill and Mark's bank account to Peter's mobile wallet, which also entails his identification cards and debit card. On the balance page, he can see how much money he has on his mobile wallet and his bank accounts. The amount of virtual cash is displayed in a pie chart diagram (green, red, and blue) with the amount on. The green pie is money to be used for school lunch. Red money is for clothes. The blue money is to be used for any purpose. The green and red money are the designed money from his parents to buy lunch at school and new pair of jeans and cannot be used for anything else. So, now Peter cannot buy hamburgers for lunch. Instead, he has to buy the regular vegetarian school lunch. Peter is, of course, outrageous and thinks that his freedom and privacy is hampered, but his parents who pay for the lunch are happy campers.

The idea of restricted-use money is not new – it is quite common as a proprietary currency. For instance, governments issue "food stamps" that can be used for food purchase only in designated locations, casinos issue proprietary "chips" that can be used for gambling, and airlines issue "frequent flyer miles" that can be used for flying tickets [3]. In contrast to such proprietary currency, the smart money is a customizable general purpose legal tender that can be restricted or conditioned as desired. Instead of functioning as a designated proprietary fixed-purpose token, smart money (just like a smart contract) affords a customizable multi-purpose digital medium of value exchange in everyday use by anyone.

The transition into smart money-based monetary system requires intermediary platforms that help financial institutors and users alike to experience the new technology and develop it further without abandoning the familiar and trustworthy legacy system. A transition period is necessary not only to allow banks and governments to experiment with different flavors and configurations as well as to develop a support infrastructure but also to allow developing public confidence in the new monetary system. While smart money can provide ample economic incentives to both governments and banks, it is not clear if smart money will

appeal to business organizations let alone the general public. Clearly, one way to develop public interest in adopting smart money would be to develop it as complementary currency [8] that is aligned with the worldview and value systems of intended users. For example, green money that supports or prefers environmentally friendly products and services, healthy money that supports health-oriented products and services, local money that supports local business, and so on.

We envision a multitude of cases where smart money can be of interest. In addition to numerous business opportunities, it will, of course, create a public debate concerning technical and organizational issues as well as social and ethical issues. Different stakeholders, such as banks, merchants, consumer agencies, politicians, health organizations, human rights and refugee organizations among others will take different positions from their respective perspectives. If we believe that digital tender will become ubiquitous in global transactions banking, then the emergence and diffusion of DLT-based smart money is inevitable and deserves further investigation.

References

1 Avital, M., Beck, R., King, J.L., Rossi, M. and Teigland, R. (2016). "Jumping on the blockchain bandwagon: Lessons of the past and outlook to the future." Proceedings of the 37th International Conference on Information Systems, Dublin, Ireland

2 Chae, J, and Hedman J. (2015). "Business models for NFC-based mobile payments." Journal of Business Models, 3(1), 29-48.

3 Chan, M., Kemp, S., and Finsterwalder, J. (2016). "The concept of near money in loyalty programmes." Journal of Retailing and Consumer Services, 31, 246-255.

4 Cortet, M., Rijks, T., and Nijland, S. (2016). "PSD2: The digital transformation accelerator for banks." Journal of Payments Strategy and Systems, 10(1), 13-27.

5 Hedman, J., and Henningsson, S. (2015). "The new normal: Market cooperation in the mobile payments ecosystem." Electronic Commerce Research and Applications, 14(5), 305-318.

6 McKinsey. (2014). Global Payments 2014: A Return to Sustainable Growth Brings New Challenges.

7 Scott, A., and Bolotin, L. (2016). Introducing the Open Banking Standard: Helping customers, banks and regulators take banking into a truly 21st-cnetury, connected digital economy (ODI-WP-2016-001).

8 Seyfang, G., and Longhurst, N. (2013). "Desperately seeking niches: Grassroots innovations and niche development in the community currency field." Global Environmental Change, 23(5), 881-891.

3.2 On Hostile Blockchain Takeovers

Joseph Bonneau (Stanford University, US)

Abstract. Most research modelling Bitcoin-style distributed consensus protocols (sometimes called "Nakamoto consensus") has focused on attempts to prove incentive compatibility. That is, models attempt to prove that under certain assumptions about attacker motivation a protocol will exhibit desired stability properties such as an exponentially low probability of long chain forks or a distribution of mining rewards that is close the amount of work contributed (called fairness or chain quality). Typically, models assume that the utility

function for all participants in the system is the amount of monetary rewards acquired within the protocol (e.g. for Bitcoin, the amount of mining rewards earned denominated in BTC). This leads to the most tractable models.

It is often acknowledged that a more realistic utility function is monetary rewards denominated in an external currency (such as US dollars). For this reason, some mining strategies which deviate from the standard protocol and lead to increased in-system rewards may yield less utility if they affect the exchange rate and therefore provide fewer ex-system rewards. However, modeling the impact of miner behavior on exchange rates is difficult, so this analysis is usually qualitative.

Rarely considered is a miner whose goal is not simply to acquire monetary rewards, but to destabilize a blockchain (even at a financial loss). Such a miner, who can fairly be called an attacker to the system, was called a Goldfinger attacker by Kroll and Felten (KF 2013). They can also be conceptualized as a hostile takeover, a term that is more appropriate for proof-of-stake systems.

I argue that revisiting the dynamics of a Goldfinger-style attack may yield new insights into the stability of blockchain protocols. In particular, it provides an interesting comparison between ASIC-dominated blockchains (such as Bitcoin), commodity hardware-dominated blockchains (such as Ethereum), and proof-of-stake systems.

Methods of obtaining mining capacity. For an attacker aiming to subvert a proof-of-work blockchain, they must obtain control of a large amount of mining capacity. We can consider whether the attacker is obtaining mining capacity permanently or temporarily, and whether they are introducing new capacity into the system or capturing existing mining capacity. This yields four basic attack strategies:

Temporary control. Obtain new capacity: **Rent.** Obtain existing capacity: **Bribe.**
Permanent control. Obtain new capacity: **Build.** Obtain existing capacity: **Buy out.**

Note that an immediately that a difference emerges between three types of systems:

- For ASIC-dominated blockchains, such as Bitcoin, the rent strategy is not possible because there is a negligible amount of Bitcoin mining hardware that is not already dedicated to Bitcoin mining.
- For pure proof-of-stake blockchains, neither rent nor build are possible, as the "capacity" in the system is fixed.

We can make some initial observations about each approach.

Rental attacks (on Ethereum). Rental is only possible for commodity-hardware mined blockchains. Ethereum fits this description today as mining is dominated by graphics cards (GPUs). An attack would consist of renting a large amount of capacity from a system such as Amazon's Elastic Compute Cloud (EC2). Currently, EC2 rents NVIDIA K80 GPUs for about USD0.20 per hour at spot prices (bulk discounts are available), which can perform about 24 MH/s, a little more than 1 millionth of the Ethereum network hash rate. So, as a very rough estimate for about USD400,000/hr an attacker could rent enough hardware to perform a 51 percent attack on Ethereum. Presumably only a few hours of such an attack would be sufficient to cause a major loss in value to the system, which has a market cap of over USD2.5 billion. Thus, it appears that Ethereum is relatively vulnerable to Goldfinger attacks.

It is worth noting that GPU rental is relatively inefficient. Currently Ethereum miners earn roughly USD40,000/hr in block rewards, whereas renting this capacity on EC2 would cost 10x those rewards. This premium means, however, that the attack has no long-term risk for the attacker.

Building attacks. Consider the cost of building enough new mining capacity to subvert Bitcoin. We can take as a representative example the AntMiner S7, a recent ASIC miner. It retails for about US$500 and can perform nearly 5 TH/s. Conveniently, this is about one millionth of the network hash rate-implying an upfront capital cost of about $500 million to obtain enough hash power to perform a 51 percent attack on Bitcoin. Of course, this figure is very approximate and it would be far cheaper to buy this hardware in bulk. Still, it appears to be roughly 3 orders of magnitude more expensive to perform such an attack on Bitcoin than to perform the rental attack described above on Ethereum. Bitcoin's market cap is a little less than an order of magnitude higher, but this still implies a capacity-building attack is 2 orders of magnitude more expensive (not to mention considerably slower and more complex logistically) to execute. This is an argument in favor of ASIC-friendly mining puzzles.

As for building attacks on Ethereum, the most efficient GPU hardware available currently costs about USD10/MH/s, suggesting a cost of about USD200 million to build towards 51 percent capacity. Note that this is several times more expensive (relative to the market cap) than for Bitcoin. Perhaps more capacity has been built for Ethereum as it is recyclable.

Bribery attacks. Mechanisms for bribery attacks were considered by Bonneau (Bonneau 2016). There are several approaches, including direct bribery, running a mining pool that pays excess rewards, smart contracts which deliver payment, or leaving bribes available on an attacker's fork. It is difficult to estimate the premium an attacker would need to pay to break miner loyalty and convince them to work on a fork that would be highly detrimental to the system. With negligible premiums, bribery is very cheap, requiring only half of the rate of network rewards (about USD40,000/hr for Ethereum or USD100,000/hr for Bitcoin). Presumably, similar economics apply to proof-of-stake systems.

Buy-out attacks. Buy-out attacks would involve either purchasing mining capacity from current owners or purchasing currency (in a proof-of-stake system). The cost of such an attack appears straightforward. For proof-of-work systems, it should cost about half of the net present value of all future mining rewards (with a steepened discount rate due to reflect likely future growth in network capacity). For proof-of-stake systems, half of the value of the system must be bought up.

It appears that proof-of-stake systems are much more secure here, as the attacker must buy half of all value of the system, whereas with proof-of-work the attacker must only buy half of the future mining rewards (which must be strictly less valuable than the entire market cap). In this case the term "hostile takeover" seems appropriate.

In either case, there is an interesting possibility of a race to the door among current capacity owners. Imagine that an attacker credibly announces they will buy out half of all capacity and then use it to destroy the system. Current capacity owners will have a strong incentive to sell to avoid being left in the 49% which does not sell and hence loses everything. As they being to sell and the attack appears more likely to succeed (which is easy for the attacker to signal as the amount of capacity grows) this could lead to a death spiral of lowered prices and increased confidence the attack will succeed.

Commodity proof-of-work systems appear less likely to suffer from a race-to-the-door, since capacity owners who do not sell to the attacker can still sell their hardware even if the attack succeeds.

Countermeasures. For all of the attack models, there is the possibility of countermeasures by current capacity owners. Current owners can respond in kind to building, renting, or bribing. With buy-outs, they can attempt to set a market floor by offering to buy more capacity themselves. This may be a profitable strategy-if a race-to-the-door is in progress

which has lowered the value of capacity, it may be profitable to buy if the attack fails and prices rebound.

Note that an attacker may respond to a buy-out attack by building (or renting) new hardware. This may be a wise strategy for a coalition of miners who would otherwise be stuck with a worthless 49 percent mining share after a successful attack. This countermeasure is not possible for proof-of-stake systems, in which a successful buy-out attack will be permanent.

Comparison. At first glance, proof-of-stake systems appear less vulnerable to Goldfinger attacks. They are not vulnerable to rental or building attacks. Bribery attacks appear similar, while buy-out attacks appear strictly more difficult. However, proof-of-stake is more fragile in that building new capacity is not available as a countermeasure.

Commodity proof-of-work systems appear more resilient to buy-out attacks as a race to the door is less likely to develop. However, ASIC proof-of-work systems are not vulnerable to rental attacks.

Open questions.

- Is the cost of Goldfinger attacks a useful lower bound on the security of a given system?
- Is there a strict ordering between the three main types of system considered here in terms of resilience to Goldfinger attacks? Or are they incomparable?
- Which attack strategy is the most plausible in practice?
- Is there a minimum amount of reward miners should receive (relative to the market cap of the coin) for security purposes, to ensure the disincentive to sell is high? Or will this simply cause more capacity to be built?

3.3 Can Blockchain Be Used to Secure and Enhance Groupware Communication in a Distributed Messaging Environment?

Peter Eklund (IT University of Copenhagen, DK)

Abstract. For many years I worked with security and law enforcement agencies with fundamental requirements for secure communications. While there are few guarantees that communications will never be intercepted and decrypted, secure communication is largely ameliorated by RSA encryption (to various strengths), legislative policy and, in the modern era, by the shear volume of communications occurring. Researchers even now talk about pre- and postquantum secure encryption, so even super-computational adversaries are envisaged in the defense of encrypted systems.

Spoofing attacks on the other hand, where one or more parties in the communication masquerades as a trusted information source, can never be entirely eliminated with encryption alone. Spoofing has increasingly become a tool for criminals and oppositional (supra-)national cyber-agencies. Spoofing attacks have even been used militarily, to stealth field resources, and to feint the existence of field resources where they do not exist.

There are two main types of spoofing, IP spoofing [5], where the TCP/IP packets are intercepted and the 'man in the middle' replaces the IP address of the legitimate message with his own. Usually, IP spoofing occurs at the DNS level, so the DNS resolves an otherwise legitimate URL to a fake one1. IP spoofing is also the basis for denial of service attacks [1], where a host site is overwhelmed with pings from IP address which appear legitimate,

but are not. Interestingly, one way to overcome this is to use a massively distributed PP distributed network – like a P-to-P Napster topology – to fragment the message content and make direct interception only viable so far as intercepting a small fragment of an encrypted message.

