CAPCO

Journal

THE CAPCO INSTITUTE JOURNAL OF FINANCIAL TRANSFORMATION

Operational

Development of Distributed Ledger Technology and a First Operational Risk Assessment

Udo Milkau, Frank Neumann, Jürgen Bott

APEX 2016 AWARD WINNER

FINANCIAL TECHNOLOGY

Download the full version of The Journal available at CAPCO.COM/INSTITUTE

#44
11.2016

Empowering the Financial World

FISGLOBAL.COM

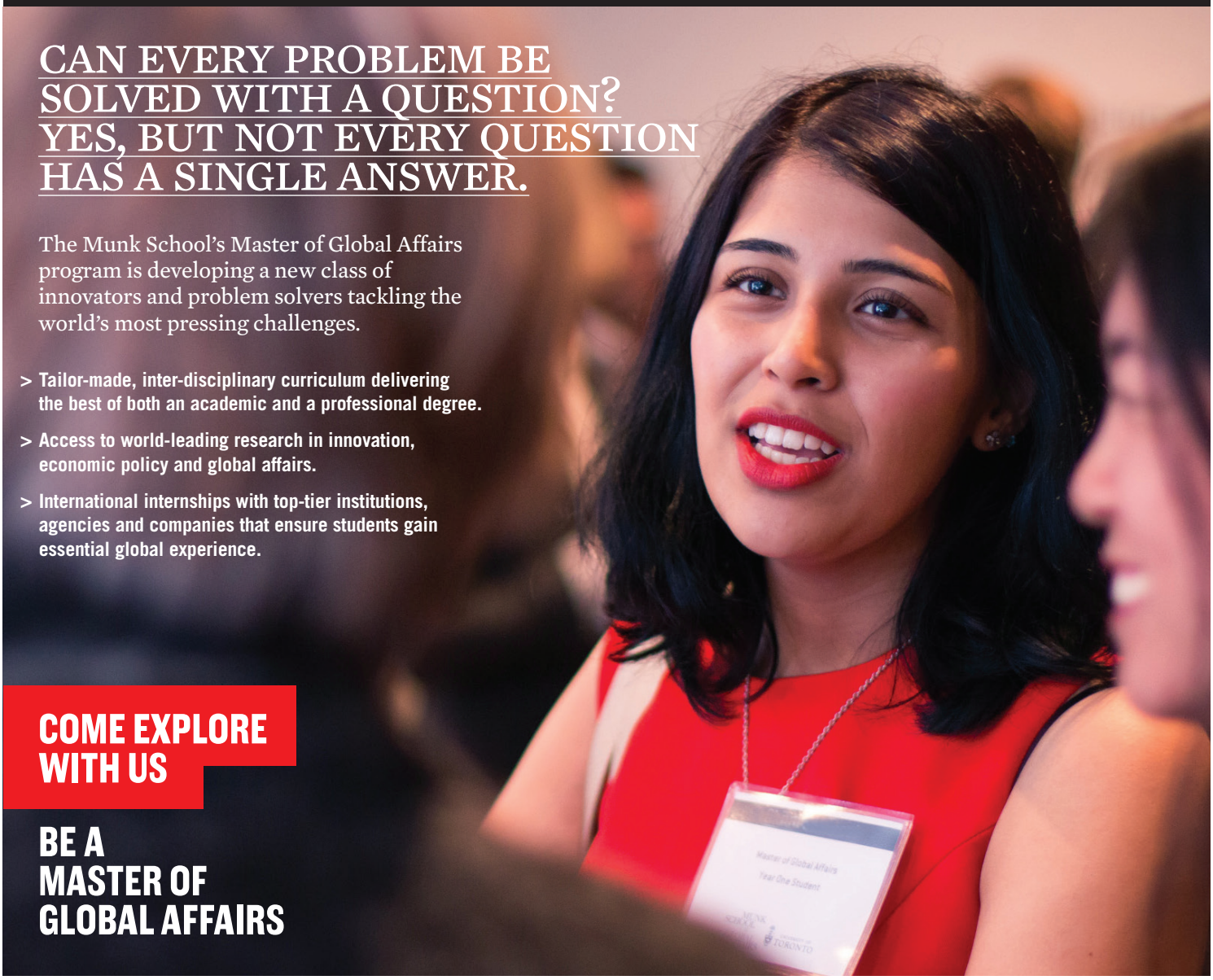
FIS

Journal

The Capco Institute Journal of Financial Transformation

Recipient of the Apex Award for Publication Excellence

WHAT ARE THE DRIVERS AND DISRUPTIONS THAT DETERMINE INNOVATION AND PROSPERITY?



CAN EVERY PROBLEM BE SOLVED WITH A QUESTION? YES, BUT NOT EVERY QUESTION HAS A SINGLE ANSWER.

The Munk School's Master of Global Affairs program is developing a new class of innovators and problem solvers tackling the world's most pressing challenges.

- > Tailor-made, inter-disciplinary curriculum delivering the best of both an academic and a professional degree.
- > Access to world-leading research in innovation, economic policy and global affairs.
- > International internships with top-tier institutions, agencies and companies that ensure students gain essential global experience.

COME EXPLORE WITH US

BE A MASTER OF GLOBAL AFFAIRS

MUNKSCHOOL.UTORONTO.CA
MGA@UTORONTO.CA

MUNK SCHOOL OF GLOBAL AFFAIRS
UNIVERSITY OF TORONTO

Financial Technology

Operational

Transformational

Development of Distributed Ledger Technology and a First Operational Risk Assessment[1]

Udo Milkau – Chief Digital Officer - Transaction Banking, DZ BANK AG, Frankfurt; and Goethe University, Frankfurt
Frank Neumann – DZ BANK AG, Frankfurt
Jürgen Bott – Professor of Business Administration, University of Applied Sciences in Kaiserslautern/Zweibrücken

Abstract
Distributed ledger technology (DLT) is a new approach, first implemented by Bitcoin, the basic features of which are the elimination of any intermediaries in peer-to-peer (financial) transactions and the replacement of "trust" by a game theoretical approach of consensus among all participants who agree "to play a repeated game." The promises of DLT are more efficiency (by removal of redundant intermediaries), more resilience against attacks or manipulation (through multiple replicas and chaining of transactions with mutual references), and more security for asset owners (by making an original transaction technically unalterable/immutable). Nevertheless, the so-called "TheDAO hack" in June 2016 made clear that a complex DLT-based software system is vulnerable against manipulation if one has in-depth understanding of the code and its errors. In this paper, a first risk assessment of the new technology of "smart contracts" is made and the question about "code is law" is discussed. While the basic concept of Bitcoin does not raise new types of operational risk, the current technology of "smart contracts" has a fundamental flaw due to the combination of complex software (with inherent probability of errors and software aging) on one side and the static/non-changeable, approach of blockchain on the other. Static/non-changeable contracts can be used for short-term "one-time" interactions, but any long-term relationship has to be governed by common standards, legislative frameworks, and operational risk management – together providing the possibility for adoption to real world changes. These findings are in line with the recent development of DLT to distributed "private" ledgers and to central share services utilities for, for example, post-trading processing for a closed group of participants with pre-identified roles and responsibilities.

1 We would like to thank the following for their comments on the previous drafts of this article: Helmut Siekmann (Goethe University Frankfurt, IMFS), Christian Janze (Goethe University Frankfurt, E-FinanceLab), Ritva Tikkanen (Justus Liebig University Gießen), Roman Beck (IT University of Copenhagen), Thomas Schönfeld (PwC, Frankfurt), and especially thank Wolfgang König (Goethe University Frankfurt, Managing Director House of Finance) for the organization of the E-FinanceLab Fall Conference 2016 on "Blockchain: technology, legal and regulation, and application in the finance realm." The views expressed in this article are those of the authors and are in no way representative of the views of their employers.