Address Resolution spoofing is another form of spoofing [5]. The ARP (Address Resolution Protocol) is used in resolving spoofed IP addresses with Media Access Control or MAC addresses for data transmission. ARP spoofing occurs when the attacker transmits spoofed ARP communications across a local area network in an effort to link the interceptors MAC address to the IP address of a legitimate network user. Any information intended for that user's IP address will, when the technique is used successfully, be transmitted to the attacker, instead of legitimate intended recipient [5]. ARP spoofing is usually employed to steal data, modify it in transit, or for otherwise scrambling communications traffic on a LAN. The technique also enables denial-of-service and man-in-the-middle attacks as well as session hijacking. My research question is therefore, **"can blockchain be used to eliminate or minimize the risk of spoofing attacks in a communication network, and if they can be used what is the performance hit from using it?"**.

Together with a student of mine at the IT University of Copenhagen – the student has himself, as part of a startup activity, developed a groupware communication tool (http://dallr.com) – we are looking to compare the performance hit on the users in the communication environment by comparing three different implementations of the tool. The first is the existing tool wrapped in a VPN, the second is a version that uses proof-of-stake [4] and Tendermint (https://tendermint.com) as the blockchain middleware, and the final variant is a version of the tool running on the Ethereum blockchain (https://www.ethereum.org), using proof-of-work as the consensus mechanism.

The objective of our work is **'to show, by way of engineering a proofof-concept and software simulation, how performant the blockchain varients are with the VPN version. Namely, by introducing irrefutability and decentralisation from a proof-of-stake blockchain, we can achieve non-assailable spoofing security, but can we can do so in a away acceptable to the systems users'**. In this case, acceptable to the system users means that the performance overhead introduced by the blockchain middle-ware results in latencies of less than 200ms for a system of 1000 users [6]. The key empirical work here is to achieve 200ms latencies but to measure, at what actual cost? How many database servers, content servers and web-services infrastructure is required to make this work to latency goal, and what are their specifications (cost) of the architecture needed to achieve this timing?

Importantly also, if proof-of-stake is the consensus mechanism, there is necessarily some trade-off against the distributivity of the consensus provers across the blockchain, and likely therefore a more centralized control authority results. A secondary research question is therefore under the proof-ofstake a trade-off, does the system still exhibit the characteristics of true distributed consensus protocol, or is it it is more closely identified as a centralized authority?

References

1 Denial-of-service attack-detection techniques. IEEE Internet Computing, 10(1):82–89, 2006.
2 Daniel J. Bernstein. Introduction to post-quantum cryptography, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.
3 Rita Boland. Military website spoofing is no laughing matter. SIGNAL Magazine, 2011.

4 Aggelos Kiayias, Ioannis Konstantinou, Alexander Russell, Bernardo Machado David, and Roman Oliynykov. A provably secure proof-of-stake blockchain protocol. IACR Cryptology ePrint Archive, 2016:889, 2016.
5 Andrew Lockhart. Network Security Hacks. O'Reilly and Associates, Inc., Sebastopol, CA, USA, 2004.
6 Fiona Fui-Hoon Nah. A study on tolerable waiting time: How long are web users willing to wait? In AMCIS, page 285. Association for Information Systems, 2003.
7 F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer. Comprehensive approach to intrusion detection alert correlation. IEEE Transactions on Dependable and Secure Computing, 1(3):146–169, July 2004.

3.4 Evolving the Social in the Socio-Technical System of Blockchain

John Leslie King (University of Michigan - Ann Arbor, US)

Abstract. Blockchain technology seems promising in its own right, and might be "disruptive." We have a poor track record predicting what new technologies mean over the long run, and an even poorer record knowing in advance what is truly disruptive. However, there is considerable experience with social evolution. Blockchain is already is a socio-technical system. Even if Blockchain technology enables changes in the social, prediction of technology is flawed. The evolution of some aspects of the socio-technical system is easier to predict. Often the social is more important than the technology in the evolution of the socio-technical system.

Blockchain technology has already had *some* important effects, as seen with the cybercurrendy Bitcoin. This illustrates that many social dimensions are unresolved. Central banks have deliberated on whether to permit use of the cybercurrency, with some prohibiting and some permitting. This paper covers four issues regarding the social evolution of the Socio-Technical System of Blockchain.

The Social Importance of Financial Systems. Financial systems – Blockchain's first large application area – has high social importance. Maintaining the stability of such systems is as important as the state's maintaining a monopoly on the use of force. Financial systems are vital to social welfare. Few national or regional banking authorities permit financial services without adherence to strict regulatory structures. An example is counterfeit, outlawed since ancient times and subject to harsh penalties. Suppression of counterfeit became more important by the advent of fiat money that has no intrinsic value (e.g., precious metal content). Laws prohibit fraud, manipulation, insider trading, and other behaviors considered damaging to financial systems. Financial authorities maintain "full faith and credit" as essential to a stable economy and society. Authorities and those they represent take this seriously. The legal framework for financial systems evolved with new technologies, usually with delay. The bigger the potential social change brought by technology, the longer the delay.

Understanding Trust. New technologies often bring new ways of looking at basic social issues such as trust. Trust is an ancient issue, recognized as important for millennia, but not well understood. Trust is tied to identity and verification, but we do not really understand how. We will learn more as Blockchain grows. There is an historical analog. Human capacity for natural language was deepened by efforts at natural language processing (NLP) by

computers. “Machine translation” (MT), or translating one natural language faithfully into another using computers, was in the early days of computers thought to be “just around the corner.” In the 1950s there was optimism that MT would be accomplished in one or two decades. Yet more than 60 years has passed and MT still has not delivered. MT is better than it once was, but it is not faithful. Human capability in natural language was shown by NLP to be far more sophisticated than the NLP experts imagined. Technology and techniques were no match for reality. MT might one day achieve its potential, but the ease with which humans do “natural” things masks how amazing those things are. We often do not realize this until we start trying to demonstrate that technology and technique can do such things. Technology and technique thereby become part of research efforts to understand these deeply “human” skills. Replacing them with automated aids might remain as an endeavor, but learning shifts to research.

The Socio-Technical Imperative. Technologies that affect human welfare through systemic effects reach far beyond “the technology.” A well-established example is combustion of fossil fuels in Carnot engines that exploit the heat gradient. Carnot engines enabled a significant part of the industrial revolution, primarily through external combustion, especially steam engines or transport as in ships and trains as well as manufacturing. Later there were internal combustion engines (e.g., gasoline and diesel engines and turbines) used in transport and to produce electricity. Much of the 19th and 20th centuries were devoted to finding sources of fossil fuels and operating the social systems to supply them and to defend those supply lines. Modern organization was constructed to provide the products and services made possible by Carnot engines. In the 21st Century much concern shifted to managing the by-products of combustion, especially as carbon has moved from the lithosphere to the atmosphere and made the “greenhouse” effect important in climate change. Similarly, long-term health and environmental effects have emerged around materials used in modern systems (e.g. chlorinated hydrocarbons, asbestos, dioxins, heavy metals like mercury and lead, and radioactive isotopes of elements such as strontium and plutonium). Technology became increasingly important to social welfare, and socio-technical systems evolved to provide subsidy (e.g. limits on possible liabilities from nuclear power generation mishaps), regulation (e.g., restriction of atmospheric and water pollution) and control (mandatory safety and risk mitigation actions). Many technologies now evolve socio-technical systems before they appear in the marketplace.

Management of Risk. Risk has become a determining factor, and effective risk management is required of any technical innovation. However, the context of risk has not remained fixed over time. At one time concern was limited largely to the capital at risk. Investors wanted to know what would happen under different possibilities: project failure, capital loss, inadequate investment return. Capital risk remains, but liabilities now include benefits and liabilities from the consequences of the original action that might materialize later, (e.g. intellectual property rights, health problems in offspring of those originally exposed to particular materials). Systemic future effects are taken into account to understand and manage the implications of new technology. Debates occur between those who want to buffer the downside on every foreseeable risk vs. those who wish to desire uninhibited innovation and argue that problems can be remedied after they occur. In the most extreme and cartoon-like of these debates, the former are characterized as Luddites who stand in the way of progress, while the latter are characterized as ignorant of problems that have arisen from new technologies that that created effects that could not be remedied (e.g., premature death) or that cost a great deal to remedy later.

Taken together these four issues will shape the evolution of Blockchain from a technological innovation into socio-technical systems. It is too late to keep Blockchain technology out of the socio-technical systems realm because the first major application of the technology has been to financial systems, Such systems are inevitably socio-technical. Financial authorities are vigilant, ready to take action on anything new, in part because the realm of finance has certainly inherently conservative aspects that deflect or slow down innovation, and in part because history shows instances in which the unscrupulous have exploited new technologies to take money from others by fraud. Blockchain will *never* escape the gravity well of socio-technical systems because it was first applied in an area that is inherently part of socio-technical systems. It's path has become set.

The evolution of the Blockchain socio-technical system will revolve at least in part around trust. Many – perhaps most or all – potential applications of Blockchain technology are to arenas where trust is important. Applications in finance entail the concept of "full faith and credit" and are inherently an institutional and social. Applications in health records, trade documentation, and so on are also institutional. Blockchain technologies cannot do away with trust issues because trust is embedded in social life and has been for a very long time. It might be part of what makes humans human (e.g., part of the genetic code), even if often manifested in social structures. However, Blockchain technology could, at least in principle, shift trust from institutional authorities to technology around scarcity, security and contracting. Blockchain uses blocks that are scarce (usually computationally so) and can therefore carry economic value. If the blocks and the links that connect them in a chain can be made secure, the system can be relied on. Blockchain retains a transparent and reliable record of transactions enabling binding contracts. This, in principle, enables distributed trust, but this trust is in the system rather than in the technology, per se. The scarcity issue might be covered adequately, but security (and therefore contracting) are less certain. The Bitcoin world has been "hacked" more than once, and people are confronted daily with evidence of unauthorized access to "cyber" systems, making Cybercurrency (or anything else cyber) suspect. As long as there is public uncertainty about security, most people will trust Blockchain only if a trusted institution serves as "residual claimant" on trouble. This extends beyond security to any threat to the technology, including limitations on scale, scope, or speed of operation. Some of these threats to Blockchain technology will materialize with use, and not before. We will not know they are issues until we encounter them.

The socio-technical imperative is reinforced by incumbents. Incumbents support continuity in existing systems, and will not embrace disruptions that will diminish their influence. The proponents of Blockchain are not incumbents with power, but are seen as "fringe" players. If Blockchain gains influence this will change over time. But it is not easy to change existing systems due to legal and regulatory apparatus that cannot be changed without time-consuming processes (e.g., allowing for public comment). Incumbents can also find ways to appropriate aspects of important new technologies, ensuring that they remain powerful in any new socio-technical regime. The popular discourse is replete with stories of how disruptive technologies have empowered the new and decimated the old, but a careful look at socio-technical system evolution suggests that incumbents are not easily replaced, while the new are easily recruited to become incumbents. That is, the "upstarts" become "incumbents" pretty quickly. Meet the new boss; same as the old boss.

Finally, risks seldom fall and remain disproportionately on those who cannot bear them. The larger institutional order that manages risk at the societal level will most likely manage risk in Blockchain applications. This is because social institutions protect other social institutions to permit risk to remain managed as in the past. For example, when the U.S.

insurance industry refused to insure nuclear power plants against all possible liabilities in the case of mishaps, the U.S. Congress stepped in with legislation that capped liability for nuclear power plant mishaps at levels far below what most experts recognized as potential liabilities. Thus, commercial insurance companies insured nuclear power plants. It is questionable whether online purchasing would have taken off as it has were credit card companies (and by extension, payment systems like PayPal built on the credit card system) bore the risks of fraudulent use of consumer accounts. Most consumers could use payment systems based on credit cards with essentially no risk. (This benefit has been generally extended to consumers for all such uses of these payment systems.) The risks inherent in Blockchain – and all important technologies carry risks – will be borne by institutions (e.g., the U.S. Federal Deposit Insurance Corporation in finance), or by new institutional agencies that cannot "walk away" from responsibility.

3.5 Open Source Software Research and Blockchain

Juho Lindman (University of Gothenburg / Chalmers UT, SE)

Abstract. This short paper investigates ways in which earlier open source software (OSS) research can help us explain blockchain-related phenomena. We review OSS literature and identify three such areas: 1) blockchain and OSS 2.0, 2) community development, and 3) forks.

Introduction. Earlier work on cryptocurrencies has used the openness of the software source code to decrease the risks of a system being perceived as a security black box and thus increase development trust. Both early examples of blockchain technology – Bitcoin and Ethereum – were open source projects. However, it should be noted that OSS is also contested in this context: There is an ongoing discussion regarding the importance of the source code openness and the underlying technological infrastructure. In this paper, we do not try to solve this issue but instead provide some insights OSS research may offer as blockchain moves forward.