INTRODUCTION: FROM VULNERABILITIES OF THE BITCOIN ECOSYSTEM TO THE "THEDAO HACK"

DLT, also known as "blockchain," has been capturing interest since the publication of Ali et al.'s (2014) article in the Bank of England Quarterly Bulletin. Even though we are still coming to grips with this new technology, reading through the many analyses of DLT it is not clear whether it is a solution looking for a problem or whether many genuinely believe that it will solve all problems of the previous decades. In reality, while DLT is an innovative jigsaw puzzle of existing pieces and can be a catalyst for new applications and solutions, as with all new technologies one has to assess its operational risk ramifications – especially if used for critical financial infrastructures.

One frequently used narrative suggests that "blockchain" provides a cryptographically secured, immutable, and resilient registry of transactions concerning rights of ownership. In other words, it would be a real "golden source" without any need of regulated and/or trusted intermediaries. However, a number of incidents with Bitcoin, such as insolvency of the Bitcoin exchange Mt. Gox, criminal Ponzi schemes such as the pyramid scheme "MMM," or the fraud after a "security breach" at the Bitcoin exchange Bitfinex [Baldwin and Poon (2016)] make one question the validity of such claims. The Bitfinex case is quite informative since it notified clients that it will "share" the losses across its entire user community irrespective of whether a client was actually affected and where and in which currency their funds were [Finextra (2016)].

Those rather well known types of risks in the context of virtual currencies have already been widely covered elsewhere [EBA (2014)] and will not be covered in this article. Our decision to exclude them was also related to the fact that (i) they all followed well-known modus operandi and (ii) they happened outside of Bitcoin blockchain and in the "real" world of fiat money. Nevertheless, it should be mentioned that the European Commission published a number of proposals for amendments to the current directive on fighting money laundering, financial crime, and terrorist financing as a result (July 5, 2016). These included proposals to bring virtual currency custodian wallet providers (CWPs) and virtual currency exchange platforms (VCEPs) within the scope of the directive as obliged entities. The European Banking Authority (EBA) commented on that proposal and according to EBA's point of view: "There is a risk that consumers and business partners of VCEPs and CWPs may not be aware that the imposition of requirements on VCEPs and CWPs for AML/CFT purposes does not include or imply consumer protection or prudential safeguards, including capital requirements, calculation of own funds, safeguarding requirements, separation of client accounts, and the extensive authorization liability" [EBA (2016)].

All the aforementioned issues concerning asset protection are aligned with the current regulatory initiatives and do not depend per se on new technologies. However, the so-called "TheDAO hack" exhibited unique characteristics, since someone was able to exploit vulnerabilities in the underlying blockchain technology and the "smart contract" extension. TheDAO is a so called "decentralized autonomous organization," which is an organization with no people and based only on codes representing contractual relationships. In June 2016, an "attacker" was able to take the equivalent of more than U.S.$40 mln from TheDAO. The fact that it happened within the rather complex technical system raises many questions, such as: was it a "software error" or a (intended, but hidden) feature of the written code? Was it a "game" in a closed environment with peculiar rules or some criminal action against applicable laws?

In this paper, the first risk assessment of DLT and "smart contracts" is presented. It is aligned with the framework of Aven (2011), with the main focus being (i) the assumptions and limitations of the technology, (ii) its usability and reliability, and (iii) our understanding and communications about it.

As DLT – and even more so smart contracts – is a rather new technology, this paper will cover it in a step-by-step format. This approach includes an analysis of the fundamental limitations of DLT and provides a risk assessment of the extension to smart contracts. It also scrutinizes the sociological aspects of new technology, where an entire community wants to believe in the benefit of a new technology without considering its theoretical limitations and without applying the common standards of operational risk management.

THE ROAD TO THE BLOCKCHAIN – POSSIBILITIES AND IMPOSSIBILITIES IN A NUTSHELL

As DLT deals, by definition, with transactions concerning rights of ownership (something "ledgers" are designed for), its foundation is a distributed network of participants that want to execute transactions, i.e., transfer of rights of ownership in a network of linked computer systems ("nodes"). Of course, the classic example is the Internet, in which the end-users never know which other nodes forward their messages, which routes are taken, and which nodes dynamically join or exit the network.

For more than 40 years, distributed computer systems have been studied, and the possibilities and impossibilities of the technology assessed [Attiya and Ellen (2014)]. Those fundamental impossibilities and conditional possibilities of distributed computing have to be the first step in risk assessment, as they provide the theoretical foundation and, consequently, the fundamental framework, in which the technology works.

- The "two generals problem" (or "byzantine generals problem" [Akkoyunlu et al. (1975)]): the impossibility of synchronizing two or more participants via a network of unknown (i.e., trustless) nodes in a finite time. It has to be remarked that this concerns the synchronization in general and not the exchange of secure, encrypted messages.
- "Byzantine fault tolerance" [Lamport et al. (1982)]: possibility of resilience of a network of known nodes against failure or manipulation based on a voting consensus with a pre-defined fall back option in case of timeout (typically handed over to an external third-party, such as human pilots in case the triple autopilot system cannot "agree").
- Impossibility of distributed consensus [Fischer et al. (1985)]: impossibility of a consensus in a distributed network with the conditions that (i) one process/node may fail and (ii) the consensus should be reached in finite time.
- Proof of work concept [Dwork and Naor (1992)]: basis for a probabilistic approach to select a neutral referee in a network of ex-ante trustless nodes. As with any voting in an open, anonymous, computer network for a quorum consensus can be compromised by a single faulty entity simulating multiple identities ["Sybil Attack," see Douceur (2002)]. Proof of work provides a "game theoretical" solution for consensus under some conditions.
- Introduction of the concept of "software aging" [Parnas (1994)]: understanding that software systems always have errors, which result from the interaction of the different layers, but especially that software can "get old" and will develop "unexpected" errors over time due to the complexity of the technology and the interaction of multiple layers.
- CAP-theorem [Brewer (2000 and 2012)]: impossibility in any networked shared-data system that one can achieve all three desirable properties: consistency, availability, and partition tolerance (= fault tolerance, if part of the system fails).
- Development of "secure hash algorithm 2" [SHA-2 (2001)]: SHA-2 – as an example of hash functions – is a set of injective hash "one-way" functions designed by the National Security Agency (NSA) and published by the U.S. National Institute of Standards and Technology (NIST) for the cryptographic protection of sensitive information against manipulation, especially when stored in or transmitted via open networks.
- Double spending problem [and its prevention; see Osipkov et al. (2007) and Hoepman (2008)]: possibilities to prevent so called "double spending" as a failure mode of electronic cash schemes, as any electronic message, i.e., a bit string of 0's and 1's, can be copied and sent to manifold different beneficiaries in a network.

With this set of possibilities and impossibilities in distributed computing, the scene was set at the end of the last decade for practical solutions to solve the challenge of "electronic cash" in distributed computer systems under certain limitations (see Figure 1 for illustration of an approach to distinguish DLT from general database management systems).