Blockchain and OSS 2.0. We investigate Bitcoin and Ethereum as examples of blockchain technology. Bitcoin (protocol and crypto-currency) was introduced in 2008 and implemented as an open source project [6]. Later, the Bitcoin Foundation was founded to support development efforts [10] that rely on the global OSS developer community. Ethereum was introduced in 2013. The main driver was the disagreements concerning what kinds of scripting to include in Bitcoin to enable smart contracts. Ethereum quickly attracted a large following.

Discussion regarding open and openness gained a boost in 1999 when a group of OSS proponents, including Eric Raymond (1999) and Bruce Perens (1999), decided to increase OSS credibility. Their literature led to a fertile but contested research terrain tightly coupled with the increased industrial engagement of OSS by commercial companies [15]. The result was a steady increases in the industrial use of OSS [3] and OSS-like practices for software production (Linden et al., 2009). Over time, the tools and practices related to OSS changed (for example, from Sourceforge to GitHub(s) and intranet-based implementations of OSS). Ultimately, even the most critical voices found themselves engaged with OSS (for example, Microsoft joined the Linux Foundation on Nov 16, 2016).

Thus, OSS 2.0 relies on commercial involvement [3], but enthusiasm around Bitcoin / Ethereum from companies, entrepreneurs, and industries grew quickly compared to similar earlier developments in other OSS projects. One of the reasons is quite obvious: Blockchain proponents understood early that the developer community would need help from the cryptocurrency users, vendors, and intermediaries or the network to grow and to realize benefits.

Another interesting similarity between OSS and Blockchain is the strong political polarization of these innovations, not unlike what happened with the first free software vs. commercial software and then free software vs. OSS in the 90s [15]. Many early enthusiasts for OSS and Blockchain were motivated by the "bazaar-style" radical decentralization of the technology (often motivated by liberal political philosophy). In OSS, the divergent interest of incumbent companies and volunteer communities was identified – and at least partly solved – using different kinds of OSS 2.0 approaches.

Community-driven development. Research in open platforms [11, 4] and in "openness" [1] provide useful starting points to discuss Blockchain. Openplatforms literature discusses third party participation in design, and the key elements to this are boundary resources.

Open source research has discussed OSS governance of the development communities, meaning OSS project direction, control, and coordination [8]. The governance consists of three literature streams: 1) different incentives for independent developers to participate in open efforts (for example, [5], 2) efforts to provide support for the coordination activities (for example, [2]), and 3) encourage building a welcoming culture [8].

Forks. Forks have been a topic of research for some time in OSS [7]. There is variation in how the term is used, but usually fork means a situation where the developer community disagrees on the development roadmap (or a different focal issue), and this results in a situation where several different competing and backward-incompatible versions of the code base are in use.

In most open source projects, forks are both a safeguard of openness and detrimental to the development efforts because they dilute contributions and developers during the different versions (Fogel 2006: 88, Moody 2009). Viseur (2012) found the majority of forks studied were motivated by a need for technical specialization, and forks rarely were followed by the extinction of the original. Robles and González-Barahona (2012) claimed, based on an in-depth analysis of 220 forks, that they take place in all software domains, can be friendly or competitive, and have become more frequent in recent years. For example, Ethereum has undergone already four so-called hard forks (backwardincompatible), so this research is becoming pivotal again.

Summary. OSS research offers several insights that may be usable in Blockchain context regarding how to solve different kinds of tension between voluntary communities and commercial companies. The artefact's openness is obviously an interesting point of departure, but more critical questions may be related to guaranteeing the incentives of the different actors and matching divergent interests. The re-emergence of forks also raises questions where OSS may provide some analytical tools for discussion.

References

1 Aksulu, A. and M. Wade (2010). "A comprehensive review and synthesis of open source research." Journal of the Association for Information Systems 11(11): 576.

2 Crowston, K., et al. (2005). "Coordination of free/libre and open source software development."
3 Fitzgerald, B. (2006). The Transformation of Open Source Software. MIS Quarterly, 30, 3, 587-598.
4 Ghazawneh, A. and O. Henfridsson (2013). "Balancing platform control and external contribution in third-party development: the boundary resources model." Information Systems Journal 23(2): 173-192.
5 Lerner, J. and Tirole, J. (2002). Some Simple Economics of Open Source. Journal of Industrial Economics, 50, 2, 197-234, June.
6 Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
7 Nyman, L. (2015). Understanding Code Forking in Open Source Software: An examination of code forking, its effect on open source software, and how it is viewed and practiced by developers. Helsinki, Finland, Hanken School of Economics.
8 Markus, M. L. (2007). "The governance of free/open source software projects: monolithic, multidimensional, or configurational?" Journal of Management and Governance 11(2): 151-163.
9 erens, B. (1999). The Open Source Definition. In: Dibona, C. and Ockman, S. (eds.). Open Sources: Voices from the Open Source Revolution. O'Reilly Media, Sebastopol, CA.
10 Teigland, R., et al. (2013). "Breaking out of the bank in Europe-exploring collective emergent institutional entrepreneurship through bitcoin."
11 Tiwana, A., et al. (2010). "Research commentary-Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics." Information systems research 21(4): 675-687.
12 aymond, E. (1999). The Cathedral and The Bazaar – Musings On Linux And Open Source By An Accidental Revolutionary. O'Reilly Associates, Sebastopol, CA.
13 obles, G. and González-Barahona, J. (2012) A Comprehensive Study of Software Forks: Dates, Reasons, and Outcomes. Proceedings of the 8th IFIP WG 2.13 International Conference, OSS 2012, Hammamet, Tunisia.
14 Viseur, R. (2012) Forks impacts and motivations in free and open source projects. International Journal of Advanced Computer Science and Applications, Vol. 3, No. 2.
15 Weber, S. (2004). The Success of Open Source. Harvard University Press, Harvard, MA.

3.6 Blockchain-Enhanced Trust in International Trade

Gerhard Schwabe (Universität Zürich, CH)

Abstract. Many industries struggle to improve the processes, which involve large volumes of exchanged documents between different untrusted organizations. While transporting goods, monetary payments are needed. To enable these payments and ensure that the goods are transported, financial institutions play an intermediary role in relationships between buyers and sellers. Managing payment processes for trade includes the process of document exchange (e.g. invoices, insurance certificates, shipment documentation, etc.) between different organizations, while sold goods are on their way from the seller to the buyer. These processes become more cumbersome and their complexity increases if transactions cross national borders. International trade for goods and services accounted for more than USD24 trillion USD in 2014 (World Trade Organization 2015). By its very nature, trade can feature several interactions between previously unknown, untrusted third parties. In addition to the

potential trust issue between buyer and seller, several intermediate entities might be involved in the process. Every additional intermediary increases the risk of process delays or fraud, and also causes higher processing costs for collection, verification and coordination of the required documentation. Fraud risks are exasperated by lacking coherent overarching legal rules and law enforcement mechanisms.

Introduction. Many industries struggle to improve the processes, which involve large volumes of exchanged documents between different untrusted organizations. While transporting goods, monetary payments are needed. To enable these payments and ensure that the goods are transported, financial institutions play an intermediary role in relationships between buyers and sellers. Managing payment processes for trade includes the process of document exchange (e.g. invoices, insurance certificates, shipment documentation, etc.) between different organizations, while sold goods are on their way from the seller to the buyer. These processes become more cumbersome and their complexity increases if transactions cross national borders. International trade for goods and services accounted for more than 24 trillion USD in 2014 (World Trade Organization 2015). By its very nature, trade can feature several interactions between previously unknown, untrusted third parties. In addition to the potential trust issue between buyer and seller, several intermediate entities might be involved in the process. Every additional intermediary increases the risk of process delays or fraud, and also causes higher processing costs for collection, verification and coordination of the required documentation. Fraud risks are exasperated by lacking coherent overarching legal rules and law enforcement mechanisms. As a best practice today, payment transactions between untrusted sellers and buyers are often facilitated through a letter of credit (LoC). A LoC is "an agreement that the bank of the buyer, called the issuing bank, will arrange a credit to guarantee payment as soon as the supplier can prove that the goods have been shipped" (Hulstijn and van der Torre 2005). Such inefficiencies as delays, paper-heaviness, lack of trust between the intermediary organizations, as well as risks of fraud hamper the overall process of trade. In order to let organizations, which are exposed to lack of trust, work together effectively, interorganizational trust has to be established. However, the more stakeholders are involved into the process, the less inter-organizational trust exists: they have not enough knowledge to trust each other, they are based in different countries with different legal systems, the working partners change often, etc.

The process is very costly, bears the risk delaying the shipment, and relies on trust established by a third party, such as banks. Blockchain technology is often seen as a disruptive way to transform processes that rely on a trusted third party into a much leaner, decentralized and automated form. In our research, we follow the goal to explore the potential of blockchain technology and smart contracts for international trade at the example of a LoC. Thus, we look how blockchain technology can be used to enhance trust in international trade.

We follow a Design Science Research (DSR) methodology (Hevner et al. 2004; Gregor and Hevner 2013; Nunamaker et al. 2015). Our key contribution is an explanatory design theory (Baskerville and Pries-Heje 2010) for enhancing trust in international trade at the example of a Letter of Credit. We built a prototype for a blockchain based LoC (called BLOC) and validated it in several rounds in dialogue with representatives from a leading logistics company and four Swiss banks. By doing so, we contribute to scientific discourse on blockchain technology and its applications and explore how a blockchain-based system may replace the trust in the monetary processes in the domain of trade finance. Furthermore, we bring value and useful knowledge to practitioners who face the problem of working with large numbers of documents, which should be created, accessed or amended by different parties, and also be tamperproof.

Related work. International trade has been always considered as an important driver of global prosperity. Since in international trade, business partners often lack reciprocal trust, currently an effort must be made to establish the exact financial terms between an importer and an exporter (Antras and Foley 2011). This relationship between importers and exporters can be handled without any mediation (Antras and Foley 2011). However, if the stakes are high, the process is often intermediated by banks on both sides, and the process can also involve more actors (e.g., an insurance, a carrier), which influence the whole process of contract execution. If there was trust between all involved stakeholders, such transaction costs could be avoided, since they would render these activities unnecessary. Trust is a crucial component for successful transactions regardless of whether they are executed in a physical or virtual space (e.g., online marketplaces) (Son et al. 2006).

Due to the nature of international trade, we regard the lack of inter-organizational trust to be unavoidable. However, we argue that to a large extent, inter-organizational trust could be replaced with mutual trust in an IT artefact. While there may be genuine trust in the blockchain technology itself, on an application level, trust in IT artefacts rarely appears in isolation. It rather must be viewed in conjunction with the trustworthiness of other actors in a 'trust network', most importantly the provider of the technology (Söllner et al. 2016). There can be a trust transfer in both directions: the application of a trustworthy artefact may enhance the trustworthiness of the provider and vice versa.

In our study, we propose a design solution, which is based on the blockchain technology and in particular the concept of smart contracts. By the year 2016, the blockchain technology has received significant attention both by researchers and practitioners, and is often considered to bear the potential for a technological revolution not only in the field of FinTech, but in any other domain that might benefit from a secure and trustworthy history of events or data records. From a technical perspective, the technology of blockchain represents a distributed ledger, which allows the users of the network to agree following the concept of consensus and, therefore, build trustless agreement which exclude possible intermediaries from the process. Due to these properties, the Ethereum blockchain appears to be a promising technological basis for creating an IT artefact in which multiple stakeholders can trust as a substitute for lacking inter-organizational trust.

Exploring the proposed solution. In our work, we developed a system that replaces inter-organizational trust by trust in a blockchainbased IT artefact, and thus facilitates trade administration between parties that otherwise have no means to trust each other. To solve this, our architecture and BLOC incorporate multiple features that support the establishment of trust in IT according to prior work (Söllner et al. 2012). In fact, the blockchain technology itself delivers multiple such characteristics off the shelf. One of those properties is transparency, since all data on the blockchain are public by default, which makes it possible for anyone to read all data stored on the blockchain. In addition, it can be argued that public blockchain implementations have a benevolent operator, since they are run entirely decentralized, i.e. due to the absence of a controlling operator, there is no possibility of a non-benevolent operator. Even though the prototypical solution was kept very simple by design, and did not map the business logic that exhibits anything remotely close to the complexity of real-world processes in the investigated domain, the experts confirmed that all business requirements for solving the investigated problem were met. They were also confident that a solution such as the one proposed could be developed or integrated into a more generic, scalable business process support platform, which could be used even in a real-world context.

First, from the technological point of view the blockchain technology itself shows potential for several use cases in the domain of international trade, as it can eliminate fraud issues, and overcome issues the result from a lack of trust when dealing with unknown counterparties.

Moreover, the nature of smart contacts, as self-executable programs, could bring value to the business and significantly automate the overall process and, therefore, reduce transaction and administrative costs. Two interview partners even admitted for LoC to be a relatively unattractive product for their respective banks, which they might readily stop to offer if they could safely do so without losing customers for more profitable areas of business. Bearing this in mind, their openness towards automation of the LoC process with a blockchain-enabled solution is not surprising.