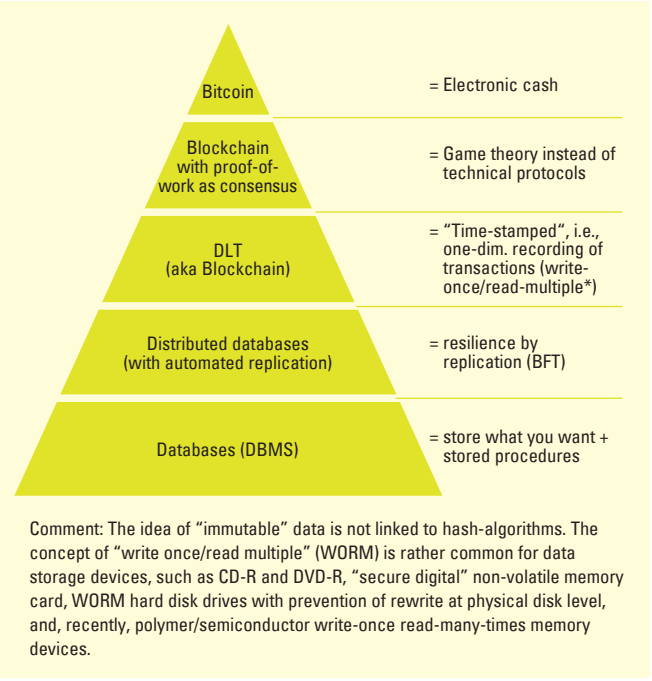


Figure 1 – A schematic approach to distinguish DLT and established database management systems

THE CONCEPT OF BITCOIN – GAME THEORY AND EVENTUAL CONSISTENCY

The quest for "electronic cash" had the goal of creating a substitute for real cash in an open distributed computer network of equal peers without any intermediaries that could provide "trust."

In 2008, Satoshi Nakamoto (2008; a pseudonym) published a paper entitled "Bitcoin: a peer-to-peer electronic cash system," [see, for example, Ali et al. (2014)]. It is well known that this first implementation of DLT is inefficient, expensive, rather slow, and without sufficient capacity as compared with established payment system networks.

Nevertheless, Bitcoin was a solution to the question above – but with clear assumptions. The innovation of Bitcoin was thinking out-of-the-box and, consequently, a game theoretical solution with a "proof-of-work" to select one neutral referee instead of "democratic" voting protocols [Decker and Wattenhofer (2013)]. The game had

a set number of parameters that had to be accepted by all. First, all "players" have to pledge their stakes (investment in computer resources = cost for hardware, energy consumption, etc.). Second, the "proof-of-work" is the virtual equivalent to tossing the dice (to decide who may start a game). Third, the winner will be the referee for the next block with a fixed sequence of new transactions and is rewarded with a combination of newly created Bitcoins (i.e., seigniorage) and transaction fees (paid by the users).

With this set of parameters, Bitcoin is a repeated game and a closed-loop system, in which (i) transactions and (ii) incentives for the winners are closely linked together by the same "electronic cash," i.e., Bitcoins. Any transfer of the concept of Bitcoin to other rights of ownership – e.g., property – raises the question of how to include an incentive in the model without the need of external intermediaries.

This game theoretical approach comes with the principle disadvantage of the probability of two referees – at different nodes in an extended network with latency – creating different new blocks with different transactions in parallel at the same time ("fork"). In the Bitcoin blockchain, such forks happen with approximately 1.7% of all new blocks [Decker and Wattenhofer (2013)]. This – temporary – inconsistency will be automatically restored later by the blockchain algorithm, but this "interregnum" can last up to one hour, as recorded in mid-2015. When a system trades "social" trust for an "algorithmic" substitution, one has to recap Niklas Luhmann's statement that "trust is a mechanism to reduce complexity" [Luhmann (1968)]. The substitution comes with a price tag (inefficiency) and downsides (limited finality).

While The Economist [2015] called the blockchain technology "The trust machine," the implementation of Bitcoin only has an "eventual consistency" [Decker and Wattenhofer (2013)]. Eventual consistency is neither new in distributed computing [Lindsay et al. (1980) and Vogels (2009)] nor unknown in banking [Wattenhofer (2016)]. Imagine an ATM in offline mode, i.e., the ATM is able to perform transactions but is temporarily not connected with the bank's host. A customer can make a withdrawal with their debit card using an offline transaction limit assigned to the card. A transaction could be completed even if there are insufficient funds on the account, as long as the offline transaction limit is sufficient for the stand-alone withdrawal. At a later point in time, when the ATM is back in the network again, a reconciliation process has to align the bank's ledger.

A second example is the SEPA Direct Debit Core Scheme (SDD), which grants payers a "no-questions-asked" refund right within eight weeks. A merchant debiting a payer's account by a SDD transaction has to wait for those eight weeks to reach finality or, respectively, has to calculate and manage the probability of a client's recall (i.e., credit risk).

Synopsis I

Independent of the inefficiency of Bitcoin, the probabilistic approach is no source of operational risk. Of course, eventual consistency implies a typical credit risk exposure for the beneficiary, which is rather common in payments. Nevertheless, insight into the game theoretical approach of the concept, the nature of a blockchain as a repeated game, and careful consideration of the assumptions (e.g., of an egalitarian – non-hierarchical – peer-to-peer network) are required.

THE REALITY OF THE BITCOIN ECOSYSTEM – TOWARDS CENTRALIZATION

The actual Bitcoin ecosystem has diverged from the original concept. Firstly, typical "users" of Bitcoin are not keen to operate a part of a payment infrastructure, but want to make Bitcoin payments in a simple and convenient way. Those customers use Bitcoin wallet providers and have to rely on them as "custodians" for their funds in the bitcoin ecosystem [Leinonen (2016)]. Secondly, the costly proof-of-work (with huge electrical power consumption and large investments in dedicated hardware) represents a negative externality with socially inefficient excess of resources.

This paves the way for a centralization of the Bitcoin ecosystems with an onion-like structure between a core of dedicated nodes (mining pools) and typical users. The current Bitcoin ecosystem is starting to resemble informal money transfer systems, typically "Hawala" systems [Passas (2006)], which work with a clearing of information messages between agents in different countries (hawaladar), typically based on some kinsmanship.

In addition, the centralization of computing resources within so-called mining pools opens the door to the possibility of a "51% attack," i.e., one attacker with more than 50% of the computational "hashing" power in the ecosystem could calculate proof-of-work solutions in sequence faster than the rest of the network and rewrite the transaction history [Decker and Wattenhoffer (2013)]. One mining pool, Ghash.io, reached 50% of the bitcoin network's hashing power in June 2014 [Cawrey (2014)]. The centralization can also be found in other blockchain systems, e.g., in Ethereum, with one mining entity ("dwarfpool") dominating the system with circa 48% of the resources in March 2016 [Dienelt (2016)]. For a deeper discussion, the reader is referred to the literature [Sirer and Eyal (2013), Eyal (2014), Hearn (2016)].

The onion-like ecosystem is antagonistic to the original egalitarian peer-to-peer concept. As Joichi "Joi" Ito wrote in a blog [Ito (2015)]: "there is currently centralization in the form of mining pools and core development, [but] the protocol is fundamentally designed to need decentralization to function at all."

It's worth noting that there is a current trend to centralized systems – especially in payments (see Figure 2). Different from the traditional model of the payments industry with interoperable banks and central banks, the initial steps were towards (i) centralized business platforms, such as PayPal, which internalize all accounts (buyers' and sellers' accounts) and (ii) the Bitcoin approach of a fully decentralized electronic cash system. But the more recent developments are even closer to the concept of central "utilities," be they provided by a central bank (central bank digital currency) [Broadbent (2016), Barrdear and Kumhof (2016) and Reuters (2016)], Bitcoin service providers, distributed "private" ledgers (see below), or even bank-owned initiatives, such as the SWIFT global payments innovation initiative [SWIFT (2016)].