Second, the immutability of the information saved in the blockchain is beneficial in a way that the origin of the documents, and any amendments in the document flow could be tracked. This increases the transparency of the process, and thus creates trust in the information system. Therefore, blockchain can be used to compensate for the missing trust in the inter-organizational relationship. However, the blockchain technology is relatively new, and development of applications on its basis still have experimental character, therefore, it is not sufficiently clear where its boundaries are and in which use cases blockchain can unfold its full potential. Critics might point out that transaction costs and throughput with blockchain might not yet be ready for enterprise-grade applications. Other researchers have gathered first evidence regarding the transaction costs and throughput on the Ethereum blockchain, discussing the trade-offs regarding costs, trustworthiness and latency of the public Ethereum blockchain as compared to private instances (Weber et al. 2016). We are therefore confident that the current performance limitations of blockchain will be solved in the future. Our work seeks to solve the problems inherent to storing and exchanging documents required for complex processes across multiple organizational boundaries, and often spanning multiple languages and legal frameworks. In addition to offering a solution to the practical problem, this research also illustrates a use case for distributed ledger technologies outside the realm of financial transactions (as seen in the Bitcoin blockchain), particularly with Ethereum's blockchain implementation and its smart contract feature.

In environments where stakeholders have no means to trust each other, as regularly encountered in the domain of international trade, designing IT artefacts that replace inter-organizational trust with trust in the IT artefact itself, is crucial for the involved parties to benefit from the same transaction cost reduction.

We argue that the blockchain technology includes features necessary for creating trust in an information system and, therefore, addresses and has potential to resolve at least several of above discussed challenges, namely many unknown stakeholders, fraud and a missing common framework, lack of transparency, and different IT capabilities. Considering the relatively young, and not entirely uncontroversial history of Ethereum and blockchain, it can be argued whether or not the technology itself is trustworthy for a specific purpose. Therefore, it is essential to consider carefully, in which cases the use of blockchain makes sense, and where another technology with different properties might be advantageous.

We conclude that the LoC process still faces important challenges, which we set out to solve using a DSR approach. In particular, current LoC processes still display inefficiencies like being paper-heavy processes, including manual processing of transactions, and risks which hamper the trade finance sector. We propose a blockchain-based design theory to eliminate the problems related to the lack of trust in inter-organizational processes in the domain of international trade. Moreover, we conclude that such an architecture would be beneficial for any domain that involves a large number of the documents in a supply chain or workflow, with many stakeholders that are geographically distributed, and particularly when fraud is a potential issue.

Limitations and future work. We did not make observations of how the process is going on in detail from perspectives of different parties (banks, carriers, insurance companies, etc.). This task does not seem trivial because of the nature of the process, as it refers to cross-border shipments and relationships between organizations which are located in different countries.

We believe that the insights from this study can bring a valuable contribution as it highlights the problems in the trade finance industry which are similar to processes from other areas (for example, in logistics, energy sector, medical sector, etc.). In doing so, we bring a better understanding of the issues in inter-organizational relationships, and discuss opportunities and challenges for the application of the blockchain technology in this scenario. We see a high potential in developing studies also in other domains and testing whether the formulated design theory holds up there, too.

Furthermore, the external validity of the study should be improved, this should be addressed in the future research activities. Therefore, we would also like to inspire the researchers to make their impact into the research on blockchain considering a large variety of aspects, from underlying cryptology and its limitations to ecosystems.

References

1 Antras P, Foley CF (2011) Poultry in motion: a study of international trade finance practices. National Bureau of Economic Research
2 Baskerville R, Pries-Heje J (2010) Explanatory design theory. Business and Information Systems Engineering 2:271–282.
3 Gregor S, Hevner AR (2013) Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly 37:337–355. doi: 10.2753/MIS0742-1222240302
4 Hevner AR, March ST, Park J, Ram S (2004) Design Science in Information Systems Research. MIS Quarterly 28:75–105. doi: 10.2307/25148625
5 Hulstijn J, van der Torre L (2005) Analyzing Control Trust in Normative Multiagent Systems. BLED 2005 Proceedings 6.
6 Nunamaker JF, Briggs RO, Derrick DC, Schwabe G (2015) The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research. Journal of Management Information Systems 32:10–47. doi: 10.1080/07421222.2015.1094961
7 Söllner M, Hoffmann A, Hoffmann H, Wacker A, Leimeister JM (2012) Understanding the formation of trust in IT artifacts. Association for Information Systems,
8 Söllner M, Hoffmann A, Leimeister JM (2016) Why different trust relationships matter for information systems users. European Journal of Information Systems 25:274–287.
9 Son J-Y, Tu L, Benbasat I (2006) A descriptive content analysis of trust-building measures in B2B electronic marketplaces. Communications of the Association for Information Systems 18:6.
10 Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J (2016) Untrusted business process monitoring and execution using blockchain. In: International Conference on Business Process Management. Springer, pp 329–347
11 World Trade Organization (2015) International Trade Statistics 2015.

3.7 Autonomous pension funds on the blockchain

Peter Sestoft (IT University of Copenhagen, DK)

Abstract. We propose that life-based pension funds, such as those that pay a whole life annuity, can be fully autonomous and operate without a central trusted pension fund. In particular, payments and benefits, asset management, and estimation of liabilities (reserves, discounted future cash flows) can in principle be implemented using self-executing contracts, for instance on a blockchain infrastructure such as Ethereum.

Core activities of a pension fund. We consider life-based insurance-style pension funds, such as those that pay a whole life insurance: a guaranteed income stream to the insured person from retirement age until his or her death.

A pension fund comprises the following activities: (a) Enter contracts with pension customers; (b) receive a stream of payments from active, eg. working, pension customers; (c) pay a stream of benefits to retired and disabled pension customers; (d) regularly send forecasts to pension customers of their expected future benefits based on the contracts and the payments made; (e) invest and manage the assets that result from payments minus benefits; (f) regularly report to regulators to demonstrate that assets are suf- ficient to cover liabilities, namely, the obligations to pension customers; (g) pay taxes on the payments and benefits streams; (h) in general, react to life events, notably disability, retirement and death, of the pension customers.

Autonomous pension funds. We propose that all of these activities may be implemented using selfexecuting contracts on a distributed ledger such as Ethereum, and discuss some of the concerns raised by and requirements for implementing this idea. We might call an organization, or distributed algorithm, along these lines an autonomous pension fund (APF). We argue that it is technically feasible to create such an entity as an autonomous organization:

- Activities (b), (c) and (g) are mainly processing of contract-regulated payments and seem clearly implementable using self-executing contracts and a cryptocurrency.
- Activities (d) and (f) can be based on the highly developed actuarial mathematics in the Scandinavian/German tradition, typically formalized with stochastic state models and Thiele's differential equations. This approach can be implemented and operationalized in software in a very general form, as evidenced by eg. Edlund's Actulus Portfolio Calculator.
- Activity (e) could be run in the manner of TheDAO on Ethereum (though preferably without the mistakes and vulnerabilities). How to invest the assets can be decided by voting, with automatically imposed limits on composition (expected return, risk, maturity, . . .) of the investments, to match them to the liabilities as forecast using actuarial mathematics.
- Activity (h) depends on insurance-related life status and events being reportable in a trustworthy and automated way, so that self-executing contracts can act on them. This is very nearly the case in much of northern Europe. Life status includes gender, age, marital status, citizenship and tax status; and life events include retirement, becoming unemployed, becoming disabled, retiring, recovering from these events, and death.
- The life-based pension contracts mentioned in (a) can be formalized in a domain-specific language, that is then used in (b), (c), (d), (f), (g) and (h), and in constraining the investment decisions in (e) so that the asset composition matches the expected obligations. Namely, given such formal pension contracts, one can compute expected future cashflows,

discounted expected obligations (reserve) and risk of default (as per EU Solvency 2 requirements); and one can generate pension forecasts, distribute monthly payments (into the fund) on pension products, compute monthly benefits, and more. A prototype of such a domain-specific language has developed, though not for blockchain use, in a collaboration between the company Edlund A/S, Copenhagen University, and the IT University of Copenhagen.

- Life-based insurance and pension operate on more "objective" states (active, disabled, retired, dead) of the insured than most property insurance, where more human work is needed to assess the degree of damage, counter insurance fraud, and so on. Hence life-based insurance and pension are amenable to a larger degree of automation than is property insurance.

Challenges and advantages. Some crucial questions and concerns about the practical feasibility of an autonomous pension fund include:

- Pension promises are extremely long-term obligations. A 25-year old woman entering the labor market in 2017 may retire in 2062 and may expect to rely on her pension income until 2087 or even longer. What reasons does she have to trust that the autonomous pension fund keeps it promises, or even exists, over such a long time span? Clearly, regulation plays a role here, but so does trust in the technology
- Pension funds are heavily regulated, nationally (in highly countryspecific ways) and internationally (eg. EU Solvency 2). This is both to reassure pension customers the pension funds are able to fulfil their promises, and to ensure that the pension products they sell agree with tax regulation.
- What pension products are preferred by customers is considerably in- fluenced by what tax deductions they offer, and by what pension products are mandated eg. in general labor market agreements ("overenskomster"). Thus products offered by the autonomous pension should be certified by tax authorities to allow for expected deductions and to satisfy the general requirements.
- An autonomous pension fund would avoid many of the costs of commercial pension funds, such as those owned by banks whose shareholders expect a return on their investments. Even the many Danish pension funds that are customer-owned (such as most labor market funds, PFA, ...) and in general very efficient, have non-negligible costs. Danish pension funds manage approximately 500 billion Euro, corresponding to 1.6 times annual GDP, and with such large amounts of money under management, even small inefficiencies translate into large absolute costs.

References

1 The DAO of accrue. A new, automated investment fund has attracted stacks of digital money. The Economist. May 21st 2016.
2 Christiansen, Grue, Niss, Sestoft, Sigtryggsson: An Actuarial Programming Language for Life Insurance and Pensions. International Congress for Actuaries 2014, Washington DC.
3 Edlund Actulus Portfolio Calculator, https://edlund.dk/loesninger/actulus
4 DIRECTIVE 2009/138/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).
5 Emin Gun Sirer: Thoughts on The DAO Hack, blog post 17 June 2016, http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/

3.8 De-hyping DLT and Pragmatic Use of DLT in Banking

Udo Milkau

Abstract. Some authors of well selling books such as Don and Alex Tapscott assign tremendous potentials to blockchain, the technology underlying Bitcoin. Blockchain - or technically: Decentralized Ledger Technology (DLT) - is recognised as a "truly open", distributed and "democratic", and "immutable" platform that fundamentally changes what we can do online, how we do it, and who can participate. According to their views, the new technology facilitates peer-to-peer transactions without any intermediary such as bank or governing body. Accordingly they titled their latest book (2016) "Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World". However, a practitioner in a bank has to ask three questions:

1. What problem is the technology solving and what is the economic benefit?
2. What changes in business models can be catalysed and/or triggered by DLT?
3. And the third question is what social benefit can be provided by DLT?

This Provocation Paper will briefly discuss those three questions and try to "de-hype" the technology behind blockchain from the point of view of tangible real-world implementations.

Evolution and Taxonomy of Blockchain and Distributed Ledger Technology. The original idea of Satoshi Nakamoto's concept paper (pseudonym, 2008) was to develop Bitcoin as "A Peer-to-Peer Electronic Cash System" with the blockchain as the combination of existing technologies as underlying platform to solve this one and only problem. This issue is related to two well-known problems in distributed computing:

- The Byzantine Generals Problem, describing issues in establishing a secure synchronisation of participants, who exchange messages e.g. payment transactions, in a distributed network of unknown nodes, which cannot be trusted ex-ante.
- The Double Spending Problem, meaning the possibility to spend electronic cash (as a sequence of zero's and one's) twice by broadcasting multiple malicious transactions into a distributed network without any central entity that keeps track of the state of the network by providing a central "clock" to validate the correct sequence of transactions (original vs. copy).

A list of examples for the re-used technological building blocks is given in Table 1. Nevertheless, a key for the solution for "Electronic Cash" was the change of paradigm as Bitcoin applies a game theoretical approach with the selection of one neutral referee to achieve distributed consensus. This "blockchain" – in the original design for Bitcoin – comes with a number of assumptions and limitations: It is a closed-loop, repeated game played by peers without any hierarchy, but also without any generic link to the physical world (such as e.g. represented by central bank money).

It is a probabilistic system with only eventual consistency (see e.g. Decker und Wattenhofer, 2013). In principle, eventual consistency is not new to banking and accounting (!), but has to be understood. It is based on a number of technological parameters, which - by design - make the Bitcoin blockchain inefficient and very costly, slow and with limited capacity, and fully readable or transparent (as contradiction to "anonymous" physical cash).

The original design of the Bitcoin blockchain is an alternative model for payments, which has to be compared and to compete with (i) traditional payment transactions between interoperable banks based on fiat / central bank money and (ii) centralised platforms such

as e.g. PayPal, American Express or Western Union, which perform and book payments internally, and have interfaces to the outside world and the two sides of the market (typically merchants and consumers).

The development of the original Bitcoin blockchain is shown in Figure 1. Without going into the details, the actual Bitcoin ecosystem departed significantly from design and assumptions. Today, the Bitcoin "processing" is centralised in four - and interconnected - "mining pools" representing 80 percent of the hashing power as a proxy for the contribution to the system; and the formal and/or informal governance is concentrated at a handful of "core developers". Additionally, Bitcoin users do not want to run a payment system at all – they want to pay and – for certain reasons – use a means of payments comparable to PayPal, AliPay, VISA, MasterCard, iDEAL, paydirekt et cetera. Last but not least, attempts to give Bitcoins some "official" painting were unsuccessful1 due to insufficient asset protection.

It can be discussed, whether Bitcoin is in a dead-end road. Nevertheless, a number of derivatives of the original blockchain approach have been developed. Figure 1 is an attempt to compile the taxonomy of the current development, but has to be limited on major trends of the development. First, one finds a rather nice oxymoron with the proposals for "central bank digital currencies" based on blockchain. However without a link to settle transaction in central bank money - e.g. securities transactions or trade finance businesses – a blockchain would be limited to closed-loop systems. Second, a number of developments have been proposed to improve some of the deficits of Bitcoins. One example is the implementation of "off-chain channels" for transactions (such as duplex micropayment channels), and the other one is additional anonymity by "zero knowledge" (which in turn has assumptions and limitations by itself).

Third, extensions have been made to include "smart contracts", i.e. tuning complete scripts to represent a state machine, to the blockchain. In an open "public" blockchain approach, the replication of the distributed database including those "stored procedures" results in a global state machine running on all nodes with all readable scripts and all transactions in parallel. Although many enthusiast seem to be fascinated by such public programmable blockchains like Ethereum (and many others), Ethereum is an example for more forks of the development with (i) an announced change from "proof-of-work" to a new consensus model called "Casper" and (ii) the foundation of a "private" Ethereum Enterprise Alliance end of Feb. 2017.

Fourth, a number of commercial initiatives focussed on permissioned consensus protocols (without distributed ledgers), e.g. Ripple with the "Interledger Protocoll" or the R3 consortium with Corda™, which is "inspired by the blockchain".

Fifth, SWIFT as traditional payment network between interoperable banks is testing DLT based on the open source "Hyperledger" in the framework of its Global Payment Initiative (GPI). As all those trends (and many more) are derivatives of the original set of building blocks of the blockchain, the practical question for use of DLT in banking will be:

How can some building blocks (technology and game theory; as e.g. illustrated in Table 1) be combined to solve actual business problems and do those solutions provide advantages compared with more "traditional" elements by an economic evaluation of costs, quality-of-service, speed, or security and cyber resilience?

From "Code is Technology" to "Code is Law – Layers of Business Processes. The original concept of Bitcoin blockchain can be described as a distributed "golden record" for the rights to transfer a token (representing "electronic cash" in a closed-loop peer-to-peer system). Concerning the extension of "smart contracts", one can e.g. find the following definition on the webside of www.ethereum.org:

"Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk." (accessed: 11.3.2017)

Applying a reality check on this statement, one can find some critical constrains:

- applications Yes, i.e. computer code, scripts, stored procedures et cetera!
- run exactly as programmed4 But who will corrects code errors in the future during the life cycle of a "smart contract"?
- without any possibility [=] third party interference But with possible interference of "peers" as demonstrated during the so called "The DAO" hack!
- represent the ownership of property [and] move funds But any ownership (and legal transfer) depends on the applicable legal framework such as e.g. securities law legislation and the access to funds as legal tender!
- without counterparty risk No, as any contract with a promise of repayment in the future (loan, mortgage, bond, promissory note et cetera) will have a counterparty risk in general (and "escrow" would be a contradictio in adiecto to any credit arrangement)!

That constrains reveal that technology is only one layer in a contractual relationship (although the terminology "smart contracts" entails a misunderstanding about the capabilities of a piece of computer code). Figure 2 provides a schematically structure of the different layers from "technology" to "law"5 and "risk". In between "governance" and "standards" are needed to handle to dynamic aspect of any non-trivial computer code (with errors to be corrected and changes to be made during the life cycle of the code) and to provide lingua franca for all participants in a network industry.

With the right understanding about possibilities and constrains of a new computer technology, DLT can be the trigger or catalyst for industry-wide or even cross-industry discussions and development of "distributed" business processes and "networked" business models. One historical example for an innovation, which triggered the development of law over centuries in different countries, is securities law legislation. Starting with the "technology" of tradable shares as "securities" based on paper documents, new legal concepts of the representation of ownership ("shareholding") developed. This process is still ongoing, as the European harmonisation of the Securities Law Legislation is one of the Giovannini barriers to be worked on.

The "inspiration by blockchain" and discussion about business models in the 21st century may be the largest efficiency gain, the blockchain will bring to financial services in the future.

The Blockchain as a Sociology Experiment. The question "Cui bono" from the discussion about DLT, could be answered very lightly: For the time being writers, consultants, and careerists in financial services have a measurable benefit. Nevertheless, DLT concerns some basic questions of the "digital" society in the 21st century. Maybe, it is merely a temporal correlation by chance, but the concept paper by the pseudonym "Satoshi Nakamoto" was written in 2008 at the peak of the global financial crisis (triggered by the preceding sub-prime mortgage crisis). The idea of (electronic) cash without any intermediaries including banks and central banks is far from being new. Friedrich August von Hayek demanded in his book "Denationalisation of Money" (1976) an end to the monopoly of governments on (central

bank) money and proposed a competition, as entrepreneurs should be permitted to innovate in the monetary sector, such as by creating "neutral" currencies or minting commodity money?

The second question is related to the first one, a competition of currencies could once more lead to monopolies – especially if we remember the development of the Bitcoin systems from a peer-to-peer network to an onion-like hierarchy. Joi Ito pointed out: "[T]here is currently centralisation in the form of mining pools and core development, [but] the protocol is fundamentally designed to need decentralisation to function at all." (Ito, 2015) Therefore, research is needed to understand the dynamic development of networks in competition, and especially of social networks. The third issue is the question of the "costs of trust". Niklas Luhmann wrote his seminal book "Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität" in 1968. Regarding "trust is a mechanism to reduce social complexity", trust provides a reduction in transaction costs and has an economic benefit. The substitution of trust of "permissionless" blockchains like Bitcoin comes with associated costs leading to the question of a desirable social optimum in a balance between trust and technology.

A last questions concerns the motivation of those promoters of "smart contracts" claiming that "Code is Law" would be an improvement to the current contract law (in the different versions of diverse legal legacies). From the author's point of view, this "mechanistic conception" of the world is an expression of the wish to avoid the uncertainty and complexity of the 21st century and to turn back the wheel to a reductionist concept as e.g. expressed by Frederick Winslow Taylor in his book "Priciples of Scientific Management" of 1911 based on his experiences of the business practices of the 19th century. All the more, it is very strange that a keynote speaker at a payment conference explained – obviously without any sarcasm – [quote David G.W. Birch, 9.3.2017)

"The blockchain is the solution to our problems [in financial industry]" "In fact, it's the solution to most industries' problems" "The blockchain is a religion"

Conclusion. For a rational discussion about measurable benefits, it seems to be necessary to "de-hype" DLT. The technology itself can provide advantages – such as e.g. demonstrated in a transatlantic payment transaction in eight seconds between ATB Financial, Calgary and ReiseBank, Frankfurt in 2016. However, DLT has to be compared with other existing technologies in cost-benefit analysis.

Beyond technology, the discussion about DLT can be a catalyst for new business processes, business models, or even further development of legislation. Bringing partners from different industries and government together to develop more efficient and holistic cross-industry solutions would be highly appreciated – even though the final technology would be merely "inspired by blockchain".

Finally, DLT is linked to a number of issues, which are important for social benefit in the 21st century.

Further research about the motivation behind "blockchain" could a helpful to analyze expectations, wishes, and fears about the "digital society" of the future.

References

1 Tapscott D., and Tapscott A. (2016) "Blockchain Revolution: how the technology behind bitcoin is changing money, business, and the world", Penguin, 2016.
2 "Satoshi Nakamoto" (pseudonym, 2008) "Bitcoin: A Peer-to-Peer Electronic Cash System", available at: http://bitcoin.org/bitcoin.pdf
3 Akkoyunlu, E.A., Ekanadham, K. and Huber, R.V. (1975) "Some Constraints and Trade-offs in the Design of Network Communications", SOSP '75 Proceedings of the fifth ACM

symposium on Operating systems principles, Austin, Texas, Nov. 19-21, ACM New York, NY, pp 67-74.

4 Lamport, L., Shostak, R. and Pease, M. (1982) 'The Byzantine Generals Problem', ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp. 382–401.

5 Fischer, M. J., Lynch, N. A. and Paterson, M. S. (1985) 'Impossibility of Distributed Consensus with One Faulty Process', Journal of the Association for Computing Machinery, Vol. 32, No. 2, pp. 374–382.

6 Blum, M. Feldman, P., and Micali, S. (1988). 'Non-Interactive Zero-Knowledge and Its Applications', Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC 1988), pp. 103–112

7 Haber, S. and Stornetta, W.S. (1991) "How to time-stamp a digital document", Journal of Cryptology, Vol. 3/2, pp 99–111.

8 Dwork, D. und Naor, M. (1992) "Pricing via Processing or Combatting Junk Mail" in: Ernest F. Brickell "Advances in Cryptology – CRYPTO' 92", Lecture Notes in Computer Science, Vol. 740, 1993

9 Parnas, D.L. (1994) "Software aging", ICSE '94 Proceedings of the 16th international conference on Software engineering, Sorrento, Italy, May 16-21, 1994, IEEE Computer Society Press Los Alamitos, CA, pp 279-287.

10 Brewer, E., 2000, "Towards robust distributed systems," 19th annual ACM Symposium, Principles of Distributed Computing (PODC 00), ACM, pp 7-10.

11 National Institute of Standards and Technology (2001) "Secure Hash Algorithm 2"

12 Osipkov, I., E. Y. Vasserman, N. Hopper, and Y. Kim, 2007, "Combating double-spending using cooperative P2P systems," paper presented at ICDCS, 2007, 27th International Conference on Distributed Computing Systems (ICDCS '07), pp 41.

13 Hoepmann, J. H., 2008, "Distributed double spending prevention," 15th International Work-shop on Security Protocols, Lecture Notes in Computer Science 5964, pp 2010.

14 Bott, J. and Milkau, U. (2017), 'Central bank money on blockchain – A payments perspective', Journal of Payments Strategy and Systems Volume 11, Spring 2017.

15 Milkau, U., Neumann, F. and Bott, J. (2016) "Development of distributed ledger technology and a first operational risk assessment", Capco Journal of Financial Transformation, Vol. 44., pp 20- 30.

16 Decker, Ch. und Wattenhofer, R. (2013) "Information Propagation in the Bitcoin Network", 13th IEEE Int. Conference on P2P-Computing, September 2013.

17 Lessig, L. (2000) "Code Is Law", Harvard Magazine, 1.1.2000; http://harvardmagazine.com/2000/01/code-is-law-html; accessed 11.3.2017

18 Ito, J. "Why Bitcoin Is and Isn't Like the Internet", 23.1.2015; joi.ito.com/weblog/2015/01/23/whybitcoin-is-.html (accessed: 11.3.2017)

19 Luhmann, N. (1968) "Vertrauen: ein Mechanismus der Reduktion sozialer Komplexität".

20 Birch, D.G.W. (2017) "Blockchain and Reality or what's in the blocks?", Keynote, European Payment Summit 2017, Den Hague, 8.3.2017

3.9 Bitcoin – a social movement maintained currency under attack

Marella Venkata (Aalto University, FI), Juho Lindman (University of Gothenburg/Chalmers UT, SE), Matti Rossi (Aalto University, FI), and Virpi Tuunainen (Aalto University, FI)

Abstract. Bitcoin is an open source cryptocurrency system used for the money transfers and payments without involving a financial institution. Bitcoin revolutionized the financial industry and the fiat currencies. However, bitcoin was never studied from a social movement perceptive in the literature. Typically, social movements occur when people are dissatisfied with the existing system and are looking for a change that would solve their problems. The first version of Bitcoin was released after the collapse of the Lehman Brothers, people lost their trust in the financial institutions due to the lack of transparency in their operations. A system with higher transparency was seen as a superior solution for currency and payment related questions. Bitcoin turned out to be such a system. There is no centralized authority that governs the bitcoin. All the stakeholders involved with the bitcoin are pseudonymous. Security and trust comes from the underlying technology called blockchain.

Blockchain is a decentralized and distributed database where all the transactions are recorded in a ledger. Blockchain stores the information across a network of personal computers usually called as nodes. When a transaction occurs, all the nodes in the system are notified and process it. Every node in the network can access the information and process the transactions. No single node in the system can manipulate the data because all the other nodes have access to correct information. Hence, blockchain is extremely secure.