Synopsis II

The derivation from the original concept and the development of an internal hierarchical structure centralization (instead of a peer-to-peer network) lead to the development of typical single points of failure. These vulnerabilities raise fundamental questions about the liabilities of such centralized structures – especially if not regulated as in the case of Bitcoin – to open issues concerning the risk of a "51% attacks." As long as these questions are unanswered, Bitcoin will be in legal limbo but, nonetheless, has its niche as the current usage shows. Nevertheless, the trend to centralization, as opposed to regulated interoperable intermediaries, makes one wonder about where the responsibility for an end-to-end operational risk management sits and who is liable in case of errors?

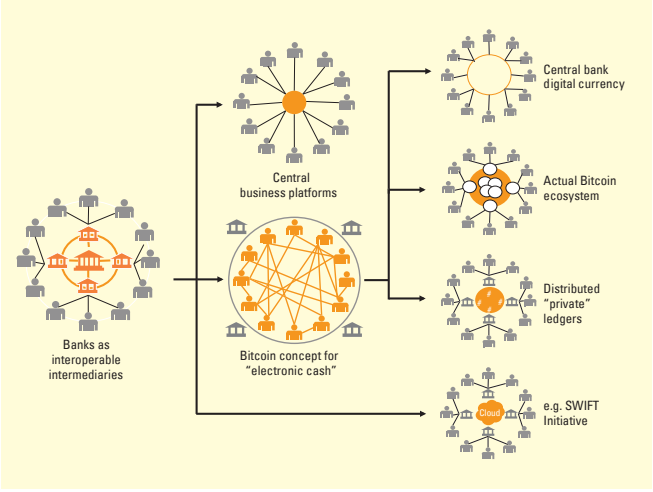


Figure 2 – A taxonomy of the current trends in banking

THE EXTENSION OF THE DLT – SMART CONTRACTS AND CODE IS LAW

The Bitcoin blockchain is a flat, sequential, one-dimensional database for the transfers of rights of ownership: Alice does not send Bitcoins to Bob's account, but broadcasts a message that a certain amount of Bitcoins can be claimed by anybody who has Bob's credentials (i.e., his cryptographic key). If someone is able to access Bob's keys, then this person has the access to Bob's assets. However, the Bitcoin blockchain has a rudimentary status concept and distinguishes "transactions" between unspent (available to be claimed) and spent (already claimed).

The so called "smart contracts" are an extension to this recordkeeping of ownership. In the current discussion, smart contracts are often described as self-executing/self-enforceable software representing contractual relations, which are stored immutably on the blockchain and, consequently, do not require any third party to create trust. In principle, a smart contract is a terminus technicus for a program code that is executed in a dedicated blockchain environment, such as Ethereum [Dienelt (2016)]. A smart contract does not do anything by itself, but has to be triggered by an external transaction and can in return create new transactions which interact with other code on the blockchain [Greenspan (2016)]. Consequently, smart contracts are similar to stored procedures in traditional database management systems. Nevertheless, every computer program is simply a sequence of zeros and ones that performs calculations and store results on a tape or "on a chain." This fundamental concept was

Code of the "smart contract"

+

Interaction with other code (i.e. other smart contracts)*

+

Compiler and virtual machine (needed to execute the code)

+

Potentially supporting services such as storage and messaging

+

Software of the blockchain itself

+

Operating systems (OS) on the distributed computers to run the local replica of the blockchain

+

Network protocol stack for the communication via the internet

* For example, in the "Ethereum" blockchain smart contract, code is written in an own programming language "Solidity," which has – per definition – the ability to provide interaction of contracts. Such intended interactions can lead to unintended reactions depending on the sequence of transactions, combination of parameters, etc.

Figure 3 – Combination of a blockchain with user provided, executable code in a complex environment of multiple layers

already described by Alan Turing as the so-called "Turing Machine" in 1937 [Turing (1936)] and has been the basis for computers since then (with the exception of parallel computing).

The crucial issue is the combination of a blockchain with user provided, executable code in a complex environment of multiple layers (Figure 3). If a blockchain contains some validated smart contracts and this code produces a result, then even 1 + 1 = 3 is "right" according to the rule of DLT. This is "code is law" according to Lessig (2000), who feared that the technical rules of cyberspace could overwrite contractual and legal norms.

Experience demonstrates that any non-trivial software has errors, and even well tested software packages typically show "low-frequency/high-severity" errors – sometimes after many years. According to Dienelt (2016), there could be approximately "100 bugs per 1,000 lines of code" in the Ethereum blockchain software. This is a new development that started 2014, and, consequently, errors are rather natural.

It would be not be fair to compare a relatively nascent technology with developments over decades, but any human-written software displays errors as inevitable companions. As a benchmark, Dienelt (2016) states that Microsoft has "one bug per 2,000 lines of code." From an operational risk perspective errors are likely to happen, hence what matters is the probability of occurrence. However, DLT will treat validated "unalterable" code as "final" and consequently excludes any probability for errors over time.

TheDAO" is the decentralized autonomous organization, an organization with the objective to implement the theoretical concept that a firm is just a set of contracts and can be set up with any people or tangible assets. It is comparable to an investor-directed venture capital fund and was crowdfunded in May 2016. The funding was stored as digital tokens in the Ethereum blockchain and the value as of 21 May 2016 was more than U.S.$150 mln provided by 11,000+ investors [Siegel (2016)]. By Saturday, 18th June, "somebody" managed to drain more than the equivalent of U.S.$50 mln into a copied "child DAO," from which they can access and forward the value after 28 days (which was the initial funding period of "TheDAO" defined in the original code). Soon after this event, there were discussions among experts about what the event actually was. Sirer (2016) stated: "I'm not even sure that this qualifies as a hack. To label something as a hack or a bug or unwanted behavior, we need to have a specification of the wanted behavior. […] The hacker read the fine print better than most, better than the developers themselves. [...] the only consistent response is to call it a job well done."

To solve this problem, Vitalik Buterin, a co-founder of the public Ethereum blockchain platform [Buterin (2016)], proposed some possible actions to "correct" the whole system according to the original "intention." But any kind of ex-post changes to the "unalterable" blockchain or any "retroactive" update to the software environment fundamentally contradicts the basic concept that blockchain is immutable and that "smart contracts" – once validated – are final and cannot be reverted or manipulated. Nevertheless, in July 2016, the Ethereum "community" – represented by the decentralized holders of the virtual currency "Ether" – voted with 97% of Ethers for a so-called hard fork solution (i.e., massive manipulation of the basic software program of the blockchain).

They supported Buterin's statement about "differences between implementation and intent." A hard fork of the Ethereum blockchain was implemented on July 20, which moved all funds of "TheDAO" to a new smart contract, returned the U.S.$40 mln and let the original owners withdraw the funds [del Castillo (2016)].

This development has two direct implications:

- The innovation of Bitcoin was the implementation of the game theoretical proof-of-work to achieve consensus and to avoid the problem that any voting in a decentralized computer network can easily be compromised with a Sybil attack. Consequently, any external "voting" – instead of the internal consensus algorithm – to solve the "TheDAO" hack is a contradictio in adiecto.
- Compared to the ex-ante rule "code is law," concepts like "original intention" open the doors for some ex-post interpretations. In the best case scenario, this leads to a teleological approach, and in the worst case, this is the road to arbitrariness.

Like any other human-made technology, smart contracts are never hundred percent secure and safe. The consequence is that (i) fault tolerance requires reliability software engineering [Lyu (1996)] and (ii) a big red "stop button" is needed in case of emergency. Thus, there has to be some intermediary outside a DLT system with a "license to kill" if some program code is going mad [Marino and Juels (2016]. Unfortunately, this is the end of immutable code in the sense of a golden record without any intermediaries.

Synopsis III

From the point of view of operational risk management, the combination of a complex software system with inevitable errors and software aging on the one side and the basic rule of "code is law" on the other has a fundamental flaw. While the concept of Bitcoin works for the right of ownership of "electronic cash" with immutable records, the extension of DLT to smart contracts depends on immutable (i.e., pre-defined and unalterable) courses of actions in a dynamic relationship between contract partners. There is an implicit assumption far from being realistic that the individual programs and the whole complex software environment are completely free of errors in the

current and any future scenario. However, "TheDAO" hack is a textbook example of a high-severity/low-frequency operational risk event, which shows up rather infrequently and is not detectable in short-term tests or in production with a limited runtime.

BOUNDED RATIONALITY AND INCOMPLETE CONTRACTS

The concept of "bounded rationality," which was developed by Simon (1957, 1991) and Gigerenzer and Selten (2002), underlines the idea that any decisions made by individuals (including decisions on how to write a software code) are made with limited rationality. In reality, not all information is available, there are cognitive limitations, or the time available to make decisions is simply not sufficient for a full calculation – whether made by people or computers. While classical economics deals with a normative concept of perfect information and pure knowledge of all possible options, "bounded rationality" is a positive approach to real situations and dynamical, path-dependent ways into the future. Consequently, any non-trivial contract cannot include ex-ante all situations to be managed later on.

The paradigm of "incomplete contracts" was further developed by Grossman and Hart (1986), Hart and Moore (1990), and Hart (1995). They argue that real-world contracts cannot specify what is to be known for every possible future contingency. In parallel to a contractual relationship, a governance model is required to solve future frictions and intermediaries can take on the role of advisors or mediators [Williamson (1979, 1985, 2002)].

As the rationality of humans – and machines – is limited, contracts will reveal incompleteness generically. The (normative) vision of a frictionless and ex-ante ultimately defined contractual relationship has to be replaced by the understanding of the actual (positive) reality of errors and inconsistencies. To remedy incompleteness, governance models are required for a balance between archaic enforcement of rules and the danger of moral hazard when freedom of contract comes without future responsibility.

It is also worth noting that – due to bounded rationality – nobody can be sure that a technical protocol like Bitcoin is free of errors and of (hidden) backdoors. No blockchain will ever be a 100% "truth machine" – and more complex protocols such as platforms for smart contracts are vulnerable to the probability of errors.

Synopsis IV
If for a split-second, one assumed that a software could be free of any errors and translate a legal contract into a code 1:1, without any problems in semantics and syntax, this code would reflect the static situation at the time of codifying. Within a closed system this may be applicable as in any game people play with fixed rules. However, dynamic contractual relationships between economic agents in reality – with contracts on paper or in the blockchain – have to take bounded rationality and incomplete contracts into account. Governance models with intermediaries and/or principle-based jurisdiction are needed to remedy those limitations, especially in the dynamic development of the real world over time. In general, human-made technology cannot overcome the limitation of bounded rationality. Mechanisms are required to solve the problem of "incompleteness" in any contractual requirement. Courts, arbitrators or, respectively, banks are essential to do this job.

DISTRIBUTED "PRIVATE" LEDGERS (DPLT)

Based on DLT in general, DPLTs were developed to facilitate decentralized recordkeeping in closed groups with ex-ante identified and registered participants, i.e., there has to be some central registry or trust center. This confronts the distributed "public" ledgers with anonymous and "trustless" peers in a distributed computer network without any intermediaries. Within such a "trusted" network, a substitute for trust between "trustless" participants is no longer required. The main remaining issue of distributed "public" ledger is byzantine fault tolerance (BFT) [Lamport et al. (1982), Castro and Liskov (1999), Castro and Liskov (2002) and Correiam et al. (2011)].

BFT ensures that a number of distributed computer systems running identical processes still achieve a consensus about the correct result in the case of one or more faulty systems. Typical examples are high-availability systems, such as autopilots in airplanes, which are working redundantly to enforce either a "majority vote" or a fallback to a predefined default case. For bookkeeping, there are no calculations to be aligned, but ledgers are to be kept synchronized. Consequently, automated reconciliation between different (internal and external) systems would be very welcome. DPLT promises to achieve this objective without the need for any manual reconciliation [Bott and Milkau (2016)]. While BFT is well established for calculation processes, the use of BFT for inter-ledger reconciliation is new and has to be compared with other technologies for the same purpose in terms of price, speed, quality, and resilience.

Synopsis V
DPLT is an option to implement byzantine fault tolerance and, consequently, enhance cyber resilience against attacks and technical outages in the financial services community as part of an active operational risk management in the first line of defense. However, it has to be clear that no technology can provide measures against financial default of counterparties or against systemic risk. To solve these issues, traditional intermediaries such as CLS for settlement

risk in FX transactions (originally Continuous Linked Settlement) or central counterparties for derivative transactions [CCPs, see, for example, Haar (2016)] are required. Those intermediaries will still play a structural role, although DLT can improve cyber resilience due to generic BFT, but with the costs of redundancy, on a technical level.

THE REDEFINITION OF SMART CONTRACTS AND SHARED SERVICE UTILITIES FOR SECURITIES

One proposed application for DPLT is securities post-trading (clearing, settlement, recordkeeping, reporting) with a redefined kind of smart contracts. As Clack et al. (2016) recently proposed: "A smart contract is an agreement whose execution is both automatable and enforceable. Automatable by computer, although some parts may require human input and control. Enforceable by either legal enforcement of rights and obligations or tamper-proof execution." The authors also proposed to implement a common language to support smart contract templates as a link between securities in the real world governed by securities legislation and smart securities on blockchain.

However, dematerialized securities, such as German "Girosammelverwahrung" [Bafin (2016)], already fulfill this definition. Any dematerialized security, which is recorded centrally at an issuer CSD, is in agreement with this definition, especially when one looks at automated dividend or interest payments, which will be initiated automatically from the issuer CSD when a data feed triggers this corporate action. Alternatively, smart contracts could automatically initiate coupon or dividend payments if triggered externally at the appropriate times with the appropriate data feed, avoiding (i) manual processes and (ii) guaranteeing that the issuer cannot default. This, however, requires that the funds are in escrow within the system (which is a strong assumption and can possibly jeopardize the business case) and that the external trigger is synchronized across the whole network.

A recent study of the Japan Exchange Group [Santo et al. (2016)] about the applicability of DLT to capital market infrastructure came to the conclusion that: "Non-deterministic factors such as time-trigger events, listening to outside data feed, or random number generation might prevent consensus because such processes are actually a challenge for smart contracts running each node to reach exactly the same result."

In addition to the technical challenge of synchronization in a decentralized network, Santo et al. pointed out the requirements for a solution to DvP (delivery versus payment) in fiat money and for payment finality with a proposed interconnection between DLT and traditional payment systems. A recent initiative by UBS [Kelly (2016)] is trying to define one possible solution with "utility settlement coin" (USC), which is described as a kind of central bank digital currency (CBDC) (see Figure 1).

However, this would be a step back when compared with TARGET2-Securities (T2S) with the integration of cash and securities settlement on one platform. DLT requires that funds for all future dividend or coupon payments and repayments are put "in escrow" in the blockchain ex-ante. Alternatively, the funds are not available on the blockchain, which brings us back to traditional reconciliation of payments along a chain of different accounting systems (i.e., the blockchain/USC/central bank money). Finally, the coding of payments from embedded options or covenants can be challenging, as a few hundred pages of contractual conditions need to be "translated" into a programming language [Sebastián (2015)].