Bitcoin is considered as a cryptocurrency because everyone accepted it as a currency. But, in reality, bitcoin is just a ledger of all the transactions that are stored across several nodes. Bitcoins are traded with the fiat currencies at bitcoin exchanges. A bitcoin exchange is a place where you can buy or sell your bitcoins using fiat currencies. Since the inception of the bitcoin, these bitcoin exchanges have become targets for the hackers. Many of these exchanges lost millions of dollars of bitcoins. They are few exchanges that declared bankruptcy after these cyber-attacks. If the bitcoins are stolen from any bitcoin exchange, the whole bitcoin economy loses the money and the value of the bitcoin diminishes. Hence, the value of bitcoin is a very volatile.

Bitcoin as a Social Movement. From a framing theory perspective of social movement, collective action frames are classified as diagnostic framing, prognostic framing, and motivational framing. Diagnostic Framing is related to problem framing and identification. Prognostic Framing involves clearly stating the solution to the described problem or a clear plan or a strategy on how to execute the plan. Motivational Framing calls for action to make things better by using vocabulary to motivate people. Bitcoin can be projected as a motivational framing as it provides a solution to the existing problem by improving the transparency and eliminating the third parties. (Robert D. Benford, 2000).

Data collection. Data is collected from several news articles and blog postings. It includes blogs such as bitcointalk, reddit, coindesk, the register etc. All the important postings are collected from the blogs for analysis and patterns are recognized from them. From these patterns, we identified the various kinds of the cyber-attacks and classified them into four groups. We further investigated the data and observed the responses that exchanges have taken to solve the problem.

Classification of Cyber-Attacks. Basing on the nature of the attack, we classified these attacks into four different categories as Code Bugs, User Errors, DDoS Attack and 51 per cent Hash Rate Attack. We also studied the responses of the exchanges for these attacks. These responses include Code Revision, implementing computer security measures, temporary suspension and complete shutdown of the exchanges.

Security Flaws in the code written for the wallet. (Code Bugs): The majority of the attacks that occurred on the bitcoin are due to the code written for the access and the security of the wallet by the bitcoin exchanges. Third-party software companies usually write this code for the exchanges. Examples of these companies are BitGo, Slock.it, Linode, Flexcoin, and Instawallet. For instance, Bitfinex teamed up with BitGo and created a multi-signature wallet whose keys are divided among a number of owners to mitigate the risk of giving them to one user. But, BitGo server was hacked and the exchange lost USD 66 million. Flexicon programmers were unable to implement the concurrency property on the distributed system. Bitcoinica alleged a hack at the web hosting provider Lionde.

User's Mistakes (User Errors): The second major cause for the attacks on the Bitcoin is due to the user's mistakes to implement the security measure on the wallet computer. Most of the users failed to follow the basic safety guidelines on the computers containing wallet. Bitfloor lost a quarter million dollars when the attacker accessed the unencrypted wallet backup key. Inputs.io email account got compromised, due to which the hosting account got compromised. Unauthorized Users who had accessed the computer with wallets. Allinvain's computer was attacked by some virus like Trojan horse, which could assess the encrypted wallet file.

Distributed Denial of Service Attacks . (DDoS Attack): DDoS Attack is happening very frequency on the bitcoin exchanges. Though DDoS Attack cannot steal the bitcoins from the wallet, it can disrupt the services of the exchange and lower the value of the bitcoin. Some attackers do it before purchasing the bitcoins, while the rest blackmail the owners of the companies to pay a significant amount of money to stop the attack.

51 percent Hash Rate Attack: 51 percent hash rate is an issue with the blockchain. If any mining pool can acquire 51 percent of hash rate, they get control on all the transactions of the blockchain and start double spending the transactions. Ghash mining pool came close to 50 percent hash rate in two instances. There is no mechanism on Bitcoin blockchain that can prevent this from happening at this point.

Classification of Responses for the Cyber-Attacks.

Shutdown: When exchanges lose a significant number of bitcoins during the attacks, they shut down their operations completely. Usually, the flaws in the code (or) failure to implement the computer security measure are the key reasons for the shutdown of the exchanges. Some exchanges try to repay their customers after the shutdown.

Temporary Suspension: In order to control the loss from the attacks, exchanges temporarily suspend their services and resume once the problem is solved. Temporary suspension of services will reduce the impact of the cyber-attacks. DDoS attacks disrupt the normal operations of the exchange and force them to suspend their services.

Code Revision: If the cyber-attack occurs due to the flaws in the newly added code, the exchanges will revert/revise the existing code to a safe state. Exchanges may lose the new features added by the code, but, will be able to contain the cyber-attack.

Computer Security Measure: When the cyber-attack happens due to any security flaws on the wallet machine, the users (or the exchanges) counter them by implementing computer security measures. Few of these security measures include encrypting the wallet keys, installing the antivirus and preventing the unauthorized access to the computer.

Classification of Stakeholders. Bitcoin is an open source project. Unlike, most open source projects where developers are the only key stakeholders, Bitcoin project involves multiple key stakeholders. We divided the people interacting with the Bitcoin into nine different types of stakeholders as Developers, Hackers, Investors, Exchanges, Vendors, Users, Supporters, Enthusiasts and Legal entities. Depending on the way each stakeholder interacts with the bitcoin, we categorized these nine different stakeholders into three categories as Functional, Economic and External groups. Developers and hackers are categorized as a functional group, while Investors, Users, Exchanges and Vendors come under Economic group. Supporters, Enthusiasts and Legal entities are considered as an external group. Bitcoin is an open source P2P transfer protocol, where developers have access to the source code. All the developers share their ideas and code enhancements through an online forum named "Bitcointalk.org". Investors are those people, who put their money in the bitcoin and wait for a while excepting the value of the bitcoin to raise. These people treat bitcoin like stocks. Users view bitcoin as frictionless currency transfer system from one person to another person. They use bitcoin primarily for money transfer purposes and commercial purposes. Enthusiasts are ones who are interested in the bitcoin, who follow the news and keep track of how things are emerging on the bitcoin platform. Researchers are part of this group. Supporters like the idea of eliminating the centralized authority. They are interested in the concept that a system can work without the inference of third parties. Libertarians are an example for this category. Hackers try to steal the bitcoins from the economy. Their main objective is to make money for themselves and diminish the reliability of the bitcoin. Exchanges are places where people can buy and sell the bitcoins. Vendors are the stores or outlets that accept bitcoins for micropayments. Bitcoin is a contentious issue for legal regulators, tax authorities, and legal agencies due to the anonymous nature of the system and lack of centralized control over the system. The legality of trading bitcoins depends on the geographic location.

Impact of Cyber Attacks on Stakeholders: Whenever a cyber-attack happens, the economic layer of the bitcoin stakeholders loses the money. Among these four stakeholders, exchanges are always the primary targets of the hackers because of the high amount of stakes involved with them. Investors are the secondary targets as they buy a lot of bitcoins and wait until the value raises. Users and vendors loss is insignificant as they have relatively low investment on bitcoin. Hence, we will examine the exchanges and investors reaction to cyber-attacks.

Over the past few years, the hackers targeted several bitcoin exchanges. The biggest attack among them was the Mt.Gox attack, where the exchange lost about 350 million dollars. Mt. Gox was the largest bitcoin exchange, roughly handling 70 percent of the bitcoin transactions. The company just posted a note on their website to the clients saying, "decision was taken to close all transactions for the time being" (Hajdarbegovic, 2014). When the losses are huge, the exchanges don't provide any information to the clients and shuts down their services. The second major attack on the bitcoin exchange was the bitfinex after which, the value of the bitcoin plummeted by 20 percent. Bitfinex remains offline, with its message announcing the hack still visible to users. Unlike Mt.Gox, Bitfinex acted responsibly. They answered the questions to customers through the social media. Yet, some of the investors lost trust in the bitcoin exchange (Higgins, August).

Biomat is the third biggest bitcoin exchange located in Poland. They lost 17000 bitcoins when their wallet, which was saved on Amazon Web Services (AWS) was erased due to a change in settings. It is one of the rarest case where the exchange openly acknowledged that they have implemented a wrong technical solution by using the Amazon Web Services. BitQuick server was compromised for a short duration. The exchange immediately issued a statement saying that they temporarily shut down the server and are investigating the cyber-attack. Similarly, Bitcash, a Czech Republic exchange openly acknowledged that their server has been hacked, compromised 4000 wallets of its clients. But, the company also used strong words to describe the situation by saying, "Unfortunately, the nightmare became a reality." (Bradbury, 2013). It would incur loss of trust and confidence among the investors when the exchange uses such strong negative statements. BIPS, a Danish Bitcoin Exchange lost 1295 bitcoins from the wallets for their clients, which worth USD1 Million. The founder of the BIPS made an announcement saying, "Web Wallets are like a regular wallet that you carry cash in and not meant to keep large amounts in". But, this statement was criticized by the clients saying, "our data is secure at BIPS". So yeah, I felt pretty goddamn secure leaving my BTC balance there." (Khandelwal, 2013). Another website named Inputs.io was hacked, the owner, who goes by a pseudo name 'Tradefortess' reported the issue two weeks after the attack. He made an apology to the clients saying, "I know this doesn't mean much, but I'm sorry, and saying that I'm very sad that this happened is an understatement." (Boase, 2013) Investors trust towards the bitcoin depends on two key factors. Firstly, the investor's personality traits like his attitude, interests, beliefs and experiences with bitcoin. Motivational framing projects bitcoin as a transparent system without a centralized authority. Investors, who are motivated with this concept, would still put their money despite the cyber-attacks. Secondly, it depends on his hugely financial situation of the investor. For instance, investors in the good financial situation and with interest in concept and the idea of the bitcoin might continue to invest in the bitcoin despite losing the money due to the cyber-attacks.

Conclusion. When the cyber-attacks incur huge losses, exchanges do tend to make a very vague statement, hiding the details of the attack. In some cases, they make very discouraging statements to their clients. By using such sort of a rhetoric, exchanges lose their reputation and trust among their clients. Rather, the exchanges should disclose complete details of the cyber-attacks and inform the response that they implemented to recovery from the attack. Exchanges should ensure the clients that such kind of attacks would not reoccur. Cyber-attacks cannot only incurs financial losses but also can create trust deficit among the investors about bitcoin. The intangible loss that occurs due to the trust deficits is of greater magnitude than that of the actual financial loss. Exchanges need to realize that investors can motivated to invest on bitcoin despite the cyber-attack and ensure them that required steps would be taken to prevent similar cyber-attacks in the future.

References

1 Boase, R. (2013, November 7). coindesk. Retrieved from coindesk: http://www.coindesk.com/hackerssteal-bitcoins-inputs-io-wallet-service/

2 Bradbury, D. (2013 , November 12). coindesk. Retrieved from coindesk: http://www.coindesk.com/czech-bitcoin-exchange-bitcash-cz-hacked-4000-user-walletsemptied/

3 Hajdarbegovic, N. (2014, February 25). coindesk. Retrieved from coindesk: http://www.coindesk.com/mt-gox-statement-claims-made-conscious-decision-halttransactions/

4 Higgins, S. (August, 2016 3). coindesk. Retrieved from coindesk: http://www.coindesk.com/bitfinexbitcoin-hack-know-dont-know/
5 Khandelwal, S. (2013, November 25). thehackernews. Retrieved from thehackernews.
6 Robert D. Benford, D. A. (2000). Framing Processes and Social Movements: An Overview and Assessment. Annual Review of Sociology, 611-639.

3.10 Scalable Funding of Blockchain Micropayment Channel Networks

Roger Wattenhofer (ETH Zürich, CH), Christian Decker, and Conrad Burchert

Abstract. The Bitcoin network has scalability problems. To increase its transaction rate and speed, micropayment channel networks have been proposed, however these require to lock funds into specific channels. Moreover, the available space in the blockchain does not allow scaling to a world wide payment system. We propose a new layer that sits in between the blockchain and the payment channels. The new layer addresses the scalability problem by enabling trust-less off-blockchain channel funding. It consists of shared accounts of groups of nodes, which flexibly create one-to-one channels for the payment network. The new system allows rapid changes of the allocation of funds to channels and reduces the cost of opening new channels. Instead of one blockchain transaction per channel, each user only needs one transaction to enter a group of nodes, in which he can create arbitrary many channels. For a group of 20 users with 100 channels between them, the cost of the blockchain transactions is reduced by 90 percent compared to 100 regular micropayment channels opened on the blockchain. This can be increased further to 96 percent if Bitcoin introduces Schnorr signatures with signature aggregation.

Introduction. Bitcoin and other blockchain based payment systems are increasingly popular. This increased popularity introduces new challenges, in particular regarding scalability and transaction speed. During peaks of incoming transactions, the blockchain cannot process them fast enough and a backlog is created. We can witness these problems right now, as transactions take longer to get confirmed by the Bitcoin network, and transaction fees are rising rapidly.