Those fundamental problems of DLT in an extended network will help to create a centralized facility shared by a group of users, as already illustrated in Figure 1 (right side). The R3 consortium recently published a concept about a shared services utility "Concord" based on an underlying "Corda" technology for transactions in financial assets [Brown (2016)] with a "blockchain-inspired" vision about one central hub for securities transactions. This idea can be appreciated, as the (missing) standardization is an old challenge in the securities and derivatives markets. Most market participants would be keen for a more pragmatic standardisation (independently from who will set the standard), as any global standard helps to reduce costs and avoid manual corrections in back-office operations.

In addition to standardization, any long-term investment in securities requires asset protection, which has to be reflected in laws and regulation. One can discuss different options [Paech (2016a, b)], but any solution has to be in the triangle between (i) a fully decentralized system with a "tangible" corpus and coupon sheet in the hand of the investor, (ii) a central "digital" registrar with the issuer, or (iii) a system of "dematerialized" securities with bilateral contractual relationship along the whole custody chain. Nonetheless, responsibilities and obligations have to be covered by law [Sams (2015)].

Finally, even the law cannot prevent default and insolvency (but can define the framework to resolve such cases). The probability of such events requires an appropriate risk management to define risk appetite, mitigate risk exposure and manage risk events.

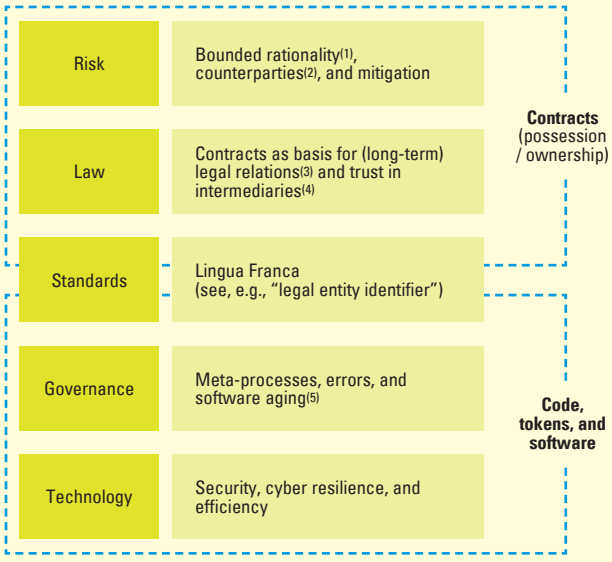
If one talks to lawyers about these questions, they will expect a precise question in legal terms. For example, in common law countries, possession is a property right in itself, while in civil law countries possession is not a right in itself but the simple fact of who has control over the asset. But control, including an entry in a database,

does not mean that there is any legal title to the object in civil law. Ask a lawyer how that relates to a data record on the blockchain in a global – cross-border/cross-jurisdiction – environment.

Short-term realistic use cases for DLT can be in those niches, in which the processing is mainly paper-based and automated reconciliation could provide an increase in efficiency and a reduction in operational risk potential (e.g., with centralized contract templates, automated checks, and instant exchange of information between the parties). Furthermore, private secondary markets for non-listed securities could be a starting point (in competition with traditional share registers) [Drummond (2016)].

Synopsis VI

Considering the current hype surrounding blockchain (for example, in terms of its potential applications in securities markets), the largest risk maybe the risk of overestimating DLT as the philosopher's stone. Especially, when used in distributed "private" ledgers (i.e., closed groups with permissioned/identified participants), the benefit of DLT comes from BFT, which provides cyber resilience plus efficiency enhancement due to automated reconciliation. However, additional layers (Figure 4) are needed to deliver a complete framework, such as for post-trade securities operations from a legal and regulatory perspective.



(1) see Grossman and Hart (1986), Hart and Moore (1990), and Hart (1995); (2) see Haar (2016); (3) see Lessig (2000); (4) see Luhmann (1968); (5) see Parnas (1994)

Figure 4 – A simplified illustration of the different layers required for a complete framework

CONCLUSION

In this paper, the current developments in DLT were reviewed from the point of view of operational risk management, and a first risk assessment was performed. The following findings were made:

- Similar to other technologies, DLT has principle limitations and underlying assumptions that have to be taken into account in an operational risk assessment.
- Although Bitcoin has generic inefficiencies, it is an innovative approach for "electronic cash" based on a game theoretical concept. And, while the consequent "eventual consistency" may be uncommon, the sources of operational risk are not, as long as the limits and assumptions are well understood and the systems is implemented with due diligence.
- The current Bitcoin ecosystem is a derivation from the idea of egalitarian peers and raises many concerns, and especially juridical questions, about liability, applicable law, etc. However, it does not generate new types of operational risk (besides misuse, fraud, etc.).
- The "TheDAO" hack made clear that current implementation of smart contracts in DLT has a fundamental flaw due to the combination of complex software (with inherent probability of errors and software aging) and the vision of an ultimately and unalterable "code is law" without any "stop button" in case of emergency.
- Any non-trivial contract between agents is subject to bounded rationality and incompleteness. Contractual relationships require governance models, intermediaries, and/or legal guidelines to cope with the "known unknowns" and the "unknown unknowns" over time as part of long-term risk management.
- DPLT is a focused option to implement byzantine fault tolerance and can improve cyber resilience and reduce manual reconciliation work, but is limited to technical measures of operational risk management.
- Any centralization towards a "utility" in global securities back-office processing would be appreciated, but this can be achieved with a set of alternative technologies. There is a significant risk to overestimate DLT beyond its technical capabilities.
- Niche application may be a first starting point for DLT based systems – especially for the register of non-exchange traded assets.

In specific, the combination of a – static – unalterable blockchain and – dynamic – contractual relationship with long-term consequences raises the question of whether "code is law" is a realistic claim. The idea of smart contracts is very mechanistic and normative, which ignores the probability of "incorrect" behavior in any complex system. For an operational risks assessment of a new technology, it is essential to distinguish between the different layers that are covered (i) by code and technology and (ii) by contracts and law (Figure 2).

These include a technology layer with possible benefits with regards to security, cyber resilience and efficiency (due to BFT and omission of manual reconciliations, etc.); a governance layer that has to cope with the complexity of – ever changing – software environments and, consequently, errors over the whole life-cycle; a standardization layer – as a core feature – that provides the lingua franca for the financial transactions (e.g., with the Legal Entity Identifier, LEI) [WFE (2016)]; a layer of contract legislation and, respectively, "trust" in intermediaries [Luhmann (1968)]; and a risk management layer that has to cover all the ex-post aspects, which are not according to the ex-ante contracts.

The risk assessment presented in this paper demonstrated that DLT can only cover the "lower" layers, which are defined by technical processes, but not those defined by contractual relationships. When technical concepts are overloaded with the expectation to solve non-technical problems, there is the risk of misunderstanding the capability of the technology. On the other hand, the discussion about blockchain is helpful as a catalyst for more discussion in the financial services industry about common standardization, shared services/centralization, and utilities for back-office operations with economies-of-scale.

REFERENCES

- Akkoyunlu, E. A., K. Ekanadham, and R. V. Huber, 1975, "Some constraints and trade-offs in the design of network communications," proceeding, SOSP '75, Fifth ACM Symposium on Operating systems principles, ACM New York, NY
- Ali, R., J. Barrdear, R. Clews, and J. Southgate, 2014, "Innovations in payment technologies and the emergence of digital currencies," Bank of England, Quarterly Bulletin 54:3, 262-275
- Attiya, H. and F. Ellen, 2014, Impossibility results for distributed computing, synthesis lectures on distributed computing theory, Morgan & Claypool Publishers
- Aven, T., 2011, Quantitative risk assessment: the scientific platform, Cambridge University Press
- Bafin, 2016, Merkblatt Depotgeschäft, Feb. 2014; www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_090106_tatbestand_depotgeschaeft.html (accessed 10.6.2015).
- Baldwin, C., and H. Poon, 2016, "Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong," Reuters, www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP (accessed 3.8.2016)
- Barrdear, J., and M. Kumhof, 2016, "The macroeconomics of central bank issued digital currencies," Staff working paper no. 605, Bank of England
- Bott, J., and U. Milkau, 2016, "Distributed ledger in payments and banking," Journal of Payments Strategy & Systems 10:2, 153-171
- Brewer, E., 2000, "Towards robust distributed systems," proceedings of the 19th annual ACM Symposium, Principles of Distributed Computing (PODC 00), ACM, 7-10.
- Brewer, E., 2012, "CAP twelve years later: how the "rules" have changed," Computer 02, 23-29
- Broadbent, B., 2016, "Central banks and digital currencies," speech, London School of Economics
- Brown, R. G., 2016, "Corda: an introduction – announcing the Corda introductory whitepaper," https://gendal.me/, posted August 24 (assessed 24.8.2016)
- Brus, L., 2016, "Ethereum to use hard fork to undo theft from The DAO," Coinfox News, July 8, http://www.coinfox.info/news/5883-ethereum-to-use-hard-fork-to-undo-theft-from-the-dao (accessed 14.7.2016)
- Buterin, V., 2016, "Thinking about smart contract security, blog, June 19, https://blog.ethereum.org/2016/06/19/thinking-smart-contract-security/ (accessed 21.6.2016)
- Castro, M., and B. Liskov, 1999, "Practical byzantine fault tolerance," proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, Feb. 1999, S. 173-186, USENIX Association
- Castro, M., and B. Liskov, 2002, "Practical byzantine fault tolerance and proactive recovery," ACM Transactions on Computer Systems (TOCS) 20:4, 398-461
- Cawrey, D., 2014, "Are 51% attacks a real threat to Bitcoin?" Coindesk, 20.6.2014, http://www.coindesk.com/51-attacks-real-threat-bitcoin/ (accessed 30.1.2015)
- Clack, C. D., V. A. Bakshi, and L. Braine, 2016, "Smart contract templates: foundations, design landscape and research directions," Aug. 4, 2016, https://arxiv.org/pdf/1608.00771 (accessed 24.8.2016)
- Correiam, M., G. Santos Veronese, N. Ferreira Neves, and P. Verissimo, 2011, "Byzantine consensus in asynchronous message-passing systems: a survey," International Journal of Critical Computer-Based Systems 2:2, 141-161
- Decker, Ch., and R. Wattenhofer, 2013, "Information propagation in the Bitcoin network," 13th IEEE International Conference on P2P-Computing, September
- de Rocquigny, E., 2009, "Quantifying uncertainty in an industrial approach: an emerging consensus in an old epistemological debate," S.A.P.I.EN.S 2:1
- del Castillo, M., 2016, "Ethereum executes blockchain hard fork to return DAO funds," Coindesk, 20.7.2016, http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/ (accessed 22.7.2016)
- Dienelt, J., 2016, "Understanding Ethereum – report," CoinDesk
- Douceur, J. R., 2002, "The Sybil attack," Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS 2002); http://research.microsoft.com/pubs/74220/IPTPS2002.pdf (accessed 20.6.2016).
- Drummond, S., 2016, "Sydney Stock Exchange's blockchain system targets venture capital funds, commodities," The Sydney Morning Herald, May 19, http://www.smh.com.au/business/banking-and-finance/sydney-stock-exchange-blockchain-targets-vc-commodities-20160518-goykn9.html (accessed 20.5.2016)
- Dwork, D. and M. Naor, 1992, "Pricing via processing or combatting junk mail," in Brickell, E. F., (ed.) Advances in cryptology – CRYPTO '92, Lecture Notes in Computer Science 740
- Economist, 2015, "The trust machine," October 31, www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine (accessed 2.7.2016).
- European Banking Authority, 2014, "EBA opinion on "virtual currencies"," www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (accessed 10.7.2014)
- European Banking Authority, 2016, "Opinion of the European Banking Authority on the EU Commission's proposal to bring virtual currencies into the scope of Directive (EU) 2015/849 (4AMLD)," www.eba.europa.eu/documents/10180/1547217/~EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD (accessed 10.7.2014)
- Eyal, I., 2014, "The miner's dilemma," ArXiv 1411.7099, available at: http://arxiv.org/abs/1411.7099 (accessed 1.2.2015).
- Finextra, 2016, "Bitfinex looks for fresh funding; spreads losses across all user accounts," August 8, www.finextra.com/newsarticle/29276/bitfinex-looks-for-fresh-funding-spreads-losses-across-all-user-acounts (accessed 8.8.2015).
- Fischer, M. J., N. A. Lynch, and M. S. Paterson, 1985, "Impossibility of distributed consensus with one faulty process," Journal of the ACM 32:2, 374-382
- Gigerenzer, G., and R. Selten, 2002, Bounded rationality, MIT Press, Cambridge, MA
- Greenspan, G., 2016, "Why many smart contract use cases are simply impossible," blog on www.coindesk.com, published on April 17, 2016; www.coindesk.com/three-smart-contract-misconceptions/ (accessed 2.7.2016).
- Grossman, S. J., and O. D. Hart, 1986, "The costs and benefits of ownership: a theory of vertical and lateral integration," Journal of Political Economy 94, 691–719
- Haar, B., 2016, "Freedom of contract and financial stability–introductory remarks," European Business Organization Law Review 17:1, 1–13