We believe that these challenges need to be addressed before Bitcoin or alternative blockchain based currencies can become mainstream. The fundamental problem of any blockchain is that all transactions must be seen by everybody. Adapting the parameters (maximum size of a block, and time between two blocks) may accommodate more transactions, however only at the cost of increased propagation time and thus higher chances of blockchain forks. More forks introduce more insecurity about double spending and ultimately may prevent the network from converging to a globally consistent state. Allowing a higher transaction rate with different parameters would furthermore increase the requirements to run a full node in the network, leading to less participants and thus less decentralization.

Previous analyses have shown, that Bitcoin cannot support more than 100 transactions per second, e.g., [2, 5]. In comparison, credit card companies easily support tens of thousands of transactions per second, e.g., Visa published to support 56,000 tx/s.

In order to become a real-world payment alternative, blockchain based cryptocurrencies must support at least the transaction volume of credit cards. However, the future may be all about micropayments, transactions involving tiny amounts of money in exchange for, e.g.,

reading a single newspaper article, or driving a short distance with a self-driving vehicle. In a world with micropayments, one may imagine that millions of transactions per second must be supported to really claim scalability.

A second major problem is transaction speed, the time from initiating a transaction until one can assume that the transaction has concluded, and is thus irreversible. With inter block times typically in the range of minutes and multiple blocks needed to reasonably prevent double spending, transactions take minutes to hours until the payment is confirmed. This may be acceptable for longterm Bitcoin investors, but not for everyday shopping or interacting with a vending machine [1].

While it is conceivable to achieve a higher transaction throughput with protocol improvements, blockchain transactions still suffer from the complexity problem of a broadcast based system. New users entering will create more transactions and thus more work for each node. A long term solution needs to overcome the broadcasting principle, and transactions need to be completed with the inclusion of just a few parties.

Micropayment Channel Networks. To solve both, scalability and speed, micropayment channel networks have been proposed. A micropayment channel provides a way to trustlessly track money transfers between two entities off-blockchain with smart contracts. Trustless means that one party can show arbitrary behaviour and it is guaranteed, that each party still eventually receives its last agreed on balance. If both parties are honest they can commit the total balance of many transfers in a single transaction to the blockchain and ignore the smart contracts. If a node crashes or stops cooperating otherwise, the smart contracts can be included in the blockchain and enforce the last agreed on state.

Micropayment channel networks were proposed simultaneously by Poon and Dryja as the Lightning Network [6] and by Decker et al. as Duplex Micropayment Channels [3]. Both approaches lock funds into a shared ownership, a channel, between two participants. To spend from this shared account, both parties need to agree.

Two participants with a joint channel can transfer money directly, which allows for quick transactions. If the parties do not have a channel, a network of multiple micropayment channels can be used together with a routing algorithm to send funds between any two parties in the network. Hashed Timelocked Contracts (HTLCs) provide a scheme to allow atomic transfer over a chain of multiple channels [3, 6, 7]. Intermediate nodes can be paid for their forwarding service by decreasing the amount of sent funds with each hop.

Since micropayment channel networks will keep most transactions off the blockchain, blockchain based currencies may scale to magnitudes larger user and transaction volumes. Also, micropayment networks allow for fast transactions, as a transaction happens as soon as a smart contract is signed – the blockchain latency does not matter.

Problems. Micropayment channel networks create new problems, which have not been solved in the original papers [3, 6]. We identify two main challenges:

- Blockchain capacity. In order to have a dense network, we need a big number of channels. The problem is that each of these channels must be rooted in the blockchain.
- Locked-in funds. Funds are locked in each and every channel. Choosing a partner to collaborate with in a channel is a commitment to that party. Closing the channel and moving the funds into a new channel with a different partner needs expensive blockchain transactions, thus there is a risk involved and partners must be chosen with consideration.

It is desirable to have a dense network to ensure short paths and failure resilience. Assuming a channel lifetime of one year and one blockchain transaction per channel, the current blockchain capacity of 7 transactions per second would allow for about 200 million

channels. For redundancy a user requires more than one channel, therefore this is not sufficient as a world wide payment system.

This estimate is of course a ballpark guess, as multiple blockchain transactions per channel are needed, and the involved Bitcoin scripts result in bigger than average blockchain transactions. On the other hand new technology might facilitate more than 7 transactions per second. A more elaborate analysis was done by Dryja, who estimated the capacity in a similar range [4]. A large scale adoption of micropayment channel networks, where, e.g., Internet Of Things devices have their own Bitcoin wallet, brings the blockchain to its limit.

The locked-in funds should be sufficient to provide enough capacity for peaks of transactions. There is a conflict of the two aims to have a low amount of funds locked up in a channel, while at the same time being flexible for these peaks. This problem becomes more difficult when the lifetimes of channels increase, as one has to predict the dynamics of currency movements in the future.

We will present a solution, which solves both problems. Payment channels will not appear in the blockchain, except in the case of disputes. Users will be able to enter the system with one blockchain transaction and then open many channels without further blockchain contact. Funds are committed to a group of other users instead of a single partner and can be moved between channels with just a few messages inside the collaborating group, which reduces the risk, as an unprofitable connection can be quickly dissolved to form a better one somewhere else. By hiding the channels from the blockchain a reduction in blockchain space usage and thus the cost of channels is achieved. For a group of 20 nodes with 100 channels in between them, this can save up to 96 percent of the blockchain space.

Channel factories. As our main contribution, we introduce a new layer between the blockchain and the payment network, giving a three layered system. In the first layer, the blockchain, funds are locked into a shared ownership between a group of nodes. The new second layer consists of multi-party micropayment channels we call channel factories, which can quickly fund regular two party channels. The resulting network provides the third layer, where regular transfers of currency are executed.

Similar to regular micropayment channels, multi-party channels can be implemented with either timelocks or punishments for dishonest parties. Our implementation with timelocks performs much better, hence we will focus on it. The regular micropayment channels of the third layer can be punishment based or timelock based independent from the implementation of the multi-party channels of the second layer

Full Version. To continue reading, we refer to the full version of this work. It gives a detailed description of the construction of channel factories and different improvements to tolerate crashes of nodes. The improvement in blockchain space usage is evaluated and found to be about 90 percent. With the introduction of signature aggregation, it can be further increased to about 96 percent.

References

1 Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., and Welten, S., Have a snack, pay with bitcoins. In 13th IEEE International Conference on Peer-to-Peer Computing (2013).

2 Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., and Gun ,E., On scaling decentralized blockchains. In 3rd Workshop on Bitcoin Research (2016). http://www.tik.ee.ethz.ch/file/74bc987e6ab4a8478c04950616612f69/main.pdf.

3 Decker, C., and Wattenhofer, R., A fast and scalable payment network with bitcoin duplex micropayment channels. In Symposium on Stabiliza-

tion, Safety, and Security of Distributed Systems (2016). http://www.tik.ee.ethz.ch/file/716b955c130e6c703fac336ea17b1670/duplex-micropayment-channels.pdf.
4 Dryja, T., Scalability of lightning with different bips and some back-of-the-envelope calculations. http://diyhpl.us/wiki/transcripts/scalingbitcoin/hong-kong/overview-of-bips-necessary-for-lightning/.
5 Gervais, A., Karame, G. O., Wust , K., Glykantzis, V.,Ritzdorf, H., and Capkun, S., On the security and performance of proof of work blockchains. In 23rd ACM Conference on Computer and Communications Security (2016). http://dl.acm.org/citation.cfm?doid=2976749.2978341.
6 Poon, J., and Dryja, T., The bitcoin lightning network: Scalable off-chain instant payments, 2016. https://lightning. network/lightning-network-paper.pdf.
7 Russell, R., Lightning networks part ii: Hashed timelock contracts (htlcs), 2015. https://rusty.ozlabs.org/?p=462.

3.11 Intermodal Transportation with Blockchain

Jesse Yli-Huumo (Aalto University, FI)

Abstract. Blockchain technology has been discussed to be the next generation technology in various industry sectors. Blockchain, originally used as the backbone for various cryptocurrencies, provides more decentralized, transparent, secure and trustworthy way to complete transactions between participants in a blockchain environment. Cryptocurrencies can be seen as the first step of blockchain. However, so called blockchain 2.0 and smart contracts have been coined to revolutionize many industries after cryptocurrencies. Whereas blockchain provides trustworthy ledger, smart contracts provide trustworthy calculations to complete contracts and transactions. One of the industries where Blockchain technology could be applied is intermodal transportation, which can be seen currently as a complex and fragmented industry. Blockchain could possibly be the solution to improve complex transportations that consists various actors and means. This proposition paper discusses the possibilities of blockchain technology in intermodal transportation.

Introduction. Blockchain is a distributed database solution that maintains a continuously growing list of data records that are confirmed by the nodes (e.g. companies) who are participated in it [1]. In blockchain, the data is recorded in to a public ledger that contains every transaction ever completed [2]. Blockchain as a solution provides various interesting perspectives on transaction as a process. Since blockchain is a decentralized solution, it does not require any third-party organization in the middle. The public ledger in blockchain is shared to all available nodes that have participated, which makes it more transparent compared to current centralized transactions (e.g. banks). The participants in blockchain are pseudo anonymous, which makes it more secure for nodes to confirm transactions.

At the moment blockchain is often known as the backbone for several cryptocurrencies. Bitcoin is the most famous example of a cryptocurrency. At the moment, there is around 250 000 transactions in a day done with Bitcoin [3]. Bitcoin uses blockchain to record all the currency transactions ever made. Bitcoin does not require any third-party organization in the middle to manage all the transactions [1]. In Bitcoin, the public ledger cannot be modified or deleted after a transaction is approved by all participants (nodes) [2]. Therefore,

Bitcoin can be seen as a good example of utilization of blockchain that provides good data integrity and security characteristics [1].

Data integrity and transparency are important characteristics of blockchain and the reason why its use could be extended also to other industries, services and applications [1]. Whereas cryptocurrencies can be seen as Blockchain 1.0, smart contracts can be seen as Blockchain 2.0 [1]. A smart contract is a contract between two or more parties that is stored to blockchain [4]. Smart contract works as a computerized transaction protocol that executes the terms of a contract [5]. A blockchain-based smart contracts would visible to all users of blockchain. Companies could write smart contracts between each other and they would be stored in blockchain. Blockchain 2.0 and smart contracts have been coined to be the next step for blockchain technology and where it could be applied. There are currently various discussions, ideas and suggestions on what industries blockchain technology could improve by adding more transparency and data integrity to provide trustworthy cooperation between companies who have participated to blockchain. One of these industries could be intermodal transportation.

Intermodal transportation and its current challenges. Intermodal transportation means transportation by more than one form of carrier during a single journey. Especially in very long distance transportation (for example country to country), it will be likely that freights are transported with various transportation methods. A single transportation can include trains, road vehicles, ships and airplanes, which are organized by different transportation companies, couriers, freight forwards and multi-model transport operators.

With various companies, transportation means, information technology systems and tracking systems included to deliver a freight from country A to B, will include challenges especially in data exchange, data integrity and transparency. It is common for logistics industry that even though there are already some standardization in data exchange between transportations, the companies own systems are often closed and industry-specific. This means that in logistics and transportation industry, the information systems are fragmented. There exists a lack of a high-level information system architecture in intermodal transportation and the information about transportations in scattered around companies own information systems. Fragmentation and lack of interoperability in information technology systems could even slow down freight transportation, which can be seen as a challenge that needs to be solved.

In intermodal transportation, the progress towards interoperable information systems has been slow, which is interesting, considering for example current airline-operations and their interoperability (e.g. Amadeus) [6]. The reason might be because intermodal transportation have to handle a variety of transportation operations basically everywhere in the world [6]. The intermodal industry is also by nature fragmented, complex and highly competitive. There exist various stakeholders, working in different modes, cultures, regions, and countries. Everyone in this industry has their own business philosophy to conduct business. There are various relationships between different stakeholders that can easily [6, 7]. Therefore, it can be seen that intermodal transportation has a need for trust between companies.

Can we solve challenges in intermodal transportation with blockchain? Blockchain has been coined by many to be the technical solution to provide a decentralized technology with more transparency, data integrity and security to complete trustworthy transactions between companies. Blockchain has already somewhat proved itself to work with cryptocurrencies and now it is the time to test it also in other industry sectors. The key detail in blockchain is that there is not any role for third-party or middle-man to manage blockchain. In freight

forwarding sector, the key role and responsibilities of a "middle-man" has been traditionally various transportation-related arrangements tasks. It is the responsibility of these arbitrators to arrange that freight transportation goes smoothly and according to agreements and contracts from place A to B. However, the challenge, like in any other industries, is the role of a middle-man and the general trust between companies. How can companies trust that the information and data integrity is trustable during the transportation? How do they know what has happened to their goods during transportation?

Especially, if the transportation has been a failure. Blockchain could possibly solve this issue. In intermodal transportation, blockchain could keep some type of "decentralized situation picture" of all the freights that are part of blockchain infrastructure. It could also give information about their route history, current status information and overall documentation. With blockchain, operators in logistics could always construct a comprehensive and up-todate status of freights that are being transported in the infrastructure. This could be used for example to extract some interesting data about freight forwarding sector, e.g. companies utilization and total transportations (both successful and unsuccessful). Companies that are part of blockchain infrastructure could write smart contracts between each other, which are then confirmed in blockchain by the nodes. The public ledger of all transportations ever made, would increase transparency in intermodal transportation sector.