- Hart, O. D., 1995, Firms, contracts, and financial structure, Oxford University Press
- Hart, O. D., and J. Moore, 1990, "Property rights and the nature of the firm," Journal of Political Economy 98, 1119–1158
- Hearn, M., 2016, "The resolution of the Bitcoin experiment," Blog January 14, https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.z8f9vtaah (accessed 19.1.2016).
- Hoepmann, J. H., 2008, "Distributed double spending prevention," 15th International Workshop on Security Protocols, Lecture Notes in Computer Science 5964, 2010
- Ito, J., 2015, "Why Bitcoin is and isn't like the internet," January 18, www.linkedin.com/pulse/why-bitcoin-isnt-like-internet-joichi-ito (accessed 30.1.2015)
- Kelly, J., 2016, "UBS leads team of banks working on blockchain settlement system," Reuters, August 24 (accessed 24.8.2016)
- Lamport, L., R. Shostak, and M. Pease, 1982, "Byzantine general's problem," ACM Transactions on Programming Languages and Systems, ACM
- Leinonen, H., 2016, Virtual currencies and distributed ledger technology," Journal of Payments Strategy & Systems 10/2, 132-152
- Lessig, L., 2000, "Code is law", Harvard Magazine 1/2000, January 1, http://harvardmagazine.com/2000/01/code-is-law-htm (accessed 26.12.2015).
- Lindsay, B., P. Selinger, C. Galtieri, J. Gray, R. Lorie, F. Putzolu, I. Traiger, and B. Wade, 1980, "Single and multi-site recovery facilities," in Draffan, I. W., and F. Poole (eds.), Distributed data bases, Cambridge University Press; also available as IBM Research Report RJ2517, San Jose, CA (July 1979).
- Luhmann, N., 1968, Vertrauen: ein mechanismus der reduktion sozialer komplexität, F. Enke Verlag, Stuttgart; in English: Luhmann, N., 1982, Trust and power, John Wiley
- Luhmann, N., 1991, Soziologie des risikos, Walter de Gruyter, Berlin; in English: Luhmann, N., 1993, Risk: a sociological theory, Walter de Gruyter, Berlin.
- Lyu, M. R., 1996, Handbook of software reliability engineering, IEEE Computer Society Press and McGraw-Hill
- Marino, B., and A. Juels, 2016, "Setting standards for altering and undoing smart contracts," in: Alferes, J. J, L. Bertosi, G. Governatori, P. Fodor, and D. Roman (eds.), Rule technologies, Lecture Notes in Computer Science 9718, 151-166
- 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), 41
- Parnas, D. L., 1994, "Software aging," ICSE '94 Proceedings of the 16th International Conference on Software Engineering, 279-287, IEEE Computer Society Press Los Alamitos, CA
- Passas, N., 2006, "Demystifying hawala: a look into its social organization and mechanics," Journal of Scandinavian Studies in Criminology and Crime Prevention 7, 46–62
- Paech, P., 2016a, "Securities, intermediation and the blockchain – an inevitable choice between liquidity and legal certainty?" LSE Legal Studies Working Paper 20/2015 (update June 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2697718 (accessed 9.6.2016).
- Paech, P., 2016b, "Integrating global blockchain securities settlement with the law – policy considerations and draft principles," Draft Conference Paper, June, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792639 (accessed 3.7.2016).
- Reuters, 2016, "UBS leads team of banks working on blockchain settlement system," Reuters, August 24; http://www.reuters.com/article/us-banks-blockchain-ubs-idUSKCN10Z147; (accessed 26.8.2016)
- Sams, R., 2015, "Bitcoin blockchain for distributed clearing: a critical assessment," Journal of Financial Transformation 42, 39-46
- Santo, A., I. Minowa, G. Hosaka, S. Hayakawa, M. Kondo, S. Ichiki, and Y. Kaneko, 2016, "Applicability of distributed ledger technology to capital market infrastructure," Japan Exchange Group, JPX Working Paper 15, August 30
- Satoshi Nakamoto, 2008, Bitcoin: a peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf (accessed 10.1.2014).
- Sebastián, J., 2015, "Smart contracts: the ultimate automation of trust?" in Digital Economy Outlook, October, BBVA Research, https://www.bbvaresearch.com/en/?capitulo=smart-contracts-the-ultimate-automation-of-trust&post_parent=97745 (accessed 21.10.2015).
- Siegel, D., 2016, "Understanding the DAO attack," blog, June 25, www.coindesk.com/understanding-dao-hack-journalists/ (accessed 2.7.2016).
- Simon, H. A., 1957, "A behavioral model of rational choice," in Simon, H. A. (ed.), Models of man, social and rational: mathematical essays on rational human behavior in a social setting, Wiley
- Simon, H. A., 1991, "Bounded rationality and organizational learning," Organization Science 2:1, 125-134
- Sirer, E. G., and I. Eyal, 2013, "Majority is not enough: Bitcoin mining is vulnerable," in Sadeghi, A. R. (ed.), Financial cryptography and data security, Lecture Notes in Computer Science 8437, 436-454
- Sirer, E. G., 2016, "Thoughts on the DAO hack," blog, June 17, http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/ (accessed 21.6.2016)
- SWIFT, 2016, https://realworldchange.swift.com (accessed 10.5.2016).
- Turing, A. M., 1936, On computable numbers, with an application to the Entscheidungsproblem, Proceedings of the London Mathematical Society s2-42:1, 230-265
- Vogels, W., 2009, "Eventually consistent," Communications of the ACM 52:1, 40-44
- Wattenhofer, R., 2016, "The science of the blockchain," CreateSpace Independent Publishing Platform by Amazon, January 27
- WFE, 2016, World Federation of Exchanges: financial markets infrastructures and distributed ledger technology, August 25; http://www.world-exchanges.org/home/index.php/files/18/Studies%20-%20Reports/349/WFE%20IOSCO%20AMCC%20DLT%20report.pdf (accessed 26.8.2016).
- Williamson, O. E., 1979, "Transaction-cost economics: the governance of contractual relations," Journal of Law and Economics 22, 223-261
- Williamson, O. E., 1985, "Contractual man," in Williamson, O. E., (ed.) The economic institutions of capitalism, Free Press, 43-63
- Williamson, O. E., 2002, "The theory of the firm as governance structure: from choice to contract," Journal of Economic Perspectives 16:3, 171-195

FINANCIAL COMPUTING & ANALYTICS

STUDENTSHIPS

Four-Year Masters & PhD

for Final Year Undergraduates and Masters Students

As leading banks and funds become more scientific, the demand for excellent PhD students in **computer science, mathematics, statistics, economics, finance** and **physics** is soaring.

In the first major collaboration between the financial services industry and academia, **University College London, London School of Economics,** and **Imperial College London** have established a national PhD training centre in Financial Computing & Analytics with £8m backing from the UK Government and support from twenty leading financial institutions. The Centre covers financial IT, computational finance, financial engineering and business analytics.

The PhD programme is four years with each student following a masters programme in the first year. During years two to four students work on applied research, with support from industry advisors. Financial computing and analytics encompasses a wide range of research areas including mathematical modeling in finance, computational finance, financial IT, quantitative risk management and financial engineering. PhD research areas include stochastic processes, quantitative risk models, financial econometrics, software engineering for financial applications, computational statistics and machine learning, network, high performance computing and statistical signal processing.

The PhD Centre can provide full or fees-only scholarships for UK/EU students, and will endeavour to assist non-UK students in obtaining financial support.

UCL LSE Imperial College London

financialcomputing.org

INDUSTRY PARTNERS

Financial:

Barclays
Bank of America
Bank of England
BNP Paribas
Citi
Credit Suisse
Deutsche Bank
HSBC
LloydsTSB
Merrill Lynch
Morgan Stanley
Nomura
RBS
Thomson Reuters
UBS

Analytics:

BUPA
dunnhumby
SAS
Tesco

MORE INFORMATION

Prof. Philip Treleaven
Centre Director
p.treleaven@ucl.ac.uk

Yonita Carter
Centre Manager
y.carter@ucl.ac.uk

+44 20 7679 0359

Layout, production and coordination: Cypres – Daniel Brandt, Kris Van de Vijver and Pieter Vereertbrugghen

Imperial College Business School | Centre for Global Finance and Technology

Centre for Global Finance and Technology

The Centre for Global Finance and Technology at Imperial College Business School will serve as a hub for multidisciplinary research, business education and global outreach, bringing together leading academics to investigate the impact of technology on finance, business and society.

This interdisciplinary, quantitative research will then feed into new courses and executive education programmes at the Business School and help foster a new generation of fintech experts as well as re-educate existing talent in new financial technologies.

The Centre will also work on providing intellectual guidance to key policymakers and regulators.

"I look forward to the ground-breaking research we will undertake at this new centre, and the challenges and opportunities posed by this new area of research." – Andrei Kirilenko, Director of the Centre for Global Finance and Technology

Find out more here:
imperial.ac.uk/business-school/research/finance/centre-for-global-finance-and-technology/

CAPCO

BANGALORE
BRATISLAVA
BRUSSELS
CHICAGO
DALLAS
DÜSSELDORF
EDINBURGH
FRANKFURT
GENEVA
HONG KONG
HOUSTON
KUALA LUMPUR
LONDON
NEW YORK
ORLANDO
PARIS
SINGAPORE
TORONTO
VIENNA
ZÜRICH