However, there are various questions and challenges that needs to be solved. It is also important to discuss what are the limitations of blockchain that could affect its applicability in intermodal transportation. In general, it can be seen as a major obstacle to get companies open up their data from their own information systems. This means that there must be some incentive for companies to do this. In addition, this type of blockchain would require extensive work to fetch data constantly from each company's own ERP system, which would require some standarzation between blockchain and ERPs. It would also require some type of hardware solution integration to follow freights in real-time.

Also, for blockchain and participating companies, record liability about each transportation can be seen as one major challenge [8]. Success of blockchain probably correlates to a level of security. Therefore, it is a necessity that blockchain would be secure that companies can have a trust to the system and other companies that information and data is not false. However, blockchain could be one of the most prominent ideas on how to improve transparency, data integrity and security in intermodal transportation.

Questions that need more discussion.

1. What challenges would blockchain solve in intermodal transportation?
2. What are the challenges of blockchain to manage and "oversee" intermodal transportation?
3. What type of blockchain is required for intermodal transportation? Public, private? How can companies join to blockchain?
4. What actors are there in intermodal transportation and what their roles would be in blockchain?
5. How to integrate transportation companies' different information technology systems (ERP) to work in blockchain?
6. What kind of technology is needed to track and monitor freights that the information is up-to-date in blockchain?
7. How to implement so-called mining and proof-of-concept used in Bitcoin to intermodal transportation environment? How are the completed transportations confirmed?
8. What type of smart contracts are needed in intermodal transportation?
9. What legal aspects are required in intermodal transportation for blockchain and smart contracts?

10. How are smart contracts confirmed? If there are e.g. 6 companies included to a single transportation, how is smart contract written, and then also confirmed?
11. How does pseudonymity work in intermodal transportation blockchain? What is the anonymity level of companies participating? If private blockchain, is it even needed?
12. What are the real benefits for companies that would decide to join this type of blockchain?
13. What resources does it require from companies to join blockchain?
14. What are the security issues that needs to be taken in consideration?

References

1 M. Swan, Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., 2015.
2 S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
3 "Bitcoin Block Explorer - Blockchain." [Online]. Available: https://blockchain.info/. [Accessed: 12-Mar-2017].
4 "Making Sense of Blockchain Smart Contracts," CoinDesk, 04-Jun-2016. [Online]. Available: http://www.coindesk.com/making-sense-smart-contracts/. [Accessed: 12-Mar-2017].
5 R. Sharma, "Why Smart Contracts Are the Future of Everything," Investopedia, 25-Jul-2016. [Online]. Available: http://www.investopedia.com/news/understanding-smart-contracts/. [Accessed: 12-Mar-2017].
6 A. Bask, J. Juga, and J. Laine, "PROBLEMS AND PROSPECTS FOR INTERMODAL TRANSPORT: THEORETICAL TOOLS FOR PRACTICAL BREAKTHROUGHS?"
7 C. L. Erickson et al., Challenges and opportunities for an ITS/intermodal freight program: final report. U.S. Dept. of Transportation, Federal Highway Administration, 1999.
8 V. L. Lemieux, "Trusting records: is Blockchain technology the answer?," Records Management Journal, vol. 26, no. 2, pp. 110–139, Jul. 2016.

3.12 Digital Institutions and the Blockchain

Pär Ågerfalk (Uppsala University, SE) and Owen Eriksson

Abstract. Blockchain technology has been suggested as a key technology to ensure trusted transactions in the digital society. There is a great promise but also known technical limitations; transaction speed and ecological footprint are two of the more prominent. However, we would argue that there are even more pressing institutional issues that need to be dealt with for blockchain technology to deliver on its promise. Addressing blockchain technology from an institutional perspective gives rise to some questions, such as:

- What are blocks referring to and how are these referred "things" identified?
- Which are the transactions (the transaction ledger) that are secured using blockchain technology?
- To what things do these transactions refer?
- Who has the authority to declare such "things" as valid institutional objects?
- What are the underlying institutional structures that give a particular blockchain its meaning?
- How do we deal with institutional identity?
- How to ensure the pragmatic validity of transactions?
- Who has the authority to initiate the first transaction secured by a new blockchain?
- How do we deal with accountability?

In this short position paper, we maintain that it is important to conceptually distinguish between the blockchain technology and the transactions (transaction ledger) that are secured using blockchain technology. Essentially, the combination of transaction ledgers and blockchain technology creates new forms of distributed digital institutional systems. Institutions are systems of rules. Such rules, which make the transactions meaningful, govern the transaction ledger, and the blockchain technology is only useful within that institutional context. In the following, we briefly problematise these issues and outline a research project that aims to engage theoretically and empirically with digital institutionalisation in the age of distributed ledgers and the blockchain.

Background. The ongoing digitalisation of society is fundamentally changing the institutions upon which society rests. Digitalisation is also creating new processes of institutionalisation and thus fundamentally changing how society is constructed and construed. For instance, the impact on the logics of the financial sector has been fundamental as digital currencies and cashless transactions have made it to the top in many countries (Worldatlas, 2016). Money is no longer a representation of a gold standard but a digital commodity (Aakhus et al., 2014). In the wake of this development, there are predictions of global banks operated by major IT companies, such as Google, Amazon and Facebook (Hussey, 2016). Also government agencies that want to renew their offerings and ways of working drive digitalisation.

Lantmäteriverket (2016), the Swedish National Land Survey, predicts that the transition from a paper-based to a digital, blockchain based process for property purchases may shorten the lead time from when a sales contract is signed until the ownership of the property is registered in the property register, from 4 months to 2 days. The transition to a digital process promises efficiency, but an equally important aspect is the promise of trust. Traditionally, a key part of building trust is a written signature on a paper document. Contracts, sales agreements and mortgages are stored on paper to build confidence and maintain legitimacy. However, the paper handling is also error prone. A problem with hardcopy mortgage documents is that they may disappear or be destroyed (Lantmäteriverket, 2015).

Blockchain technology enables the development of new types of digital institutions, including ensuring the authenticity of digital files and transactions. The development is enabled through a combination of openness, collective authentication, encryption algorithms and requirements to supply processing power. This technology enables governments and companies to manage documents or information from registers outside the organisation's firewall, without compromising security and confidence. Openness and transparency of government actions and decisions create confidence in companies and government agencies. Clearly, this openness and transparency is in line with the principle of public access. What is new with the digital public sphere and the way it works, is that not only documents but also to the institutional process can be made more open and transparent. Confidence in the institutional processes increases when these processes are openly accessible and evidently difficult to manipulate. This can be implemented, among other things, by making use of blockchain technology, which has even come to be known as the "trust machine".

Digital Institutions. Knowledge of blockchain technology is necessary when it comes to analysing contemporary digital institutionalisation. Such analysis, however, requires also an understanding of the concept of the institution. The social world is a result of institutionalisation that occurs through social interaction and consensus about how to perform activities. This creates trust since an institutionalised behaviour creates a social order based on rules, agreements and standards (Berger and Luckmann, 1966). From an ontological perspective, institutions can be seen as systems of established rules that structure social

interactions (Hodgson, 2006). Studies of institutions have largely been oriented toward the pillars that underlie institutional structures, that is rules, norms and cultural-cognitive aspects (Scott, 2003). What has been overlooked is the digital mediation of institutions and institutionalisation processes (Couldry and Hepp, 2016). Institutionalisation is about how the institutional system is created, reproduced and discontinued. These are processes that occur over time and space and across cultural and organisational boundaries. One way to understand institutionalisation is to turn to Searle (1995, 2005, 2006). Searle explains how institutional facts, such as contracts, money and deeds can be created in and through the execution of communication actions. These communication actions are deontic by virtue of them being used to creating rights, responsibilities and privileges. They must, therefore, be based on public acceptance.

The "Digital Institutionalisation" project. Understanding digital institutionalisation is about understanding and examining the relationship between institutional language, rules, processes, information, actors, actor relationships and the development of digital infrastructures. The aim of the research project 'Digital Institutionalisation' is to, in a profound way, describe how the blockchain affects and is affected by institutionalisation. Issues that may prevent such a development are rules and laws that have not kept up with the development (European Council, 2016; The Telegraph, 2017). Also, outdated IT systems, the so-called 'installed base' can be an obstacle (Tieto, 2014). An important question is also to study who has the power to design and develop a digital institutional system. The development of digital infrastructures is about power structures created or maintained (Eriksson and Goldkuhl, 2013). There are, for instance, a strong belief that technologies such as Blockchain, which enables new means of payment (such as Bitcoin), will change the balance of power in the banking sector. Power is not just about who has the knowledge of the technology. It is about who has power over the development and change of the institutional language, rules, processes, transactions, and institutional facts created.

Given the relatively sparse number of studies on digital institutionalisation in society (Mignerat and Rivard, 2009; DeVaujany et al., 2014), the results of our inquiry mainly provide a deep understanding of how digital institutionalisation occurs over time and space. Such deep understanding has both practical and theoretical implications. Our goal is to describe and to create new concepts, models and theories for how this occurs. We want to describe how an institutional design interweaves rules, languages, institutional processes, and institutional facts, and how blockchain technology could enhance such a design.

References

1 Worldatlas (2016) Top Countries Using Digital Money For Cashless Transactions, http://www.worldatlas.com/articles/which-are-the-world-s-most-cashless-countries.html (last accessed 12 March 2017).
2 Aakhus, M., Ågerfalk, P. J., Lyytinen, K, Te'eni, D. (2014) Symbolic action research in Information Systems: Introduction to the Special Issue, MIS Quarterly, 38(4), 1187–1200.
3 Berger, P. L., Luckmann, T (1966) The Social Construction of Reality: A Treatise in the Sociology of Knowledge, Garden City NY: Anchor Books, ISBN 0-385-05898-5.
4 Couldry, N., Hepp, A. (2016) The mediated construction of reality. John Wiley and Sons.
5 DeVaujany, F. X., Carton, S., Mitev, N., and Romeyer, C. (2014). Applying and theorizing institutional frameworks in IS research: A systematic analysis from 1999 to 2009. Information technology and people, 27(3), 280-317.
6 Eriksson, O., and Goldkuhl, G. (2013). Preconditions for public sector e-infrastructure development, Information and organization, 23(3), 149-176.
7 European Council (2016) Digital single market for Europe.

8 Hodgson, G. (2006). What Are Institutions? Journal of Economic Issues, XI (1).

9 Husssey M. (2016) The banks of Google, Facebook and Amazon, https://thenextweb.com/facebook/2016/05/05/banks-google-facebook-amazon/ (last accessed 27 January 2017)

10 Lantmäteriverket (2015) Säkrare och enklare panträtt i fast egendom, Utredningsrapport, Dnr 501-2015/2584 (In Swedish)

11 Lantmäteriverket (2016) Framtidens husköp i blockkedjan. Ett utvecklingsprojekt med Lantmäteriet, Telia Company, Chromaway och Kairos Future. (In Swedish)

12 Mignerat, M., Rivard, S. (2009), Positioning the institutional perspective in information systems research, Journal of Information Technology, 24 (4), 369–391.

13 Scott, W. R. (2003) Institutional carriers: reviewing modes of transporting ideas over time and space and considering their consequences, Industrial and corporate change, 12(4), 879–894.

14 Searle, J. (1995). The Construction of Social Reality. Free Press.

15 Searle, J. (2005). What is an institution. Journal of Institutional Economics, 1(1), 1–22.

16 Searle, J.R. (2006). Social ontology: Some basic principles. Anthropological Theory, 6 (12).

17 The Telegraph (2017) How to set up a new bank: It'll take you longer than you think and cost more than you think.

18 Tieto (2014) Uppstickare utmanade storbankerna på Bankdagen.

Participants

- Pär Ågerfalk
Uppsala University, SE
- Michel Avital
Copenhagen Business School, DK
- Roman Beck
IT University of Copenhagen, DK
- Christian Becker
Universität Mannheim, DE
- Joseph Bonneau
Stanford University, US
- Marcus Dapp
fortiss GmbH – München, DE
- Peter Eklund
IT University of Copenhagen, DK
- Fritz Henglein
University of Copenhagen, DK
- John Leslie King
University of Michigan – Ann Arbor, US
- Christoph Kreiterling
BaFin, DE
- Juho Lindman
University of Gothenburg | Chalmers UT, SE
- Alberto Montresor
University of Trento, IT
- Christoph Müller-Bloch
IT University of Copenhagen, DK
- Matti Rossi
Aalto University, FI
- Joachim Schrey
Noerr LLP – Frankfurt, DE
- Gerhard Schwabe
Universität Zürich, CH
- Peter Sestoft
IT University of Copenhagen, DK
- Virpi Tuunainen
Aalto University, FI
- Marella Venkata
Aalto University, FI
- Roger Wattenhofer
ETH Zürich, CH
- Jesse Yli-Huumo
Aalto University, FI